



DIGITAL 2021

ECONOMY REPORT

Cross-border data flows and development:
For whom the data flow





DIGITAL ECONOMY REPORT 2021

Cross-border data flows and development:
For whom the data flow



© 2021, United Nations
All rights reserved worldwide

Requests to reproduce excerpts or to photocopy should be addressed to the Copyright Clearance Center at copyright.com.

All other queries on rights and licences, including subsidiary rights, should be addressed to:

United Nations Publications
405 East 42nd Street,
New York, New York 10017
United States of America
Email: publications@un.org
Website: <https://shop.un.org/>

The designations employed and the presentation of material on any map in this work do not imply the expression of any opinion whatsoever on the part of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Mention of any firm or licensed process does not imply the endorsement of the United Nations.

This publication has been edited externally.

United Nations publication issued by the United Nations Conference on Trade and Development.

UNCTAD/DER/2021

ISBN: 978-92-1-113022-5

eISBN: 978-92-1-005825-4

ISSN: 2664-2255

eISSN: 2664-2263

Sales No. E.21.II.D.18

Note

Within the UNCTAD Division on Technology and Logistics, the ICT Policy Section carries out policy-oriented analytical work on the development implications of information and communications technologies (ICTs) and e-commerce. It is responsible for the preparation of the *Digital Economy Report*, previously known as the Information Economy Report. The ICT Policy Section promotes international dialogue on issues related to ICTs for development, and contributes to building developing countries' capacities to measure e-commerce and the digital economy and to design and implement relevant policies and legal frameworks. The Section also manages the *eTrade for all* initiative.

In this Report, the terms country/economy refer, as appropriate, to territories or areas. The designations of country groups are intended solely for statistical or analytical convenience, and do not necessarily express a judgement about the stage of development reached by a particular country or area in the development process. Unless otherwise indicated, the major country groupings used in this Report follow the classification of the United Nations Statistical Office. These are:

Developed countries: the member countries of the Organisation for Economic Co-operation and Development (OECD) (other than Chile, Mexico, the Republic of Korea and Turkey), plus the European Union member countries that are not OECD members (Bulgaria, Croatia, Cyprus, Lithuania, Malta and Romania), plus Andorra, Liechtenstein, Monaco and San Marino. *Countries with economies in transition* refers to those in South-East Europe and the Commonwealth of Independent States. Developing economies in general are all the economies that are not specified above. For statistical purposes, the data for China do not include those for Hong Kong Special Administrative Region of China (Hong Kong, China), Macao Special Administrative Region of China (Macao, China) or Taiwan Province of China. An excel file with the main country groupings used can be downloaded from UNCTADstat at: <http://unctadstat.unctad.org/EN/Classifications.html>.

References to Latin America include the Caribbean countries, unless otherwise indicated.

References to sub-Saharan Africa include South Africa, unless otherwise indicated.

References to the United States are to the United States of America, and to the United Kingdom are to the United Kingdom of Great Britain and Northern Ireland.

The term "dollars" (\$) refers to United States dollars, unless otherwise indicated.

The term "billion" signifies 1,000 million.

The following symbols may have been used in the tables:

Two dots (..) indicate that data are not available or are not separately reported.

Rows in tables have been omitted in those cases where no data are available for any of the elements in the row.

A dash (-) indicates that the item is equal to zero or its value is negligible.

A blank in a table indicates that the item is not applicable, unless otherwise indicated.

A slash (/) between dates representing years, e.g. 1994/95, indicates a financial year.

Use of an en dash (–) between dates representing years, e.g. 1994–1995, signifies the full period involved, including the beginning and end years.

Annual rates of growth or change, unless otherwise stated, refer to annual compound rates.

Details and percentages in tables do not necessarily add up to the totals because of rounding.

Preface

The COVID-19 pandemic has accelerated the process of digital transformation and added urgency for Governments to respond. A key challenge is how to govern and harness the surge in digital data for the global good. It has been estimated that global Internet traffic in 2022 will exceed all the Internet traffic up to 2016.

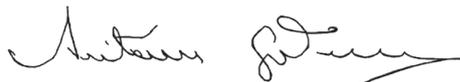
Data have become a key strategic asset for the creation of both private and social value. How these data are handled will greatly affect our ability to achieve the Sustainable Development Goals. Determining what is the best way forward will be difficult but necessary. Data are multidimensional, and their use has implications not just for trade and economic development but also for human rights, peace and security. Responses are also needed to mitigate the risk of abuse and misuse of data by States, non-State actors or the private sector.

Against this background, I welcome the *Digital Economy Report* of the United Nations Conference on Trade and Development, which examines the implications of growing cross-border data flows, especially for developing countries. It proposes to reframe and broaden the international policy debate with a view to building multilateral consensus.

It is more important than ever to embark on a new path for digital and data governance. The current fragmented data landscape risks us failing to capture value that could accrue from digital technologies and it may create more space for substantial harms related to privacy breaches, cyberattacks and other risks.

The Report calls for innovative approaches to governing data and data flows to ensure more equitable distribution of the gains from data flows while addressing risks and concerns. A holistic global policy approach has to reflect the multiple and interlinked dimensions of data and balance different interests and needs in a way that supports inclusive and sustainable development with the full involvement of countries trailing behind in digital readiness.

The United Nations offers a natural platform to advance this agenda with the involvement of all relevant stakeholders. This Report offers valuable insights and analyses, and I commend it to a wide global audience as we strive to close the digital divide and ensure that no one is left behind in the fast-evolving, data-driven digital economy.



António Guterres
Secretary-General
United Nations

Foreword

Rapid digitalization is affecting all aspects of life – including the way we interact, work, shop and receive services – as well as how value is created and exchanged. In this process, data and cross-border data flows are becoming increasingly crucial to development.

Reflecting the wide differences in the readiness to harness data that exist between and within countries, the conventional, connectivity-related digital divide is being compounded by what can be called a data-related divide. Countries with limited capacities to turn data into digital intelligence and business opportunities, and use them for economic and social development, are at a clear disadvantage.

This *Digital Economy Report 2021* points to the complexities involved in governing data and data flows across borders in ways that can bring sustainable development benefits. It also stresses that the state of the international debate on how to regulate cross-border data flows is at an impasse, and positions tend to be polarized. The current regulatory landscape is patchy, reflecting starkly different approaches adopted by different countries, with strong influences from the major economic powers.

An international framework is urgently needed to address this situation. While the Report does not provide “the solution”, its comprehensive, evidence-based analysis seeks to reframe and broaden the international policy debate. The increased interconnection and interdependence challenges in the global data economy call for moving away from the silo approach towards a more holistic, coordinated global approach. This may require new and innovative ways of global governance, as the old ways may not be well suited to respond to the new context. It may also necessitate the creation of a new international body that focuses on data-related governance, with the full involvement of developing countries and all stakeholders.

The Report reflects the commitment of UNCTAD to informing member States on how to engage in and benefit more from data and the digital economy. It will also feed into the much-needed global dialogue on how to set the rules of the game for a more inclusive outcome from digitalization. It is my hope that a holistic approach to global data governance will ultimately lead to enhanced sustainable development gains and economic benefits from the digital economy for people and businesses in countries at all levels of development.



Isabelle Durant
Acting Secretary-General
United Nations Conference on Trade and Development

Acknowledgements

The *Digital Economy Report 2021* was prepared under the overall guidance of Shamika N. Sirimanne, Director of the Division on Technology and Logistics, by a team comprising Torbjörn Fredriksson (team leader), Pilar Fajarnes Garces (lead author), Laura Cyron, Martine Julsaint Kidane, Woong Joe Ko, Vincent Riegel, Marcin Skrzypczyk and Thomas van Giffen.

The Report benefited from major substantive inputs provided by Carolina Aguerre, Shamel Azmeh, Zeynep Engin, Christopher Foster and Neha Mishra, as well as the Centre for International Governance Innovation (CIGI). Valuable comments were received from experts attending a virtual peer review meeting in February 2021, jointly hosted by UNCTAD, Research ICT Africa and CIGI. Participating experts included Susan Aaronson, Anna Abramova, Idris Ademuyiwa, Martin Adolph, Carolina Aguerre, Shamira Ahmed, Renata Avila, Shamel Azmeh, Dan Ciuriak, Niccolo Comini, Diane Coyle, Zeynep Engin, Bob Fay, Martina Ferracane, Christopher Foster, Henry Gao, Alison Gillwald, Ebru Gokce, Anita Gurumurthy, Victor Ido, Taisuke Ito, Jonathan Klaaren, Kostantinos Komaitis, Isya Kresnadi, Sophie Kwasny, Patrick Leblond, Stephen MacFeely, Moritz Meier-Ewert, Neha Mishra, Michael Pisa, Lorryne Porciuncula, Rishab Raturi, Gabriella Razzano, Nivedita Sen, David Souter, Tim Sullivan, Linnet Taylor, Stefaan Verhulst, Dong Wu and Anida Yupari. Written comments were also received from Jörg Mayer.

UNCTAD greatly appreciates additional inputs from the Economic Commission for Europe, the Economic Commission for Latin America and the Caribbean, the Economic and Social Commission for Asia and the Pacific, and the Economic and Social Commission for Western Asia. In addition, the following organizations generously provided highly appreciated inputs, based on their ongoing work: the Council of Europe; the Internet and Jurisdiction Policy Network; the Office of the United Nations Envoy on Technology; the United Nations Commission on International Trade Law; the United Nations Educational, Scientific and Cultural Organization; the United Nations Industrial Development Organization; and the United Nations Office for the Coordination of Humanitarian Affairs.

UNCTAD is grateful to the International Telecommunication Union for its support in the provision of relevant statistics.

The cover and other graphics were prepared by Magali Studer, and desktop publishing was done by Magali Studer and Carlos Bragunde. Infographics were done by Natalia Stepanova, and the Report was edited by Michael Gibson. Diana Quiros provided administrative support.

Financial support from the Government of Germany is gratefully acknowledged.

Contents

NOTE.....	iii
PREFACE.....	iv
FOREWORD.....	v
ACKNOWLEDGEMENTS.....	vi
LIST OF ABBREVIATIONS.....	xii
OVERVIEW.....	xiii

CHAPTER I RECENT TRENDS IN THE DATA-DRIVEN DIGITAL ECONOMY..... 1

A. INTRODUCTION.....	3
B. DEFINITIONS AND CHARACTERISTICS OF DATA.....	4
C. THE DIGITAL DIVIDE IN TERMS OF ICT ACCESS AND USE.....	8
1. Telephony and broadband access.....	8
2. Smartphone adoption and affordability of mobile Internet.....	10
a. Smartphone adoption.....	10
b. Smartphone and mobile data plan affordability.....	10
3. Speed of Internet connection.....	11
4. Internet use.....	13
5. E-commerce use.....	13
6. Digital gender divides.....	15
a. Gender gap in smartphone ownership.....	15
b. Gender gap in Internet use.....	15
D. GLOBAL EVOLUTION OF INTERNET AND DATA TRAFFIC.....	16
E. ESTIMATIONS OF THE VALUE OF DATA AND DATA MARKETS.....	17
F. MEASURING CROSS-BORDER DATA FLOWS.....	18
G. DATA COLLECTION.....	22
1. Digital platforms.....	22
a. Impact of the pandemic on global digital platforms.....	23
i. Digital advertising.....	23
ii. Profits.....	23
iii. Stock market prices and market capitalization.....	24
b. Influencing policymaking.....	27
i. Lobbying in the United States.....	27
ii. Lobbying in the European Union.....	28
c. Investment in AI start-ups and AI-related research and development by leading digital platforms.....	29
2. Internet of Things.....	32
H. DATA TRANSMISSION AND STORAGE.....	35
1. 5G mobile broadband.....	35
2. Submarine cables.....	36
3. Satellites.....	37
4. Internet exchange points.....	38
5. Cloud markets and data centres.....	39

I. DATA PROCESSING AND USE: ARTIFICIAL INTELLIGENCE	41
J. DATA IN RELATION TO HUMAN RIGHTS AND SECURITY.....	43
1. Privacy and surveillance	44
2. Security.....	45
3. Internet shutdowns.....	46
K. CONCLUSIONS AND ROAD MAP TO THE REST OF THE REPORT	46
CHAPTER II A REVIEW OF THE LITERATURE ON CROSS-BORDER DATA FLOWS	49
A. INTRODUCTION.....	51
B. DEFINING DATA AND CROSS-BORDER DATA FLOWS	52
C. QUANTIFYING CROSS-BORDER DATA FLOWS AND THEIR IMPACT	52
D. TYPES OF DATA	54
E. POSITIONS TOWARDS CROSS-BORDER DATA FLOWS.....	55
F. SCOPE OF RESEARCH.....	57
G. DEVELOPMENT PERSPECTIVE OF CROSS-BORDER DATA FLOWS	58
H. DRAWBACKS OF THE CURRENT LITERATURE	60
I. CONCLUSION AND OUTLOOK.....	61
CHAPTER III BACK TO BASICS: ISSUES AT STAKE	63
A. INTRODUCTION.....	65
B. DATA COLLECTION, PROFILING AND USE	66
C. THE MULTIDIMENSIONAL CHARACTER OF DATA	69
1. The economic dimension of data	69
2. Non-economic dimensions of data	71
D. OWNERSHIP, ACCESS, CONTROL AND RIGHTS OVER DATA.....	73
E. CROSS-BORDER DATA FLOWS, TRADE AND THE LOCATION OF DATA.....	74
1. Cross-border data flows versus international trade.....	74
2. The location of data.....	76
F. DIFFERENT TYPES OF DATA: IMPLICATIONS FOR CROSS-BORDER DATA FLOWS.....	78
1. Types of producers and users of data	78
a. Commercial data	78
b. Government and open data	79
c. Consumer data	79
2. Cross-cutting issues for personal and sensitive data	79
a. Personal data.....	79
b. Sensitive data	80
3. Technical aspects of data flows	81
G. POWER IMBALANCES AND INEQUALITY RESULTING FROM CROSS-BORDER DATA FLOWS.....	81
1. Concentration of market power	82
2. Data justice and inclusion	83
H. DEVELOPING COUNTRIES IN THE INTERNATIONAL DATA VALUE CHAIN	84

I. SOVEREIGNTY AND DIFFERENT LEVELS OF DATA GOVERNANCE.....	86
1. National sovereignty	86
2. Individuals, communities and groups	87
3. Geography	88
J. CONFLICTING INTERESTS IN CROSS-BORDER DATA FLOWS AND POLICY TRADE-OFFS.....	89
K. CAPACITY TO BENEFIT FROM DATA.....	90
L. CONCLUSION	91
ANNEX TO CHAPTER III: THE WAY DATA FLOW ACROSS BORDERS	94
1. The flow of data	94
a. The “client–server model”	94
b. The ISP 3-tier model	94
c. Steps in the data flow.....	95
2. How data cross national borders	95
a. Identifying cross-border data flows	95
b. Routing international Internet traffic	95
c. Registering cross-border data flows	96
CHAPTER IV MAIN GOVERNANCE APPROACHES TO THE DATA-DRIVEN DIGITAL ECONOMY WORLDWIDE: RISK OF FRAGMENTATION IN THE DIGITAL SPACE?.....	97
A. INTRODUCTION.....	99
B. MAJOR APPROACHES TO THE DIGITAL ECONOMY AND CROSS-BORDER DATA FLOWS.....	99
1. Promoting markets and innovation: the approach of the United States.....	100
2. Promoting national and public security, and championing digital development: the approach of China.....	102
3. Guarding individual rights and fundamental values: the approach of the European Union	104
4. Promoting national and public security: the approach of the Russian Federation	109
5. Championing domestic digital development: the approach of India.....	110
C. GLOBAL EXPANSION STRATEGIES BY THE UNITED STATES, CHINA AND THE EUROPEAN UNION	111
D. RISKS AND IMPACTS OF A POTENTIAL FRAGMENTATION IN THE DIGITAL SPACE	114
1. Fragmentation or convergence?	114
2. Impact of fragmentation on developing countries	115
CHAPTER V MAPPING NATIONAL POLICIES ON CROSS-BORDER DATA FLOWS.....	117
A. INTRODUCTION.....	119
B. DOMESTIC MEASURES ON CROSS-BORDER DATA FLOWS AND THEIR POLICY IMPLICATIONS	120
1. Policy rationales behind regulating cross-border data flows.....	120
a. Citizens’ protection policy lens	121
b. National security/sovereignty lens	122
c. Economic development lens	122

2.	Categories of national regulatory measures on cross-border data flows	123
a.	Scope of application	124
b.	Level of restrictiveness	125
i.	Strict localization.....	125
ii.	Partial localization	126
iii.	Conditional transfer – hard, intermediate or soft.....	126
iv.	Free flow of data	128
c.	Geographical versus accountability approach for personal data flows	128
3.	Domestic policy implications of regulating cross-border data flows.....	129
a.	The regulatory perspective: advantages and disadvantages.....	129
b.	The economic perspective: development-related necessities and risks.....	132
c.	The technological perspective: implications for global data governance	134
C.	MAPPING NATIONAL REGULATIONS ON CROSS-BORDER DATA FLOWS.....	135
1.	The regulatory spectrum for cross-border data flows	135
2.	Mapping regulations on cross-border data flows on the regulatory spectrum	136
D.	CONCLUSION	138
CHAPTER VI	REGIONAL AND INTERNATIONAL APPROACHES TO REGULATING CROSS-BORDER DATA FLOWS	141
A.	INTRODUCTION.....	143
B.	IS THERE A RATIONALE FOR REGULATING CROSS-BORDER DATA FLOWS AS INTERNATIONAL TRADE?	143
C.	REGULATION OF CROSS-BORDER DATA FLOWS IN TRADE AGREEMENTS.....	147
1.	Treatment of data flows in multilateral trade agreements	147
2.	Treatment of data flows in preferential trade agreements	151
a.	United States trade agreements	152
b.	European Union trade agreements	153
c.	Other trade agreements	154
3.	Results of regulating cross-border data flows through trade agreements	157
D.	INTERNATIONAL AND REGIONAL INITIATIVES ON CROSS-BORDER DATA FLOWS BEYOND THE TRADE DOMAIN.....	158
1.	Initiatives on cross-border data flows within the broad economic domain	158
a.	The G20 and “Data Free Flow with Trust”	158
b.	Digital Economy Partnership Agreement	160
c.	Asia–Pacific Economic Cooperation	160
d.	The Association of Southeast Asian Nations	161
2.	Initiatives on cross-border data flows beyond the economic and trade domain	162
a.	The OECD Privacy Guidelines	162
b.	Council of Europe Convention 108 and Convention 108+	162
c.	Malabo Convention	163
d.	Regional forums in Latin America.....	163
E.	CONCLUSIONS	165
CHAPTER VII	THE WAY FORWARD: IN SEARCH OF A BALANCED APPROACH	169
A.	RETHINKING REGULATION OF CROSS-BORDER DATA FLOWS.....	171
B.	THE NEED FOR GLOBAL DATA GOVERNANCE.....	174

C. KEY POLICY AREAS AND PRIORITIES	176
1. Agreement on a common understanding about definitions of data-related concepts....	176
2. Establishing terms of access to data.....	177
3. Strengthening efforts for measuring the value of data and cross-border data flows.....	177
4. Data as a (global) public good	178
5. Exploring emerging forms of data governance	179
6. Digital and data-related rights and principles.....	179
7. Data-related standards.....	180
8. International cooperation efforts on platform governance	181
D. INSTITUTIONAL FRAMEWORK	182
1. Multilateral, multi-stakeholder and multidisciplinary framework	183
2. Is there a need for an international coordinating body dealing with data-related issues?	184
E. POLICY SPACE FOR DEVELOPMENT	189
F. CAPACITY-BUILDING FOR DATA-DRIVEN DIGITALIZATION AND POLICYMAKING.....	189
1. Capacity-building for digitalization.....	189
2. Institutional capacity of Governments to regulate the data-driven digital economy.....	190
3. International support	190
G. CONCLUSIONS ON THE WAY FORWARD.....	191
REFERENCES.....	194

BOXES

I.1. Characteristics of data.....	6
I.2. Recommendations of the United States National Telecommunications and Information Administration report on “Measuring the Value of Cross-Border Data Flows”	21
I.3. Women working in AI research	32
I.4. Energy consumption of data centres and data transmissions networks	41
I.5. The semiconductor market.....	43
III.1. Internet tracking.....	68
IV.1. GAIA-X	106
IV.2. Privacy Shield and the Schrems II decision	107
IV.3. GDPR as a global standard for data protection?.....	113
V.1. Concepts related to national policies on cross-border data flows.....	120
VII.1. The Commission on Science and Technology for Development (CSTD) and international cooperation to address public policy issues related to the Internet.....	184
VII.2. Participation of developing countries in global data governance.....	186
VII.3. United Nations work on data governance-related issues.....	187
VII.4. Other initiatives of relevance for global data governance	188

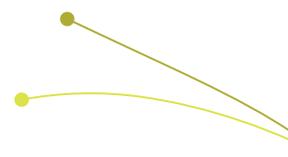
TABLES

I.1.	Internet activities undertaken by individuals, by level of development and region.....	14
I.2.	B2C E-commerce Index, by region, 2020.....	15
I.3.	Index of Digital Rights Corporate Accountability for digital platforms, 2020.....	44
III.1.	Classification of countries/country groups according to their data flows across borders, by level of development.....	85
IV.1.	Main features of data-related policies in the United States, China and the European Union.....	108
V.1.	Reasons for countries to regulate cross-border data flows.....	123
V.2.	Objectives and risks of restrictions on cross-border data flows.....	135
V.3.	Mapping of regulations on cross-border data flows.....	137
VI.1.	Participants in the Joint Statement Initiative 2019 (as of November 2020).....	151

FIGURES

I.1.	The data pyramid.....	7
I.2.	Mobile telephony and broadband subscriptions, by region, selected years.....	9
I.3.	Distribution of mobile network types coverage, rural and urban areas, by level of development, 2020.....	10
I.4.	Smartphone adoption, by region, selected years.....	11
I.5.	Price of 1.5 GB mobile broadband as a share of GNI per capita, 2019.....	12
I.6.	Broadband Internet connection speeds, global and by level of development, 2020.....	12
I.7.	Internet use, global, by level of development and by region, selected years.....	13
I.8.	Internet user gender parity score, by level of development and by region, 2013 and 2019.....	16
I.9.	Global data traffic, selected years.....	17
I.10.	Data market value, selected economies, 2016–2020.....	18
I.11.	International bandwidth, by region, 2015–2020.....	19
I.12.	Evolution of interregional international bandwidth, selected years.....	20
I.13.	Geographical distribution of the top 100 global digital platforms, by market capitalization 2021...	22
I.14.	Digital advertising spending, 2012–2022.....	24
I.15.	Profits by major digital platforms in the United States.....	25
I.16.	Profits by major digital platforms in China.....	25
I.17.	Stock prices of global digital platforms from the United States and China versus the New York Stock Exchange Composite Index.....	26
I.18.	Market capitalization of global digital platforms from the United States and China, Q4 2019–January 2021.....	27
I.19.	Lobbying by global digital platforms in the United States, 2010–2020.....	28
I.20.	Lobbying by global digital platforms in the European Union, 2015–2020.....	29
I.21.	Number of acquisitions of AI start-ups, top ten acquirers, 2016–2021.....	30
I.22.	Top 25 institutions for top-tier AI research.....	31
I.23.	Geographical distribution of AI researchers, by country of work and origin, 2019.....	31
I.24.	First job among graduates with PhDs in AI staying in the United States, by sector, 2014–2018...	31
I.25.	Geographical distribution of Internet of Things revenue by 2025.....	33
I.26.	Global number of IoT connections, by sector, 2018–2025.....	34
I.27.	5G adoption, by region, 2025.....	36

I.28.	Global mobile data traffic projections, by technology, 2020–2026	36
I.29.	Internet transmission map, June 2021	37
I.30.	Global used international bandwidth by type of provider, 2010–2020.....	38
I.31.	Internet exchange points, number and bandwidth by IXPs, by region, April 2021.....	40
I.32.	Cloud infrastructure service revenues, by provider, Q4 2020	40
I.33.	Private investment in AI companies, by economy, 2015–2020	42
II.1.	Number of publications on cross-border data flows, 1994–2020	51
III.1.	Different actors and complexity of relations in the context of cross-border data flows	89



List of abbreviations

AfCFTA	African Continental Free Trade Area
AI	artificial intelligence
APEC	Asia–Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
B2B	business-to-business
B2C	business-to-consumer
BCR	binding corporate rule
BGP	Border Gateway Protocol
BRI	Belt and Road Initiative
C2C	consumer-to-consumer
CAFTA	Central America Free Trade Agreement
CIS	Commonwealth of Independent States
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSTD	Commission on Science and Technology for Development
DEPA	Digital Economy Partnership Agreement
DSR	Digital Silk Road
FTA	free trade agreement
G2C	government-to-consumer
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDP	gross domestic product
GDPR	General Data Protection Regulation
GNI	gross national income
ICT	information and communications technology
IGF	Internet Governance Forum
IMF	International Monetary Fund
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet service provider
ITU	International Telecommunication Union
IXP	Internet exchange point
LDC	least developed country
MSMEs	micro-, small and medium-sized enterprise
ODA	official development assistance
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
RCEP	Regional Comprehensive Economic Partnership
SCC	standard contractual clause
TPP	Trans-Pacific Partnership
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
USMCA	United States–Mexico–Canada Agreement
W3C	World Wide Web Consortium
WEF	World Economic Forum
WTO	World Trade Organization

Overview

The *Digital Economy Report 2021* takes a deep dive into the development and policy implications of cross-border flows of digital data. Such data are core to all fast-evolving digital technologies, such as data analytics, artificial intelligence (AI), blockchain, Internet of Things (IoT), cloud computing and other Internet-based services. The topic is timely, as the expansion of data flows matters for the achievement of virtually all the Sustainable Development Goals, and countries around the world are struggling to determine how to deal with them from a policy perspective. The ultimate approach chosen at national and international levels will affect not only trade, innovation and economic progress, but also a range of issues related to the distribution of gains from digitalization, human rights, law enforcement and national security.

The present Report seeks to contribute to an enhanced understanding of these complex and interrelated factors, by providing a fresh and holistic view of this particular kind of international economic flow. Its analysis is based on a review of studies dealing with cross-border data flows from various perspectives, an overview of global developments and inequalities in the data-driven digital economy, and a discussion on the fundamental nature of data. The Report also looks at existing governance approaches at national, regional and multilateral levels, with a bearing on data flows. It concludes by calling for a more balanced approach to global data governance that could help ensure that data can flow across borders as freely as necessary and possible, while achieving an equitable distribution of benefits, within and across countries; and addressing risks related to human rights and national security.

Data flows are hard to measure, but growing fast

Measuring data traffic is difficult, but no matter which approach is used, the trend is steeply upwards. One forecast suggests that global Internet Protocol (IP) traffic in 2022 – domestic and international – will exceed all Internet traffic up to 2016. The COVID-19 pandemic had a dramatic impact on Internet traffic, as most activities increasingly took place online. Against this backdrop, global Internet bandwidth rose by 35 per cent in 2020, the largest one-year increase since 2013. It has been estimated that about 80 per cent of all Internet traffic relates to videos, social networking and gaming. Monthly global data traffic is expected to surge from 230 exabytes in 2020 to 780 exabytes by 2026.

Measuring *cross-border* data flows is even more challenging. In terms of volume, the most commonly used measure is that of total used capacity of international Internet bandwidth. This refers to the amount of data flowing in terms of bytes, but does not show the direction of the flows, nor anything about the nature and quality of the data. Available information also suggests that international bandwidth use accelerated during the pandemic, and that such traffic is geographically concentrated in two main routes: between North America and Europe, and between North America and Asia.

The data-driven digital economy is characterized by large imbalances...

When assessing the development implications of data and cross-border data flows, some key digital divides and imbalances need to be considered. Only 20 per cent of people in least developed countries (LDCs) use the Internet; when they do, it is typically at relatively low download speeds and with a relatively high price tag attached. Moreover, the nature of use differs. For example, while up to 8 in 10 Internet users shop online in several developed countries, that figure is less than 1 in 10 in many LDCs. Further, within countries, there are significant divides between rural and urban areas, as well as between men and women. The largest gender divides are observed among LDCs and in the African region.

In terms of capacity to engage in and benefit from the data-driven digital economy, two countries stand out: the United States and China. Together, they account for half the world's hyperscale data centres, the highest rates of 5G adoption in the world, 94 per cent of all funding of AI start-ups in the past five years, 70 per cent of the world's top AI researchers, and almost 90 per cent of the market capitalization

of the world's largest digital platforms. The largest such platforms – Apple, Microsoft, Amazon, Alphabet (Google), Facebook, Tencent and Alibaba – are increasingly investing in all parts of the global data value chain: data collection through the user-facing platform services; data transmissions through submarine cables and satellites; data storage (data centres); and data analysis, processing and use, for instance through AI. These companies have a competitive data advantage resulting from their platform component, but they are no longer just digital platforms. They have become global digital corporations with planetary reach; huge financial, market and technology power; and control over large swathes of data about their users. And they have seen their size, profits, market value and dominant positions strengthened during the pandemic, as digitalization has accelerated. For example, while the New York Stock Exchange Composite Index between October 2019 and January 2021 increased by 17 per cent, the stock prices of the top platforms rose by between 55 per cent (Facebook) and 144 per cent (Apple).

The traditional digital divide between developed and developing countries – understood in terms of Internet connectivity, access and use – remains high, and it is a recurrent challenge for development. Moreover, as the role of data as an economic resource, as well as that of cross-border data flows, has become more relevant, new dimensions of the digital divide have emerged, in connection with the “data value chain”. This concept is key for the estimation of the value of data. Value emerges in the process of transformation of raw data – from data collection, through analysis and processing into digital intelligence – that can be monetized for commercial purposes or used for social objectives. Individual data are of no value unless they are aggregated and processed. And vice versa, there cannot be digital intelligence without the raw data. For value creation and capture, both raw data and capacities to process them into digital intelligence are needed. Adding value to data is what contributes to moving up in the development process.

As the data-driven digital economy has evolved, a data-related divide has compounded the digital divide. In this new configuration, developing countries may find themselves in subordinate positions, with data and their associated value capture being concentrated in a few global digital corporations and other multinational enterprises that control the data. They risk becoming mere providers of raw data to global digital platforms, while having to pay for the digital intelligence obtained from their data.

...and a common understanding of what data, and their flows across borders, are and can do is lacking

Despite the importance of data in the evolving digital economy, there is no universally agreed understanding of the concept of data, which may lead to confusion and increase complexity in analyses and policy debates. Data are a special resource, with specific characteristics that make them different from goods and services. They are intangible and non-rival, which means that many people can use the same data simultaneously, or over time, without depleting them. At the same time, access to data can be limited by technical or legal means, resulting in varying degrees of excludability. For example, data collected by major global platforms are not readily available for others to use, giving the platform owners a monopolistic position to benefit from the data. Moreover, aggregated value may often be greater than the sum of individual values, especially if combined with other, complementary data. There can also be considerable “option” value of raw data collected, as they might become valuable if new issues that did not exist can be addressed on the basis of those data. The more detailed and granular the data, the more purposes they can be put to when filtered, aggregated and combined in different ways to provide different insights.

Moreover, data are of a multidimensional nature. From an economic perspective, they can provide not only private value for those who collect and control the data, but also social value for the whole economy. And the latter cannot be ensured by markets alone. Furthermore, the distribution of private income gains from data is highly unequal. As a result, there is a need for policymaking to support efficiency and equity objectives. However, there are also non-economic dimensions to consider, as data are closely related to privacy and other human rights, and national security issues, all of which need to be addressed.

Understanding data and their flows requires looking at them from different angles. First, there has always been *data and information associated with commercial transactions* – such as billing data, banking data, names and delivery addresses – which are mainly volunteered and rarely create policy-related issues, as long as new digital economy players work by the same rules as the conventional economy. Second, *raw data* gathered from individual activities, products, events and behaviours have no value in themselves, but can generate value once aggregated, processed and monetized, or used for social purposes. Third, the processing of raw data into digital intelligence – in the form of statistics, databases, insights, information, etc. – results in “*data products*”, which may be considered as services in trade statistics when sold across borders.

There are also different taxonomies that classify types of data according to various criteria. Important distinctions are related to whether data are collected for commercial or governmental purposes; are used by companies or the public sector; are instant or historic; are sensitive or non-sensitive; or are personal or non-personal. The categorization of data is important, as this may have implications for the kind of access that would need to be given to each type, both at national and international levels, as well as for how to handle the data and their flows across borders from a policy perspective.

Cross-border data flows are not trade and should be treated differently

The particular characteristics of data suggest that they need to be treated differently from conventional goods and services, including in their international transfers. In the new context of the data-driven digital economy, concepts such as ownership and sovereignty are being challenged. Rather than trying to determine who “owns” the data, what matters is who has the right to access, control and use the data.

There are significant difficulties in reconciling the notion of national sovereignty traditionally associated with country territories and the borderless nature, globality and openness of the digital space in which data flow. Digital sovereignty is often associated with the need to store data within national borders, but the link between the geographic storage of data and development is not evident. Assigning territoriality to cross-border data flows is also a challenge. Data can be better understood as shared, rather than as traded or exchanged.

International trade governance is informed by statistics that rely on the types, values and locations of trade (including source and destination). Such approaches are challenging, if not impossible, when tracking cross-border data flows, for which no official statistics exist. Well-established approaches applied to international trade across different territories (for example, rules of origin) cannot be easily applied to data, given their nature. The flows of raw data that are not linked to a specific exchange of a good or service are not included in the concept of “digital trade”, according to the Handbook on Measuring Digital Trade developed by several international organizations.

Beyond the technical challenges in identifying cross-border data flows, there are also political and cultural challenges. For many of the categorizations of data that can be outlined, globally agreed definitions are lacking. This sometimes makes it difficult to determine how data flows are to be dealt with. For example, varying definitions can lead to large differences in the volume of data flows that are categorized as personal data. Although data are strongly linked to trade, and they can provide strong competitive advantages to those capable of benefiting from them, cross-border data flows in themselves are neither e-commerce nor trade, and should not be regulated purely as such.

Command of data leads to information advantages, adding to the sources of potential market failure in economies built on data, including economies of scale and scope, as well as network effects. The information asymmetry inherent in the data economy seems irreducible, as there are no market solutions to correct for it. Additional trade-offs linked to the ethics of data are similarly important, including the relationship between creating value from data and data surveillance of populations, and the links between data filtering and censorship. As a consequence, the governance of data and data flows is crucial. However, while setting appropriate rules on cross-border data flows at the right point can help to guarantee data rights, reduce structural challenges and support economic development, there is no consensus on the policy approach to take.

Important implications emerge from diverging approaches to governing data and cross-border data flows

Among the major economic and geopolitical players in the digital economy, the approaches for governing data flows – and the digital economy more broadly – vary considerably, and there is, with few exceptions, little consensus at the regional and international levels. Worldwide, three main governance approaches are of particular influence. Somewhat simplified, the approach of the United States focuses on control of the data by the private sector. The Chinese model emphasizes control of data by the Government, while the European Union favours control of data by individuals on the basis of fundamental rights and values. The current context is one of tensions among these areas, particularly between the United States and China. Moreover, global digital corporations are seeking to expand their own data ecosystems.

There is a race for leadership in technological developments, as the leader may gain an economic as well as a strategic advantage, by controlling the data and related technologies, particularly with regard to AI. In this context, there is a risk of fragmentation in the digital space and of the Internet. Overall, there is a risk that a silo-oriented, data-driven digital economy will emerge, which goes against the original spirit of the Internet as a free, decentralized and open network. This would be suboptimal in economic terms, as more gains are likely to be obtained from interoperability.

Fragmentation in the data-driven digital economy would hamper technological progress, reduce competition and enable oligopolistic market structures to emerge in some areas, and lead to more government influence in others. This might have significant negative impacts for most developing countries. Fragmentation would reduce business opportunities, as the access of users and companies to supply chains would become more complicated, and data flows across borders would be restricted. There would also be more obstacles for collaboration across jurisdictions.

In spite of the risk of fragmentation, there are some signs of possible convergence among the main data realms. For example, despite its free market focus, the United States has taken steps towards restricting some foreign data-driven companies from entering its market, and banning related domestic data outflows. Meanwhile, China is hinting towards some openness to data flows. The final outcome is hard to predict, and depends on the will of policymakers worldwide to find a global solution that benefits all.

There can be various legitimate public policy reasons for countries to regulate cross-border data flows, such as the protection of privacy and other human rights, national security, as well as economic development objectives. As long as there is no proper international system regulating these flows, some countries may not see any other option than to restrict data flows in order to meet certain policy objectives. However, data localization does not automatically result in domestic data value addition. The link between the location of data storage and value creation is not obvious – there are costs as well as benefits to consider. A review of national policies suggests that they tend to vary depending on the technological, economic, social, political, institutional and cultural conditions in each country.

With data and cross-border data flows growing more prominent in the world economy, the need for global governance is becoming more urgent. Unfortunately, diverging views and positions on their regulation have resulted in an impasse on the current state of the international debate. Despite a growing number of trade agreements addressing data flows, disagreements continue to exist among the main players in the digital economy. Among members of the G20, there are contrasting views, not only on substance (for example, regarding data localization measures), but also on process.

Meanwhile, extreme positions on cross-border data flows will not be helpful, as neither strict localization nor fully free data flows are likely to satisfy the needs of countries to meet various development objectives. Regulation in this area needs to be rethought to find the basis for a middle-ground solution. New regulations will need to consider all dimensions of data, both economic and non-economic. They need to go beyond trade, and address data flows in a holistic manner, taking into account possible implications for human rights, national security, trade, competition, taxation and overall Internet governance. This raises the question of what is the appropriate international forum in which to address data-related policies for development.

There are good reasons for global governance of data and cross-border data flows

There is a strong rationale for a global data governance framework that complements other levels of data governance. The main arguments and reasons can be summarized as follows:

- Global data governance would help enable global data-sharing, and develop public goods that could help address major global development challenges, such as poverty, health, hunger and climate change.
- Technical coordination across borders – ideally at the global level – is essential to avoid further fragmentation of the Internet infrastructure and the digital space.
- Global data governance becomes more important in light of the implementation of 5G and IoT, as well as the acceleration in digitization triggered by the COVID-19 pandemic. These trends broaden the scope for vast data collection and monetization globally. Without a coherent underlying global governance framework to create trust, this could lead to a backlash in terms of data-sharing. It would also amplify already existing concerns over the lack of transparency in the data value chain, and over the unequal distribution of benefits from data.
- The proliferation of national regulations on cross-border data flows creates uncertainty and elevates compliance costs, which can be particularly pernicious for micro and small enterprises, especially in developing countries. The interconnected nature and high degree of global interdependence in the data-driven digital economy means that national policies in this area have spillovers on other countries.
- In the absence of global governance of digital platforms, self-regulation has led to market structures defined by platforms that predominantly benefit themselves, with various development and policy implications. The increasingly global reach and influence of major platforms makes it even more difficult for any single country to address related policy challenges.
- There is a need to develop a comprehensive and coherent assessment of the risks, vulnerabilities and outcomes of the business models of the digital platforms, in particular social media platforms, against a background of rising online harm at the global level.
- A global approach to data governance is needed to prevent long-standing inequalities against developing countries from becoming amplified in the data-driven digital space. It is essential to ensure that their local knowledge, needs and viewpoints become adequately represented in global policy discussions.
- Given the interdependencies and the interconnected character of the global architecture of the Internet, the future of cross-border data flows should not be determined only by a small number of major countries.

Data-driven digitalization creates global opportunities as well as global challenges that require global solutions to harness the positive and mitigate the negative impacts. Effective global governance of data is a prerequisite for data to support the attainment of the economic, social and environmental objectives of the 2030 Agenda for Sustainable Development, with people at the centre.

Efforts to develop a global approach to the governance of data and cross-border data flows should address a number of key policy areas and priorities, including the following:

- Developing a common understanding about definitions of key data-related concepts;
- Establishing terms of access to data;
- Strengthening the measurement of the value of data and cross-border data flows;
- Dealing with data as a (global) public good;
- Exploring emerging forms of data governance;
- Agreeing on digital and data-related rights and principles;

- Developing data-related standards; and
- Increasing international cooperation related to platform governance, including with regard to competition policy and taxation in the digital economy.

A new institutional setup is needed to meet the global data governance challenge

Existing institutional frameworks at the international level are not fit for purpose to address the specific characteristics and needs of global data governance. For it to be effective, a new global institutional framework is most likely needed, with the appropriate mix of multilateral, multi-stakeholder and multidisciplinary engagement.

So far, global governance of data and digital technologies has taken place along different tracks. First, most issues related to Internet governance, as a communications network, have been dealt with in various multi-stakeholder forums. A well-organized and globalized Internet community is deeply invested in approaches to coordinate Internet resources and making the network of networks function efficiently. These processes normally take place with peer-to-peer participation on an equal footing.

Second, and similarly, Convention 108 of the Council of Europe includes a forum where national Governments, regulators, private sector stakeholders and civil society representatives can all receive information and share insights on the promotion and improvement of the Convention.

Third, with the expansion of cross-border flows of data, Governments have sought to integrate their governance within international trade rules. These processes involve the negotiation of a set of rules between signatories, which may include dispute resolution mechanisms. In comparison with the other two tracks mentioned above, trade agreements are characterized by limited transparency, as negotiations tend to take place in closed processes, with little involvement of non-State stakeholders.

As an alternative to building upon existing organizations, growing calls have been made to develop a coordinating institution focused on, and with the skills for, assessing and developing comprehensive global digital and data governance. It would recognize that current global institutions were built for a different world, that the new digital world is dominated by intangibles, and that new governance structures are needed.

Achieving common ground and global solutions will not be easy. Indeed, in this age of populism, anti-globalization and competing vested interests associated with the capture of rents from the use of digital technologies and data, it may seem self-defeating to propose a new international body. Yet all of these factors make it more essential than ever to embark on a new global path for digital and data governance.

A reinforcement of the data realms or a splintering into multiple spheres would make a chaotic situation even more confusing. It would substantially diminish the value that can accrue from these technologies and the associated data, in addition to creating the space for substantial harms related to privacy, cybersecurity and other risks.

For global debates on the governance of data and cross-border data flows to be fully inclusive, they should ideally take place under the auspices of the United Nations, the most inclusive international forum in terms of country representation. Currently, developing countries tend to be underrepresented in global and regional initiatives, implying a risk of neglecting their needs, local knowledge and the cultural context in the global policy discussions, which results in increasing inequality. There are already various initiatives at the United Nations that are relevant to data governance, including by the United Nations Commission on Science and Technology for Development; the Office of the United Nations High Commissioner for Human Rights; the United Nations Commission on International Trade Law; the United Nations Educational, Scientific and Cultural Organization; the Internet Governance Forum; and the International Telecommunication Union. UNCTAD is also contributing through its three pillars of work, through research, consensus-building activities and its technical cooperation work. For the United Nations to be able to fulfil its role in this context, it will need to ensure effective links to other ongoing processes and initiatives led by civil society, academia and the private sector.

Making data flow for the benefit of all requires greater efforts to bridge the divides

Any efforts towards harnessing data and cross-border data flows will require adequate attention to the current divides that characterize the global digital economy. They can be seen not only between countries, but also between stakeholders. For example, the lack of appropriate skill sets in government directly results in insufficient representation of technical and analytical expertise in legislative and regulatory framework development processes. This in turn limits the chances of Governments to identify both the opportunities that could be afforded by digital technologies and the potential risks and threats that could emerge, as well as ways to regulate them. This risks translating into increased public dependency on the profit-driven private sector, with democratic values and individual human rights significantly undermined. Less-developed countries also suffer from losing their top talent to developed countries, and have smaller representation in setting up the global policy discussion – contributing further to the growing global inequality.

Any international framework for governing cross-border data flows needs to complement and be coherent with national policies for making the data-driven digital economy work for development. It will need to be flexible, so that countries with different levels of readiness and capacities to benefit from data have the necessary policy space when designing and implementing their development strategies in the data-driven digital economy. At the same time, national policies or strategies for development in this context are likely to fail if they do not keep the global perspective in mind.

While all countries will need to allocate more domestic resources to the development of their capacities to create and capture the value of data domestically, financial, technical and other resources may in many countries fall short of meeting those needs. This is especially true in LDCs. While the COVID-19 pandemic and its impact on government revenues have further reduced the availability of public funds, they have also made Governments and other stakeholders more aware of the need to improve their readiness to engage in and benefit from the evolving data-driven digital economy. This underscores the need for international support.

In the context of cross-border data flows, international support may focus on a range of areas. First, it can assist in terms of formulating relevant legal and regulatory frameworks. For example, less than half of all LDCs have data protection and privacy legislation in place. Second, many countries need to formulate national strategies for dealing with data and cross-border data flows in ways that can help reap economic development gains, while at the same time respecting human rights and various security concerns. Third, capacity-building activities may be needed to raise awareness of data-related issues and their development implications. Finally, in order to achieve inclusive outcomes of regional and global dialogues in this area, developing countries need to have a place at the table, as well as the means required to participate effectively in relevant processes and meetings.

Digital data and cross-border data flows play an increasingly important role in the world economy, with major implications for the attainment of the Sustainable Development Goals. Given the high speed at which data traffic is expanding – both domestically and internationally – there is an urgent need to improve the understanding of the dynamics of cross-border data flows, to enable the formulation of adequate policy responses at national as well as international levels.

This first chapter sets the stage for the Report, by providing a definition of data and highlighting some of their key characteristics. In the context of the global data value chain, it then examines recent trends in digital technologies of particular relevance to data and cross-border data flows. It underlines that the data-driven digital economy is characterized by major power imbalances between and within countries; these are reflected in the unequal levels of readiness among countries to harness data and their flows across borders for growth and development.

RECENT TRENDS IN THE DATA-DRIVEN **DIGITAL** ECONOMY



CHAPTER I THE DIGITAL DIVIDE IN TERMS OF INTERNET CONNECTIVITY AND USE IS COMPOUNDED BY A DATA-RELATED DIVIDE

Data are a special resource different from goods and services



For development purposes the distinction between raw data and data products (digital intelligence) is critical



The data-driven digital economy is rapidly evolving amid huge divides in terms of digital readiness



have no access to a mobile broadband network

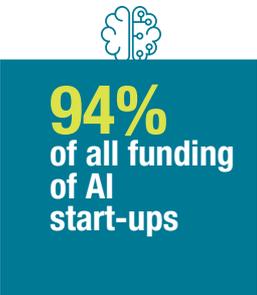
Average Internet speed



Use of Internet



Two countries stand out as the frontrunners in harnessing the value of data: the United States and China



The largest digital platforms increasingly control all stages of the global data value chain

During the pandemic their dominant positions have strengthened



The growth in data flows has just begun

Global Internet protocol traffic in 2022 will exceed all traffic up to 2016



International bandwidth use has accelerated during the last decade and is geographically concentrated along two main routes:



Data play an increasingly important role as an economic and strategic resource, a trend reinforced by the COVID-19 pandemic as many activities moved online

Cross-border data flows are a new kind of international economic flow, which lead to a new form of global interdependence

Regulating data flows at the international level has become more urgent

A. INTRODUCTION

Increasing digitalization of the economy and society is changing the ways people act and interact. One of the distinguishing features of various digital transformations has been the exponential growth in machine-readable information, or digital data, over the Internet (UNCTAD, 2019a). Such data are core to all fast-emerging digital technologies, such as data analytics, artificial intelligence (AI), blockchain, Internet of Things (IoT), cloud computing and all Internet-based services – and they have become a fundamental economic resource. The COVID-19 pandemic has accelerated digitalization processes, as more and more people have continued, to the extent possible, with their activities through online channels – for example, for working, studying, communicating, selling and buying, or entertainment (UNCTAD, 2021a).

Data and data flows, either domestic or international, can bring many benefits and contribute to solving societal challenges, including those related to the Sustainable Development Goals. While such gains should be harnessed, it is important to ensure that they are distributed in an equitable manner, rather than being captured by a few, and that social value is created. The current process of digitalization is associated with power imbalances and inequality, which need to be addressed. Data are much more than an economic resource, as they are also linked to privacy and other aspects of human rights, as well as national security. This points to the need for an integrated, holistic approach to policymaking in relation to data.

The importance of data is recognized by *The Age of Digital Interdependence – Report of the UN Secretary-General’s High-level Panel on Digital Cooperation* (United Nations, 2019). Its recommendations resulted in the Secretary-General’s Roadmap for Digital Cooperation (United Nations, 2020a), in which the need to harness data for development is also emphasized. For the United Nations system itself, the Secretary-General in 2020 presented the *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020–22* for the data-driven transformation. It notes that “Making better use of data – with approaches grounded in United Nations values and human rights – is integral to our future and service” (United Nations, 2020b:3).

Indeed, while the focus of UNCTAD at its foundation was on trade and development, it has naturally evolved towards a focus on interdependence and development, since trade and development cannot be dissociated from interdependence aspects. Thus, UNCTAD has become the focal point in the United Nations system for trade and development, and interrelated issues in the areas of finance, technology, investment and sustainable development. This is also related to the evolving context of interdependence among countries under globalization trends, as well as between national, regional and international policymaking. The data-driven digital economy has introduced a new form of interdependence, through cross-border data flows.

In the context of the data-driven digital economy, and most specifically in relation to cross-border data flows, the sentence popularized by the Uruguayan writer Mario Benedetti applies particularly well: “When we thought we had all the answers, all the questions suddenly changed.”¹ While many principles and parameters of conventional economics can be easily transferred to the digital economy, there are also many economic ideas that may not be of the same use and need to be adjusted in the new digital space. Also, as new concepts and dynamics emerge, there is a need to substantially rethink economics. It is therefore important to increase understanding of the role of cross-border data flows as a new key resource in international economic relations and development. Different questions that arise include:

- What are data?
- What are cross-border data flows?
- What are the implications of cross-border data flows for development?

¹ For the origins of this quote, see *El País*, 11 January 2016, *Queda inaugurada la nueva política*, and <https://citas.in/frases/1079317/history/>.

- What are the policy options with regard to cross-border data flows in order to maximize development opportunities and address the challenges to minimize risks in an integrated and equitable manner?

The aim of this Report is to contribute to an enhanced understanding of these issues. Building on previous UNCTAD research in this area,² it takes a deep dive into the issue of cross-border flows of digital data and the ways in which developing countries may be affected by such flows. It aims to provide a fresh and holistic view of the development implications of this new kind of international economic flow.

Issues related to the regulation of cross-border data flows are currently high up on the international agenda, particularly in the context of trade negotiations. But as already mentioned, these flows are relevant not only in the trade context, but also in relation to human rights, national security and law enforcement. Views on cross-border data flows tend to diverge widely, and the current debate is quite polarized. Some argue strongly for the facilitation of free data flows, while others stress in particular the need for domestic localization of data storage to achieve various national objectives. The current state of the debate on cross-border data flows can be described as being at an impasse.

This begs the question of how to find ways through which greater consensus can be achieved. In order to reap the full benefits from the Internet and for the data-driven digital economy to work for people and the planet, data need to be shared, including across borders. At the same time, there is an urgent need to properly regulate data flows at the international level, within the broad context of global data governance. Such regulations need to be flexible, accounting for the variety of conditions and the highly different levels of digital readiness, as well as the development objectives, of countries. As will be discussed in this Report, cross-border data flows, and the distribution of the benefits of such flows, can be governed by regulations in a range of areas. Finding a balanced governance approach is not going to be easy. The issues at hand are complex, there is a lack of common definitions, and measuring the phenomenon is challenging. This Report aims to add value in this context by contributing to strengthening the evidence base, improving understanding of the dynamics of cross-border data flows, and considering possible ways forward.

This chapter sets the stage – starting by providing a definition of data, and highlighting some of their key characteristics. Section C underlines the significant divides that still exist in terms of access to and use of information and communications technologies (ICTs). This is followed by analyses of the situation with regard to certain data-related variables that reflect new divides that are emerging in the evolving data-driven digital economy. Section D presents the global evolution of Internet and data traffic, while section E discusses issues related to estimations of the value of data and data markets. Difficulties in measuring cross-border data flows are addressed in section F. The following sections look at the evolution of data-related variables along the global data value chain: data collection (section G), data transmission and storage (section H), and data processing and use (section I). Each of these stages can take place in different countries, involving cross-border data flows. Section J explores non-economic data-related aspects linked to human rights, and trust-related issues. Section K provides some conclusions, as well as the road map for the rest of the Report.

B. DEFINITIONS AND CHARACTERISTICS OF DATA

Before looking at the evolution of the global situation in the data-driven digital economy, this section addresses the lack of clarity on the definition of data, as well as some key characteristics that make them different from goods and services. Essentially, in the digital economy, everything is data. Digitization of any product or activity (which can be generally called “events”) implies converting or coding it into a binary language of “zeros” and “ones”. Thus, everything on the Internet is numbers, and therefore data. Every zero or one represents a bit of *machine-readable* information, which is the smallest piece of

² The *Digital Economy Report 2019* focused on value creation and capture in the digital economy, highlighting the central role of data, and the implications for developing countries (UNCTAD, 2019a); and the *Information Economy Report 2017* emphasized the need to look at the interactions between global Internet governance and the international trade regime (UNCTAD, 2017). Moreover, a previous study on data flows focused on data protection issues (UNCTAD, 2016), and a recent study discussed the Joint Statement Initiative on e-commerce, including on issues related to cross-border data flows (UNCTAD, 2021b).

information that is digitally readable. These can be seen as the “virtual” representation of “real” life. The translation of real-life events into machine-readable codes of zeros and ones is made through software.

These coded events can then be transmitted through and stored in the hardware (e.g. submarine cables and data centres). The Internet is a network of networks; from the moment that bits leave the user devices and enter the network, data are flowing. Data flows refer to the transfer of these digitally encoded events (in zeros and ones) between digital devices. These data flows are not commercial transactions per se; they are just the way in which the machine-readable information is transmitted through the network. The functioning of the Internet and the digital economy is fundamentally based on how these data can flow within and between countries. Since the Internet is a global network, a large proportion of these are cross-border data flows (see chapter III on how data flow across borders).

What matters in general, and most particularly for regulation purposes, is what the zeros and ones represent in real life, in terms of “*human-readable*” information, or what can be understood by the human mind. Despite the importance of data in the evolving digital economy, there is no common understanding of the concept of data, which may lead to confusion and increase complexity in the analyses and policy debates. Indeed, most frequently in the literature and policy debates, the meaning of data is taken for granted, something that is commonly understood by everybody. It appears to be considered as a somehow homogeneous and homothetic entity – a monolith. But this is far from reality. There is in fact a significant lack of clarity about what the term means.

While many metaphors have been used to explain the nature of data, most notably oil, data are not like anything else, and these metaphors are not useful for policymaking purposes (De La Chapelle and Porciuncula, 2021). In order to understand that data are of a different nature from goods and services, as well as their value, it is important to acknowledge their specific characteristics, which are discussed in box I.1. In this connection, while cross-border data flows can have economic implications, they are a very different kind of international “economic” flow in comparison with other international economic flows, such as trade in goods and services or international financial flows, and therefore need to be approached from a different, broader perspective.

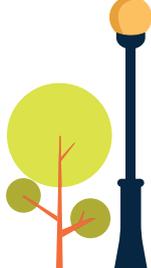
Data are small, unrelated pieces of “human-readable” information (data points), which may be numbers, but may also reveal qualitative aspects. Putting data together and processing them results in information, knowledge and wisdom that can be used to take more informed decisions. Data can be about people (such as demographics, behaviours and relationships), organizations (such as their types, activities and business relationships), the natural environment, the built environment or manufactured objects. Data can be used to make decisions with economic impacts, environmental impacts or effects on health, education or society in general (Coyle et al., 2020). Very often in the data-related analysis, and policy debates in the digital economy, these different levels of processing are mixed, although their implications vary significantly. The difference between data, information, knowledge and wisdom is illustrated in figure I.1. The pyramid reflects the use of data for good. Considering that technologies are not deterministic – i.e. not bad or good per se – but, depending on the use made of them, processing of data can also lead to negative results, for example through surveillance, affecting democratic processes. It follows that appropriate policies are needed to ensure that data are used for the benefit of people and the planet.

There is often too little distinction in the debate between different types and uses of data. Data are of different kinds and can be classified according to different taxonomies (see chapter III for a more detailed discussion on types of data). An important distinction is between volunteered and observed data. *Volunteered data* refer to information intentionally provided by the user, such as personal details shared on a social media platform or credit card information for online purchases. *Observed data* are information collected by an application or third-party software, with or without the knowledge or consent of the user, such as location data and web usage behaviour. These are extracted from activities on the web – for example, by digital platforms and from applications, connected machines and sensors – most often for free, on different aspects of users’ personal data, such as location, preferences, relationships and personal behaviour. The exponential increase in data through advances in digital technologies, particularly data analytics, relates mostly to the second kind of data. Thus, a large part of data are now observed data.

Box I.1. Characteristics of data

Data are intangible and non-rival, which means that many people can use the same data simultaneously, or over time, without them being depleted. At the same time, access to data can be limited by technical or legal means, resulting in varying degrees of excludability. In technical terms, data can be either a public good, a private good or a club good (when access to it is given to just a group of people). The place of data in the rivalry and excludability spectrum is illustrated in the box figure.

Box figure. Data in the rivalry-excludability spectrum

	EXCLUDABLE	NON-EXCLUDABLE
RIVAL	<p>Private goods: Food, oil, clothing and other manufactured products (smartphones), fish in a private pond, etc.</p> 	<p>Common goods: Forests, land, atmosphere, water, fish in the ocean, etc.</p> 
NON-RIVAL	<p>Club goods: Satellite TV, private parks, cinemas, copyrighted software, broadband Internet, paid streaming movies, etc.</p> 	<p>Public goods: National defence, air, sunshine, news, public TV, public parks, streetlight, lighthouses, etc.</p> 

Source: UNCTAD, based on Schneider (2019) and Liu (2021).

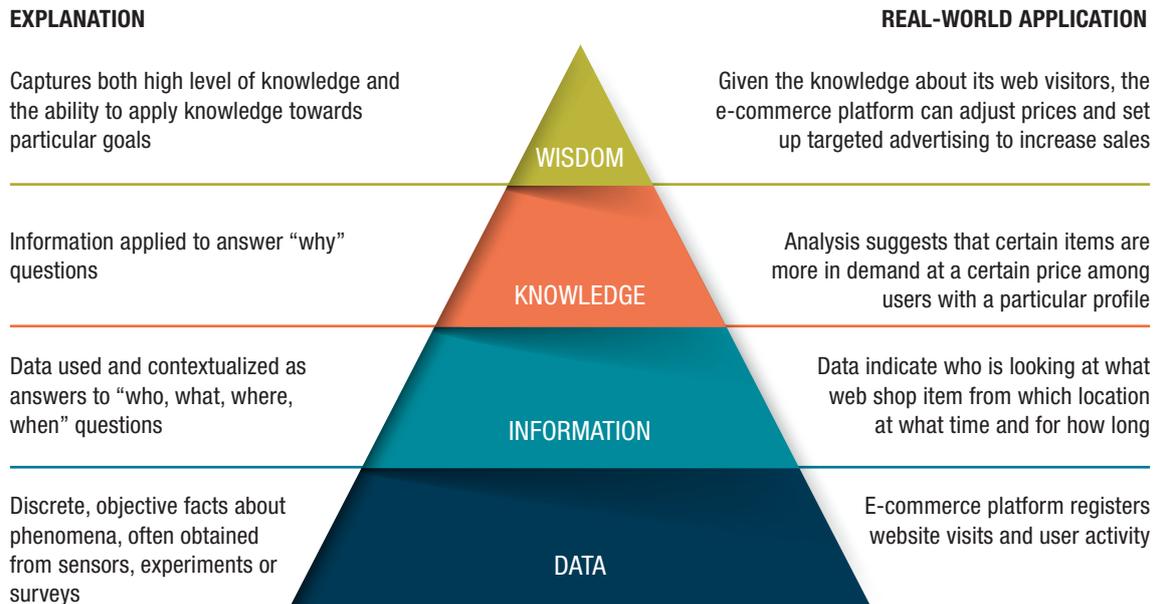
Data also often involve positive or negative externalities. Aggregated value may often be greater than the sum of individual values. Data also have a relational value – i.e. many kinds of data become more valuable from being combined with other, complementary data. Moreover, a priori individual data have no value, because it only materializes once data are aggregated, processed and used; thus, individual sources of data will have considerable “option” use or potential value, which means that they might become valuable in the event that new issues that did not exist can be addressed on the basis of those data. The more detailed and granular data are, the more purposes they can be put to because they can be filtered, aggregated and combined in different ways to provide different insights. As value lies in their use, it is highly dependent on the context (Coyle et al., 2020).

Overall, as discussed in chapter III, in economic terms, data can provide not only private value, for those who collect and control the data, but also social value for the whole economy, which points to the potential benefits of expanding access to data, publicly or privately collected, for public interest purposes. Thus, as markets alone cannot ensure social value, there is a need of policy for efficiency reasons. Moreover, there are equity reasons for policymaking, since the distribution of the private income gains is highly unequal.

Data may share some characteristics with different items, but their multidimensional nature makes them very specific and incomparable to those other items. From the economic perspective, data can be considered as an economic resource, as capital, as property, as labour and as infrastructure. But there are also non-economic dimensions to consider, as data are closely related to privacy and other human rights, as well as to national security issues. In any case, data are just data that, as will be discussed in chapter III, need to be addressed from all their dimensions.

Source: UNCTAD.

Figure I.1. The data pyramid



Source: UNCTAD, based on United States Chamber of Commerce Foundation (2014).

Another important distinction is between structured and unstructured data. *Structured data* are the easiest to search and organize, because they are usually contained in rows and columns, and their elements can be mapped into fixed predefined fields. Statistics are an example of structured data. *Unstructured data* cannot be contained in a row-column database, and do not have an associated data model. As in the case of observed data, the “big data” phenomenon is mostly related to unstructured data. An estimated 90 per cent of total data are unstructured.³ It should be noted that data are not big or small, but they can be processed in big or small amounts.⁴

It is also important to distinguish between different forms of data. First, *data and information associated with commercial transactions* – such as billing data, banking data, name, delivery address and so on – can flow across countries when these transactions are international. Be it in the physical or the digital world, these data are generally not to be commercialized per se, and they are transferred as part of normal commercial practices and codes of conduct. These data are mainly volunteered and should not create any policy-related issue, as long as new digital economy players work by the same rules as in the conventional economy.

Second, *raw data* – gathered from individual activities, products, events, behaviours, etc. – have no value in themselves, but can generate value once aggregated, processed and monetized, or used for social value.⁵ A useful definition of data for the purposes of this Report is “observations that have been converted into a digital form that can be stored, transmitted or processed, and from which knowledge can be drawn” (Statistics Canada, 2019). International flows of these *raw data*, which are a different

³ See *Forbes*, 18 October 2019, What’s The Difference Between Structured, Semi-Structured And Unstructured Data? and *Forbes*, 16 October 2019, What Is Unstructured Data And Why Is It So Important To Businesses? An Easy Explanation For Anyone.

⁴ In this connection, there appears to be some confusion in the literature and the debates with the term “data revolution”, which sometimes refers to the need to improve statistics and strengthen statistical capacities, and sometimes is taken as the digital technological revolution associated with what is called “big data” and data analytics.

⁵ Some observers consider that all data are the product of a particular context or societal mechanism, and in this sense they cannot be really qualified as raw. Acknowledging this sociological dimension, for the purposes of this Report, the term “raw” is understood as unprocessed, in the sense that no economic value is added to the data (see, for instance, Cattaruzza (2019)).

kind of flow from other international economic flows, are currently poorly regulated at the global level. In the absence of a proper international system of regulation for these data flows, it is mostly global digital platforms (or lead firms in global value chains), as well as Governments, that have access and can collect the data and control them, have the resources and capacity to refine and use (or abuse or misuse) them, and get the benefits of the data. Thus, it is “raw” (mostly observed and unstructured) data that are being massively collected with progress in digital technologies, as well as their flow across countries, that are introducing a new dimension for international policymaking to address the emerging related challenges. These raw data correspond to data at the basis of the pyramid in figure I.1.

Third, the processing of raw data into digital intelligence – in the form of statistics, databases, insights, information, etc. – results in “*data products*”. These data products correspond to information, knowledge and wisdom in the pyramid in figure I.1. They may be considered as services, and therefore their cross-border flows (when paid for) are captured in trade statistics and in trade regulations. However, the evolution of data-related technologies, and the accompanied expansion of trade in new data products/services, are mainly based on the processing of raw data. Thus, it is likely that the expansion of cross-border data flows may require adaptations of existing services trade rules.

C. THE DIGITAL DIVIDE IN TERMS OF ICT ACCESS AND USE

A brief review of the current, highly uneven state of play in the data-driven digital economy is a useful starting point to facilitate understanding of the possible development implications of cross-border data flows. In order to participate in and benefit from this economy, countries need to be able to access relevant communication technologies, which are the basis for the transmission of data. They also need to have the capabilities to make productive use of such access. There are still significant divides, within and among countries, in terms of capacities to connect to and use the Internet. Addressing these inequalities in the digital economy is key for development. This section focuses on different trends on mobile connectivity, type of connection, smartphone adoption, affordability and Internet use. However, these digital divides are a reflection of broader underlying income inequality within and between countries. Thus, acting only on ICT infrastructure policy aspects will not suffice; it is also important to address the global inequality challenge through economic policies.

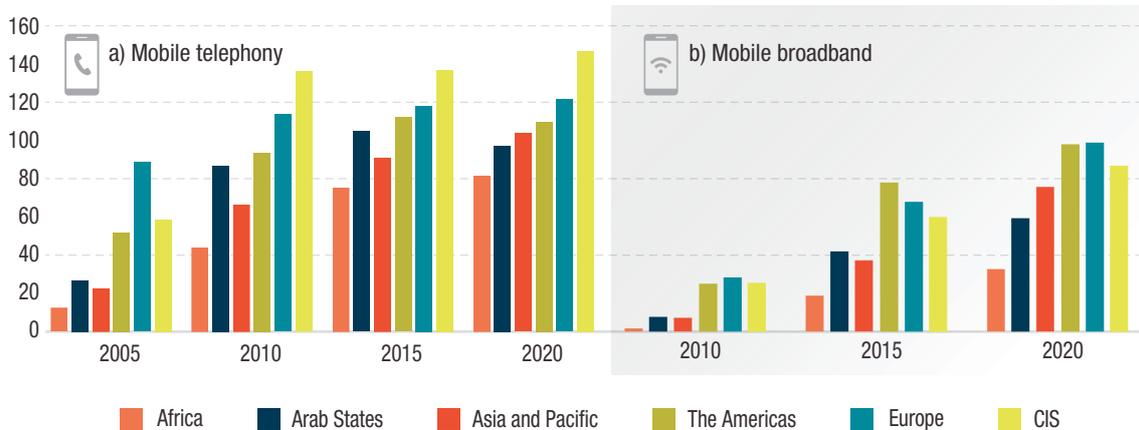
1. Telephony and broadband access

Fixed telephony has been declining in the last 15 years in both developed and developing economies, while it has never really picked up in least developed countries (LDCs). As for fixed broadband subscriptions, the penetration rate has increased in developed economies and developing countries. In the LDCs, however, the average number of these subscriptions per 100 people was virtually nil in the 2005–2020 period, as these countries have leapfrogged to increasingly efficient and accessible mobile connectivity. Although mobile telephony penetration rates in 2020 were still higher in developed countries than in developing countries, especially LDCs, the latter group experienced higher growth in this period, contributing to narrowing the gap. From a regional perspective, transition economies showed the highest rate of mobile telephony subscriptions in 2020, followed by Europe and the Americas. The lowest penetration rates were in Asia and the Pacific, Arab States and Africa. However, the latter regions, with the largest presence of developing countries and LDCs, experienced the most spectacular increases in 2005–2020 (figure I.2a).⁶

All groups of countries by level of development have experienced significant growth in mobile broadband penetration rates since 2010. However, large gaps remain over a decade later: the penetration rate in developed countries is double that of developing countries, and four times that of LDCs. At the regional level, mobile broadband subscriptions are lower than mobile telephony subscriptions (figure I.2b). The most significant growth in mobile broadband subscriptions was achieved in Africa, Asia and the Pacific

⁶ All statistics from online statistical databases used in figures and tables in this chapter were last updated in June 2021, unless otherwise indicated.

Figure I.2. Mobile telephony and broadband subscriptions, by region, selected years
(Per 100 people)



Source: UNCTAD, based on ITU Statistics database, available at www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
Notes: Country groups are those of the source. Data for 2020 are ITU estimates.

and Arab States, as they all started from very low levels in 2010. In the case of Africa, mobile broadband penetration in 2020 was nearly 20 times greater than in 2010. While this allowed developing countries to narrow the gap with more advanced countries, there is still a significant mobile broadband divide. In Europe and the Americas (including Canada and the United States), penetration rates reached almost 100 subscriptions per 100 people in 2020. The transition economies of the Commonwealth of Independent States (CIS) were relatively close to this level, but the penetration rates of mobile broadband in Asia and the Pacific, Arab States and Africa represented, respectively, three quarters, less than two thirds and only one third of the American and European levels. Mobile broadband penetration in Latin America in 2019 was estimated at 73 per cent (ECLAC, 2021).⁷

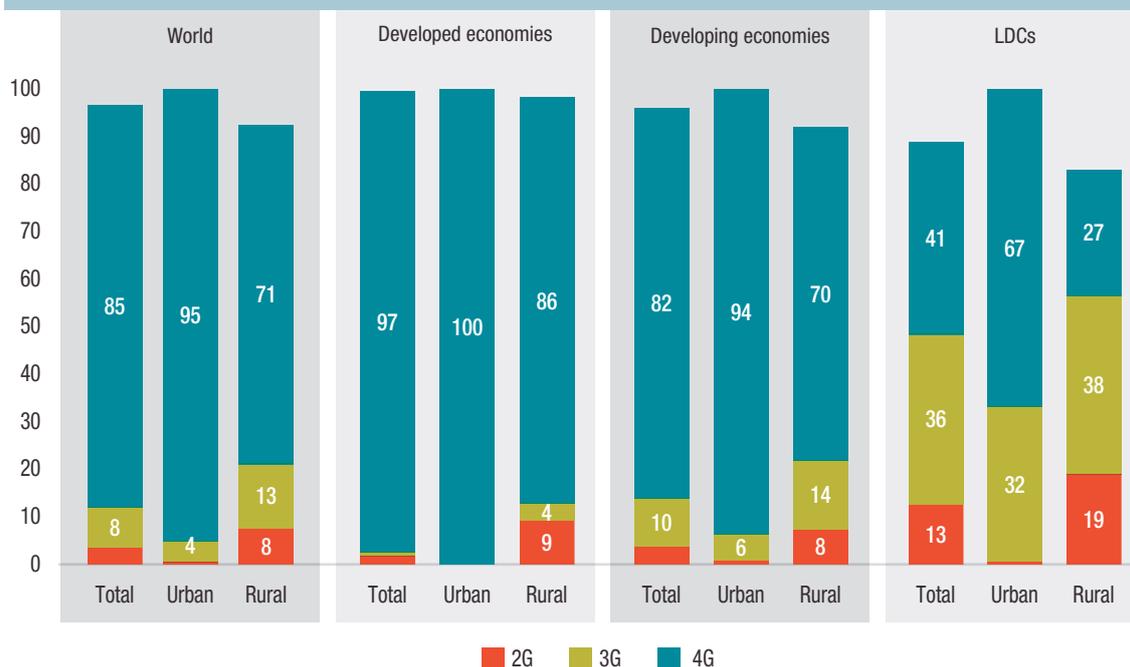
Among the reasons for this mobile broadband access gap are the differences in mobile broadband connection technologies (3G, 4G and now 5G), smartphone adoption, as well as the affordability of Internet-enabled phones and mobile data plans. Concerning mobile broadband, 93 per cent of the global population was covered by a signal from at least a 3G network in 2020 (figure I.3). The 5G networks started to be effectively implemented only in 2020. As discussed below, 5G connections are expected to become key in the context of the data-driven digital economy, as more and more data become available. About 98 per cent of the population in developed countries was covered by at least 3G networks in 2020, while that share in developing countries and LDCs was 92 per cent and 77 per cent, respectively. Therefore, in the case of LDCs, 23 per cent of the population had no access to a mobile broadband network in 2020. This is far from the United Nations Sustainable Development Goal Target 9.c to increase access to ICTs and strive to provide universal and affordable access to the Internet in LDCs by 2020 (Indicator 9.c.1 – Proportion of population covered by a mobile network, by technology). As noted above, an even lower share of the population has a mobile broadband subscription, especially in Africa, where most LDCs are located.

The technology divide is also visible within the same groups of countries, between urban and rural populations. The urban–rural access divide is most accentuated in LDCs, where 16 per cent of the rural population had no access to any mobile network, and 35 per cent could not be connected online with a mobile device (figure I.3).⁸ Still, this represents a significant improvement since 2015, when as much as 63 per cent of the rural population in LDCs lacked mobile access to the Internet.

⁷ As ITU data include Latin America in the Americas group, together with Canada and the United States, estimates of ECLAC only for Latin America are presented here.

⁸ The population with no access to mobile network is the result of the difference between the total rural population and the coverage of the sum of the three types of technologies (84 per cent). The population which is not connected online with a mobile device is the difference between the sum of the coverage by 3G and 4G (65) and the total rural population.

Figure I.3. Distribution of mobile network types coverage, rural and urban areas, by level of development, 2020
(Per cent of population)



Source: UNCTAD calculations, based on ITU Statistics database, available at www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Notes: The values for 2G and 3G networks show the incremental percentage of population that is not covered by a more advanced technology network (as an example, in the case of LDCs (total), 41+36+13=90 per cent of the population are covered by 2G, 41+36=77 per cent are covered by 3G and 41 per cent are covered by 4G). Country groups are those of the source. Data are ITU estimates.

2. Smartphone adoption and affordability of mobile Internet

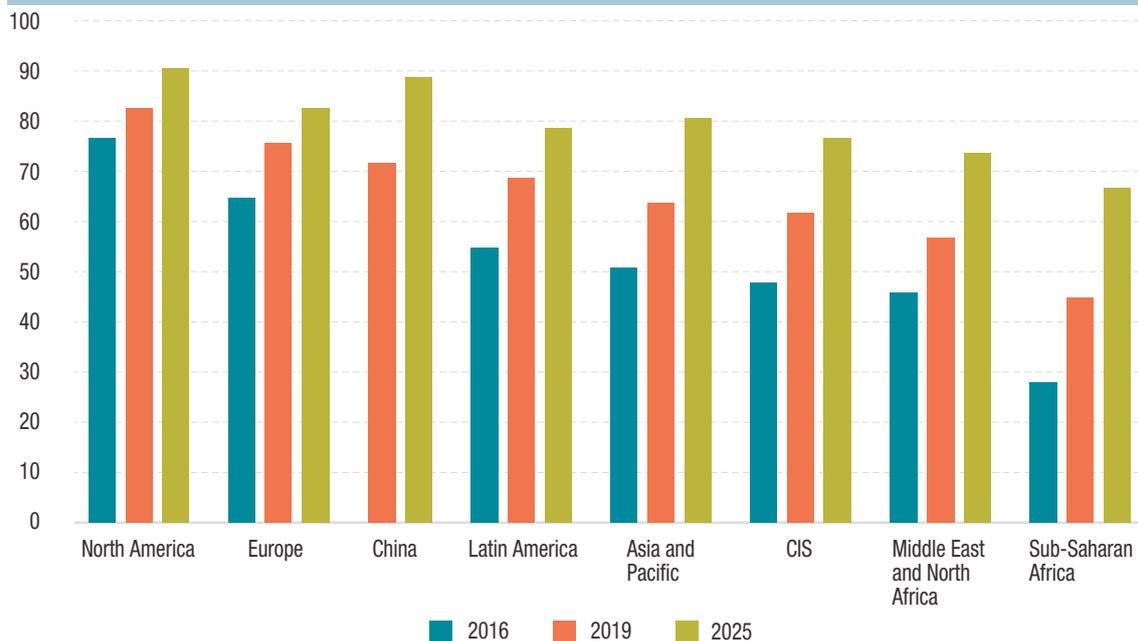
a. Smartphone adoption

Smartphones are a key tool for accessing the Internet and for transferring data. This is especially the case in most developing countries, where fixed broadband connection and computer use are less widespread. Smartphone adoption rates, as measured by the proportion of smartphones in all mobile connections, rose in all regions in 2016–2019 (figure I.4). However, gaps between regions remained in 2019. North America and Europe led in the smartphone adoption rate, followed by China. The smartphone adoption rate was lowest in sub-Saharan Africa, which, however, is forecast to experience the greatest growth in smartphone adoption by 2025. The growing trend in smartphone adoption is parallel to improvements in affordability of smartphones and data plan subscriptions, which is discussed below.

b. Smartphone and mobile data plan affordability

The cost of owning a smartphone is a barrier to connectivity and to fully benefitting from the data-driven digital economy in developing countries. GSMA (2020b) measured the affordability of the cheapest Internet-enabled feature phone or smartphone among different regions. In 2019, the cost of such a device represented on average 4 per cent of monthly gross domestic product (GDP) per capita in high-income countries. In countries with lower income per capita, this proportion was more than double in Latin America and the Caribbean (9 per cent), and as high as 30 per cent in sub-Saharan Africa. Purchasing an Internet-enabled phone or a smartphone does not, however, automatically lead to Internet access, which also requires a mobile data plan subscription.

Figure I.4. Smartphone adoption, by region, selected years
(Per cent)



Source: UNCTAD, based on GSMA (2017) and GSMA (2020a).
Notes: Country groups are those of the source. Data for 2025 are forecasts.

Mobile data plans are essential for making full use of mobile devices,⁹ offsetting the divide between developed and developing countries for staying connected at a fair cost. The Broadband Commission's Advocacy Target 2 says that, by 2025, entry-level broadband services should be made affordable in developing countries, at less than 2 per cent of monthly gross national income (GNI) per capita.¹⁰ In 2019, the target of 1.5 GB of mobile broadband to cost less than 2 per cent of monthly GNI per capita was achieved by 95 countries: 47 developed countries, 44 developing countries and 4 LDCs (figure I.5). ITU and UNESCO pointed out in their report on the state of broadband that, while the global data plan prices were declining between 2013 and 2019 (-15 per cent annual growth average), “for at least 40 countries, predominantly LDCs, entry-level mobile broadband services cost 5 per cent or more of average monthly GNI per capita. For 19 of those countries, the average cost is at alarming levels, greater than 10 per cent and 20 per cent” (ITU and UNESCO, 2020:16).

3. Speed of Internet connection

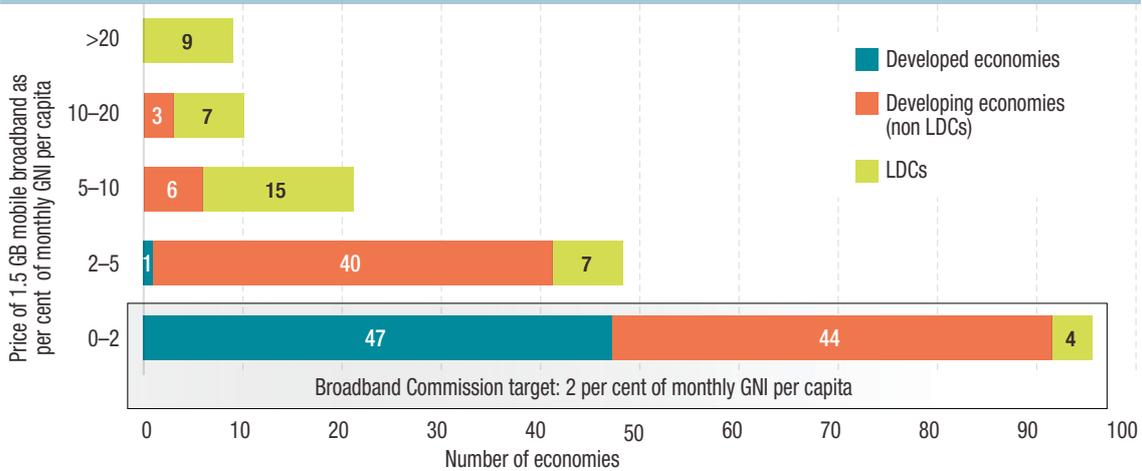
The speed of Internet connections is a key determinant for the capacity to generate and use data traffic. As the technology and use of the Internet have been evolving very rapidly in the last 20 years, the quality of connection matters. Different average speeds of connection may be good enough for basic activities, such as Internet browsing or emailing, but not for others, such as video calls.

In 2020, the speed of the *fixed* broadband Internet connection was on average higher than the speed of the *mobile* broadband Internet connection within all groups of economies, except LDCs (figure I.6). While this difference was less accentuated within the developing and transition economies, for developed economies, the average speed of the fixed connection was as much as double the speed of the mobile connection. The divide in the quality of Internet connection is very significant between the developed

⁹ In this context, data relate to the capacity to transmit information in terms of zeros and ones, thus the bytes available to be used.

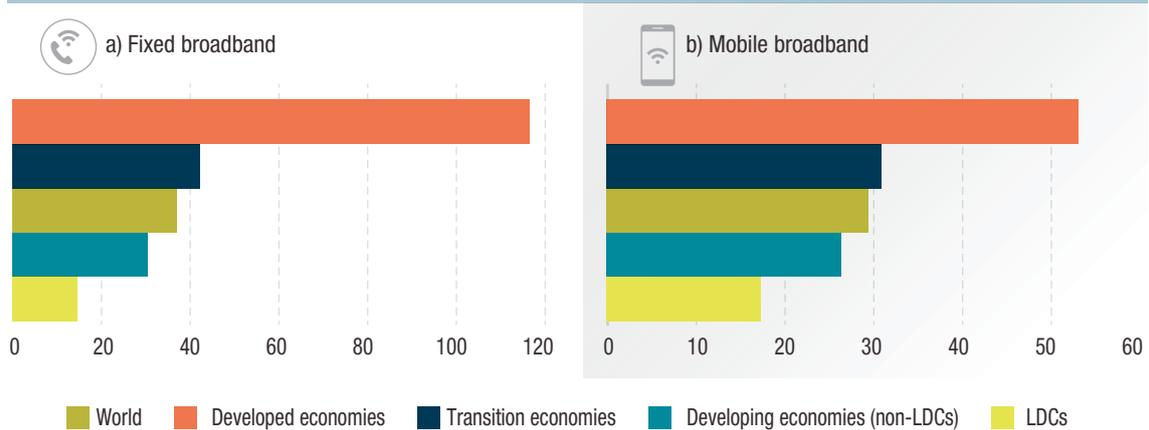
¹⁰ In 2018, the Broadband Commission launched the framework of Targets 2025 in support of “Connecting the Other Half” of the world’s population (see www.broadbandcommission.org/broadband-targets/).

Figure I.5. Price of 1.5 GB mobile broadband as a share of GNI per capita, 2019
(Number of economies)



Source: UNCTAD, based on ITU and UNESCO (2020).

Figure I.6. Broadband Internet connection speeds, global and by level of development, 2020
(Megabits per second)



Source: UNCTAD calculations based on Ookla, Speedtest Global Index, available at www.speedtest.net/global-index (accessed April 2021).

Notes: The global and group averages are the medians of the speed averages of countries.

economies and other economies. Concerning the fixed broadband connection, the observed average speed in developed economies was almost eight times that of LDCs, reflecting infrastructure and technological gaps (for example, in the diffusion of optical fibre).

Regarding mobile broadband connection speeds, the gap between developed economies and the rest is narrower. The deployment of mobile broadband access seems to be more beneficial for developing and transition economies, considering its cost and the technical capacities needed. This may indicate that the path to follow for LDCs should be to prioritize the development of mobile broadband access, as its average Internet connection speed is higher. However, while 3G and 4G technologies seem to be sufficient today, they may not be enough to effectively run the applications of the future. It will therefore be advisable for countries with nascent mobile broadband infrastructures to directly leapfrog the stages of ancient technologies and focus on 5G deployment, where funding and technical capacities are available.

4. Internet use

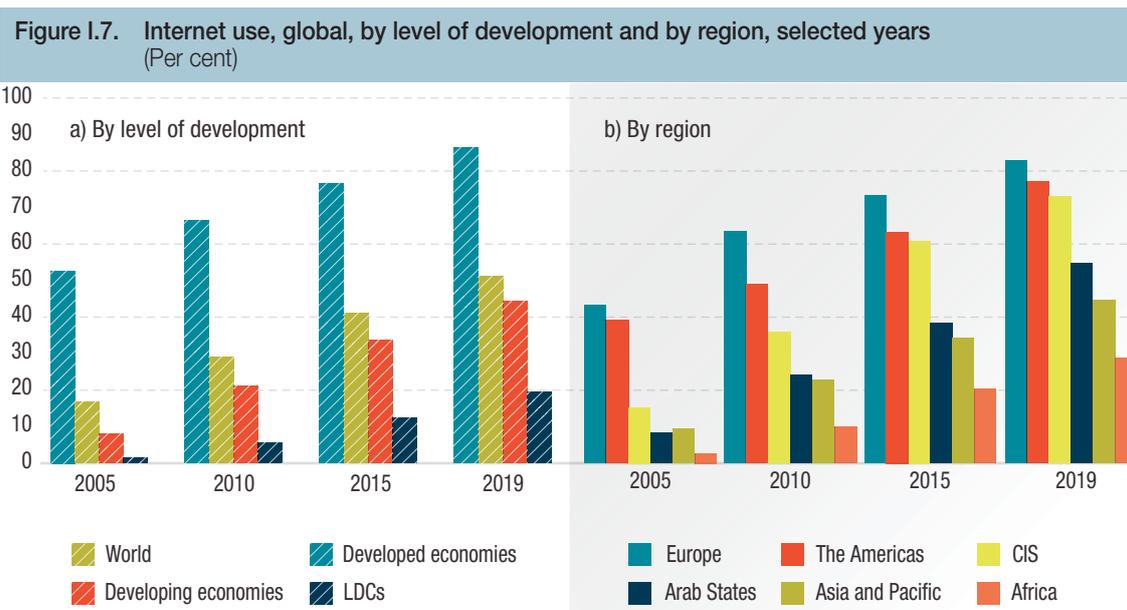
The deployment of fixed and mobile connectivity, the lowering costs of data plans, the wider use of mobile devices (feature phones, smartphones and tablets) and faster Internet connections have contributed to the upward trend of Internet use (figure I.7). In 2019, more than half the world's population used the Internet, a considerable increase from just above one tenth in the beginning of the 2000s. Nevertheless, the proportion of Internet users in developing countries (44 per cent) and LDCs (20 per cent) was still far behind that in developed countries. This divide remains a key issue of concern for the international community. The Broadband Commission for Sustainable Development 2025 Advocacy Target 3 suggests that, by 2025, broadband Internet user penetration should reach 75 per cent worldwide, 65 per cent in developing countries and 35 per cent in LDCs. "Forecasts based on current growth projections suggest that global Internet adoption by 2025 may only reach 70 per cent... For LDCs, the forecasted level by 2025 is 31 per cent" (ITU and UNESCO, 2020:21).

From a regional perspective, Europe and the Americas (including the United States, Canada and Latin America and the Caribbean) have been leading in Internet use the last 15 years. By contrast, even if other areas (especially Africa and the Arab States) experienced significant growth, Internet use was still significantly lower at the end of the period. Africa in particular lagged behind, with less than 30 per cent of individuals using the Internet in 2019. Internet use in Latin America was at 67 per cent (ECLAC, 2021).

In terms of economic development, it is also relevant to know which are the kinds of activities in which the Internet is used. For example, participation in social networks is less productive in economic terms than buying or selling goods online (e-commerce is discussed in the next subsection). An indication of the activities that individuals undertake using the Internet are shown in table I.1. For example, the use of Internet banking is much higher in developed economies than in transition and developing economies although, among these, Asia leads by far. This is also the case for purchasing or ordering goods or services. Participation in social media is high in all the regions considered, and it is higher in developing economies than in developed and transition economies.

5. E-commerce use

Among Internet users, the kind of activities that people engage in varies considerably. While more than 80 per cent of Internet users in some European countries shop online, in many LDCs the corresponding share is below 10 per cent (UNCTAD, 2021c). In Rwanda, for example, only 9 per cent of Internet



Source: UNCTAD, based on ITU Statistics database, available at www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
Notes: Country groups are those of the source.

Table I.1. Internet activities undertaken by individuals, by level of development and region (Per cent)					
Internet activity	Developed economies	Transition economies	Developing economies - Africa	Developing economies - Asia	Developing economies - Latin America and the Caribbean
Internet banking	62.3	14.9	9.8	34.8	11.6
Sending or receiving email	84.9	44.8	46.6	59.7	52.4
Making calls (telephoning over the Internet/Voice over Internet Protocol, using Skype, iTalk, etc.)	56.9	71.0	47.6	63.2	73.4
Reading or downloading online newspapers or magazines, electronic books	76.4	41.5	38.6	46.0	30.3
Getting information about goods or services	83.9	50.9	30.6	68.0	51.8
Getting information from general government organizations	55.1	11.1	17.6	20.9	23.2
Interacting with general government organizations	54.5	5.7	12.1	25.6	10.7
Purchasing or ordering goods or services	53.9	18.2	14.6	29.1	13.1
Seeking health information (on injury, disease, nutrition, etc.)	62.4	37.5	24.3	47.1	41.1
Making an appointment with a health practitioner via a website	16.4	3.9	4.0	7.6	3.1
Participating in social networks	70.4	70.7	86.3	87.2	79.0
Accessing or posting opinions on chat sites, blogs, newsgroups or online discussions	13.9	11.6	45.1	26.5	26.0
Selling goods or services	16.8	7.0	3.5	6.4	9.3
Using services related to travel or travel-related accommodation	55.0	5.7	7.5	25.2	28.4
Doing a formal online course	8.1	4.5	17.5	15.9	28.5
Consulting wikis, online encyclopedias or other websites for formal learning purposes	23.8	14.6	17.2	13.2	31.4
Listening to web radio	61.2	17.0	13.3	20.9	11.2
Watching web television	41.1	8.8	30.2	33.1	18.1
Streaming or downloading images, movies, videos or music, playing or downloading games	57.4	52.9	64.2	66.4	50.8
Downloading software or applications	19.0	5.5	62.8	41.0	20.7
Looking for a job or sending/submitted a job application	17.4	9.8	14.3	19.9	16.6
Participating in professional networks	21.0	3.6	5.9	6.4	0.7
Uploading self/user-created content to a website to be shared	38.8	33.4	12.7	21.3	35.6
Taking part in online consultations or voting to define civic or political issues	9.8	3.5	5.5	8.1	N/A
Using storage space on the Internet to save documents, pictures, music, video or other files	38.7	15.0	17.5	20.8	21.7
Using software run over the Internet for editing text documents, spreadsheets or presentations	28.0	4.3	6.1	11.7	4.8

Source: UNCTAD calculations, based on ITU World Telecommunication/ICT Indicators database.

Notes: Country groups are those of the source. Averages for country groups are medians of countries for which data are available and for the latest year, which varies between 2015 and 2019.

users used the Internet to buy something online in 2017. E-commerce developments greatly depend on a country's capacity or readiness to engage in and benefit from the digital economy. The UNCTAD business-to-customer (B2C) E-commerce Index, which is calculated as the average of four indicators, shows the existing differences among countries. The regional values of the 2020 index are shown in table I.2. The relative strengths and weaknesses generally differ. For East, South and South-East Asia, the only indicator below the world average is Internet use. In Latin America and the Caribbean, the main opportunities for improvement are found in postal reliability. To facilitate more inclusive e-commerce, African countries would benefit from catching up in all areas covered by the index.

6. Digital gender divides

While the above discussion focuses on the digital divide among countries, the gender digital divide is highly visible within countries in terms of both smartphone ownership and Internet use.

a. Gender gap in smartphone ownership

A 2018 survey on a sample of developed and developing countries in terms of female and male ownership of smartphones by the Pew Research Center (2019) showed that, for both women and men, on average, smartphone ownership in their respective groups was lower in developing countries than in developed countries (48 and 71 per cent for women, 52 and 80 per cent for men, respectively). The gender gap, defined as the difference between the smartphone ownership rates for males and females, relative to the smartphone ownership rate for males, was on average wider in developing economies than in developed economies. However, it narrowed on average between 2015 and 2018. The greatest gender gap in 2018 was noted in India (56 per cent) and the smallest in the Philippines (-9.6 per cent), where more women than men owned smartphones.

b. Gender gap in Internet use

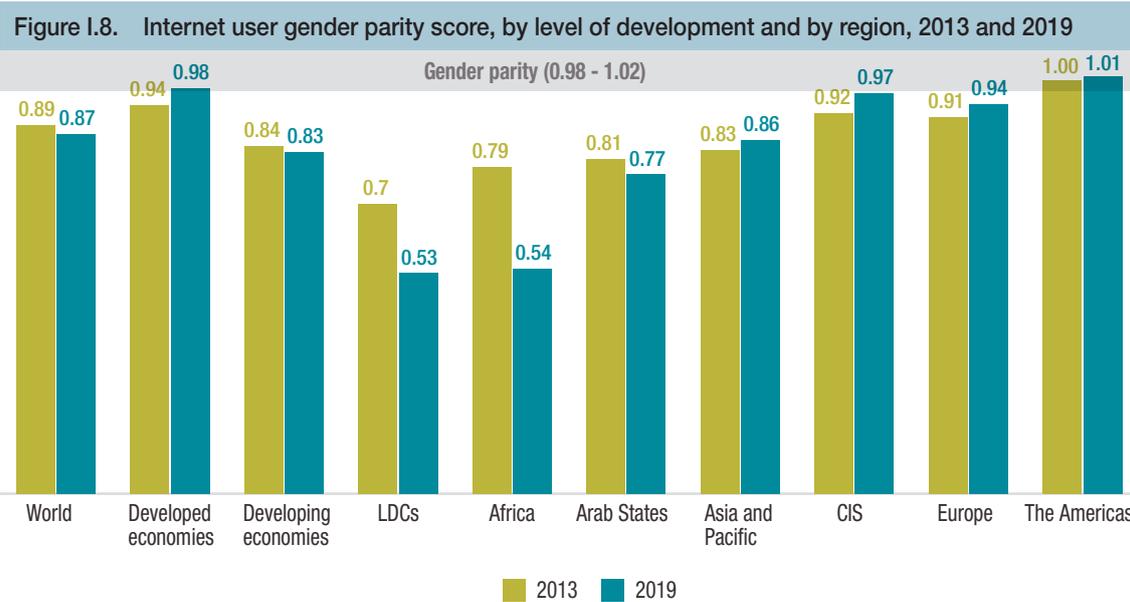
ITU (2020) estimated that, globally, the level of the male and female population using the Internet in 2019 was 55 and 48 per cent, respectively. This translates into a gender parity score of 0.87 (figure I.8), where total parity at a level of 1 is the target. The gender parity score is calculated as the proportion of women who use the Internet divided by the proportion of men.¹¹ At the global level, the score decreased slightly between 2013 and 2019. It increased in Asia and the Pacific, CIS, Europe and the Americas. However, it decreased in the Arab States, and especially in Africa (from 0.79 to 0.54). Similarly, while it increased in developed countries, it decreased marginally in developing countries, and significantly in LDCs (from 0.70 to 0.53).

Table I.2. B2C E-commerce Index, by region, 2020

Groups, by region and level of development	Share of individuals using the Internet (2019 or latest)	Share of individuals with a bank account (15+, 2017)	Secure Internet servers (normalized, 2019)	UPU postal reliability score (2019 or latest)	2020 Index value	2019 Index value (2018 data)
Africa	30	40	28	21	30	31
East, South and Southeast Asia	57	60	54	58	57	58
Latin America and the Caribbean	64	53	50	29	49	48
Western Asia	77	58	45	50	58	59
Transition economies	71	58	60	59	62	63
Developed economies	88	93	84	80	86	87
World	60	60	53	47	55	55

Source: UNCTAD (2021c).

¹¹ A value smaller than one indicates that men are more likely to use the Internet than women, while a value greater than one indicates the opposite.



Source: UNCTAD, based on ITU (2020).
 Note: Country groups are those of the source.

The COVID-19 pandemic put the spotlight on all the connectivity and usage divides discussed above. As people reacted to the pandemic-related lockdown measures by increasingly connecting to the Internet to be able to continue with their activities, those countries and sectors within countries that lagged behind in terms of connectivity found higher difficulties in coping with the pandemic. Although there was a global upsurge of e-commerce around the world in 2020, many smaller businesses in developing countries struggled to go digital and meet the growing demand for online sales.¹²

The remaining huge divides in terms of connectivity, access, affordability and availability of ICTs, within and between countries, have been the traditional focus of analyses and policies. Moving forward, it will become increasingly important to address these divides for developing countries, and particularly LDCs, to be able to advance in the digital economy for development. As more and more aspects of life and activities become digitalized, and data increasingly become a key resource for development, other aspects related to the capacity to access and transfer data represent additional dimensions of the digital divide. The following sections therefore look at the global evolution of data and Internet traffic, as well as at emerging divides related to the collection, transmission and use of data.

D. GLOBAL EVOLUTION OF INTERNET AND DATA TRAFFIC

The importance of the Internet and digital data for economies and societies continues to grow. Their expansion, as measured by Internet Protocol (IP) traffic, is an estimation provided by private sector proprietary statistics, as there are no official country statistics on this matter. The methodologies used are not standardized, not totally clear, and the periodicity of publication of data is not necessarily regular. Thus, assessing the evolution of global Internet and data traffic is not an easy task. Nevertheless, the different estimations all suggest that global Internet and data traffic has exploded in recent decades, and that this rapid growth is expected to continue with the ongoing fast progress in digital technologies.

Regarding global IP traffic, it would appear that the most updated data were those already presented in UNCTAD (2019a),¹³ which showed that IP traffic was expected to more than triple between 2017 and 2022. Most Internet traffic takes place in the Asia and the Pacific and North America regions, with

¹² For a global review on COVID-19 and e-commerce, see UNCTAD (2021a).

¹³ The analyses in UNCTAD (2019a) were based on Cisco (2018). It appears that Cisco is no longer publishing these forecasts and trends, and now publishes an Annual Internet Report (Cisco, 2020), which does not include IP traffic statistics.

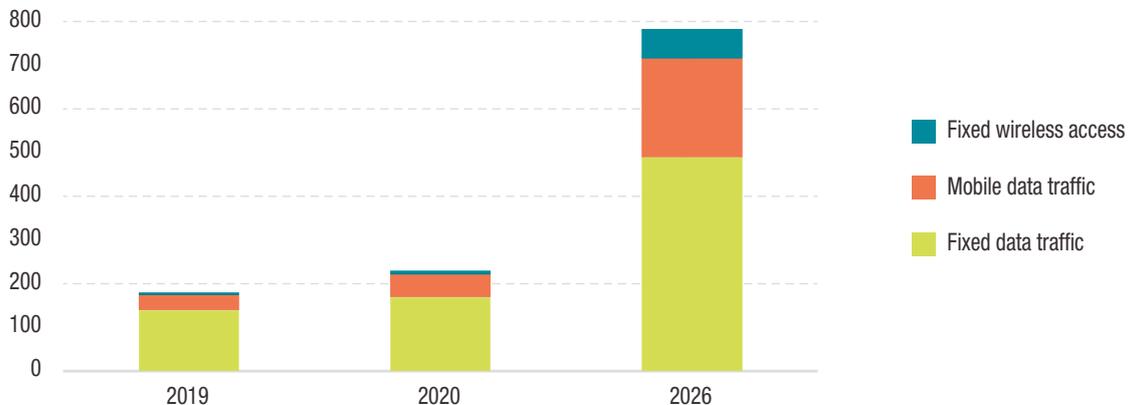
very little share accounted for by Latin America and the Middle East and North Africa. According to one forecast, global IP traffic in 2022 is expected to exceed all the Internet traffic up to 2016.¹⁴ Moreover, the number of devices connected to IP networks will be more than three times the global population by 2023 (Cisco, 2020).

The COVID-19 pandemic had a dramatic impact on Internet traffic, as most activities increasingly took place online. Global Internet bandwidth use rose by 35 per cent in 2020, a substantial increase over the 26 per cent growth of the previous year. Driven largely by the response to the pandemic, this represented the largest one-year increase since 2013. Although from March 2020 such traffic patterns shifted and volumes surged, the Internet has proven remarkably resilient in coping with the sudden changes associated with the pandemic. Many network operators have been accelerating plans to add capacity to stay ahead of demand (TeleGeography, 2021a).

According to Ericsson (2020), mobile network data traffic increased by 50 per cent between the third quarter (Q3) of 2019 and Q3 2020. Global data traffic reached 180 and 230 exabytes per month in 2019 and 2020, respectively (figure I.9). By 2026, this volume is forecast to more than triple, to reach up to 780 exabytes per month. Fixed data traffic accounted for almost three quarters of all data traffic in 2019. However, with the increasing number of mobile devices and IoT, data traffic by mobile broadband is expected to grow faster and reach almost one third of the total data volume in 2026.

By other accounts, in 2020, 64.2 zettabytes of data were created or replicated, defying the systemic downward pressure asserted by the pandemic on many industries, and its impact will be felt for several years. It is estimated that the amount of digital data created over the next five years will be more than twice the amount created since the advent of digital storage. Global data creation and replication will experience a compound annual growth of 23 per cent in the 2020–2025 forecast (IDC, 2021a).

Figure I.9. Global data traffic, selected years
(Exabytes per month)



Source: UNCTAD, based on Ericsson (2020).

E. ESTIMATIONS OF THE VALUE OF DATA AND DATA MARKETS

Measuring the value of data remains a major challenge. The concept of the “data value chain” is key for the estimation of the value of data. Value emerges in the process of transformation of raw data – from data collection, through processing, and analysis, into digital intelligence – that can be monetized for commercial purposes or used for social objectives (UNCTAD, 2019a). In this process, individual data are of no value unless they are aggregated and processed. And there cannot be digital intelligence without the raw data. For value creation and capture, both raw data and capacities to process them into digital intelligence are needed.

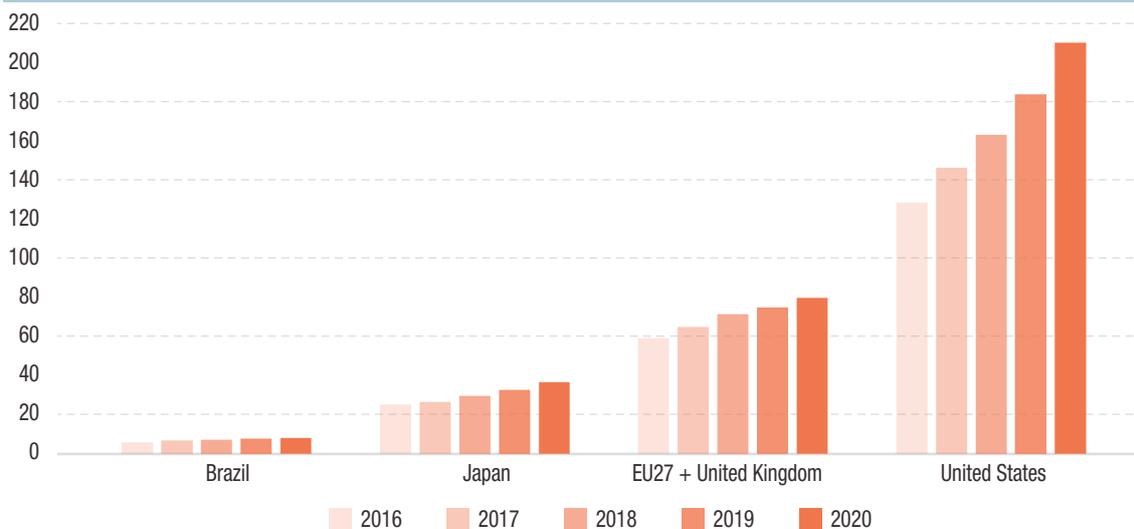
¹⁴ See Cisco, 27 November 2018, Cisco Predicts More IP Traffic in the Next Five Years Than in the History of the Internet.

A priori, without knowing how the data will be used, the value of raw data cannot be estimated. But raw data can be understood to have potential value. Moreover, contrary to goods, data are non-rival and they can be used several times without being depleted. In addition, there are not properly developed and formalized raw data markets; as will be further discussed in chapter III, data cannot be thought of in terms of ownership, but mostly in terms of rights and access. There is no marketplace with supply and demand for raw data; they are currently basically extracted from users. Most often, when referring to data markets, it concerns markets for digital intelligence (or data products).

Most of the estimations of the value of data actually refer to the value of such markets for data products. These estimations may provide some indication of the value of the raw data used in the production of these data products; if the value of data products increases, the value of raw data should increase accordingly. But they provide little information on how to differentiate the value of raw data from the value added during the processing and monetization of the data. Indeed, in terms of development, what matters is the domestic value added in production processes in the developing countries.

As an illustration, the European Data Market Monitoring Tool defines the data market as “the marketplace where digital data is exchanged as ‘products’ or ‘services’ as a result of the elaboration of raw data” (European Commission, 2020a). This tool includes an international comparison of the value of the European Union data market (including the United Kingdom) with those of the United States, Japan and Brazil, as shown in figure I.10. The value of data markets has increased significantly in the last five years, in all the economies analysed; however, in Brazil, the value of the data markets remains relatively low over the period. The dominant position of the United States is evident from this analysis.¹⁵

Figure I.10. Data market value, selected economies, 2016–2020
(Millions of euros)



Source: UNCTAD calculations, based on European Commission (2020a).

F. MEASURING CROSS-BORDER DATA FLOWS

Measuring cross-border data flows is even more difficult. Indeed, there is currently no practical way to measure them. They are mainly assessed through proxies, but with little success, as they are far from providing useful indications and evidence for policymaking and development purposes.¹⁶

¹⁵ Statistics offices in various countries are working to improve the estimations of the value of data. See, for instance, Statistics Canada (2019).

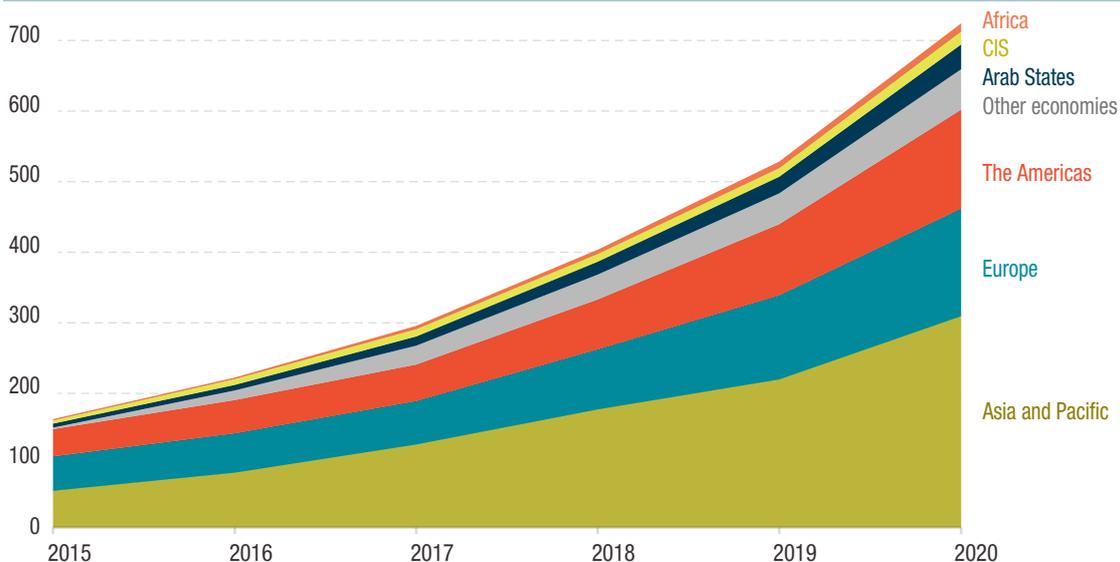
¹⁶ Further discussions on the difficulties of measuring cross-border data flows and the importance of improving their measurement can be found in National Telecommunications and Information Administration (2016); Coyle and Nguyen (2019); and Cory (2020).

In terms of volume, the main measure used is international bandwidth. According to ITU, “international Internet bandwidth refers to the total used capacity of international Internet bandwidth, in megabits per second (Mbit/s). Used international Internet bandwidth refers to the average traffic load of international fibre-optic cables and radio links for carrying Internet traffic. The average is calculated over the 12 month period of the reference year, and takes into consideration traffic of all international Internet links... The combined average traffic load of different international Internet links can be reported as the sum of the average traffic loads of the individual links”.¹⁷

Data on international bandwidth are provided by ITU and TeleGeography. ITU provides statistics on international bandwidth capacity and usage by country. World total international bandwidth use accelerated in 2020. Most international bandwidth was concentrated in the regions of Asia and the Pacific, Europe and the Americas, while the share of Africa remained very small (figure I.11).

Openly available data from TeleGeography, shown in figure I.12, illustrate the growth in international bandwidth and a forecast for 2024. Most interregional bandwidth is between North America and Europe, and between North America and Asia. Among developing countries, the North–South connection between North America and Latin America registers the highest interregional bandwidth. This information, however, only refers to the amount of data that flow in terms of bytes, without indicating in which direction they flow. It does not distinguish between data inflows and outflows from any particular region/country. Moreover, these bytes refer to both raw data and data products.¹⁸

Figure I.11. International bandwidth, by region, 2015–2020
(Terabits per second)



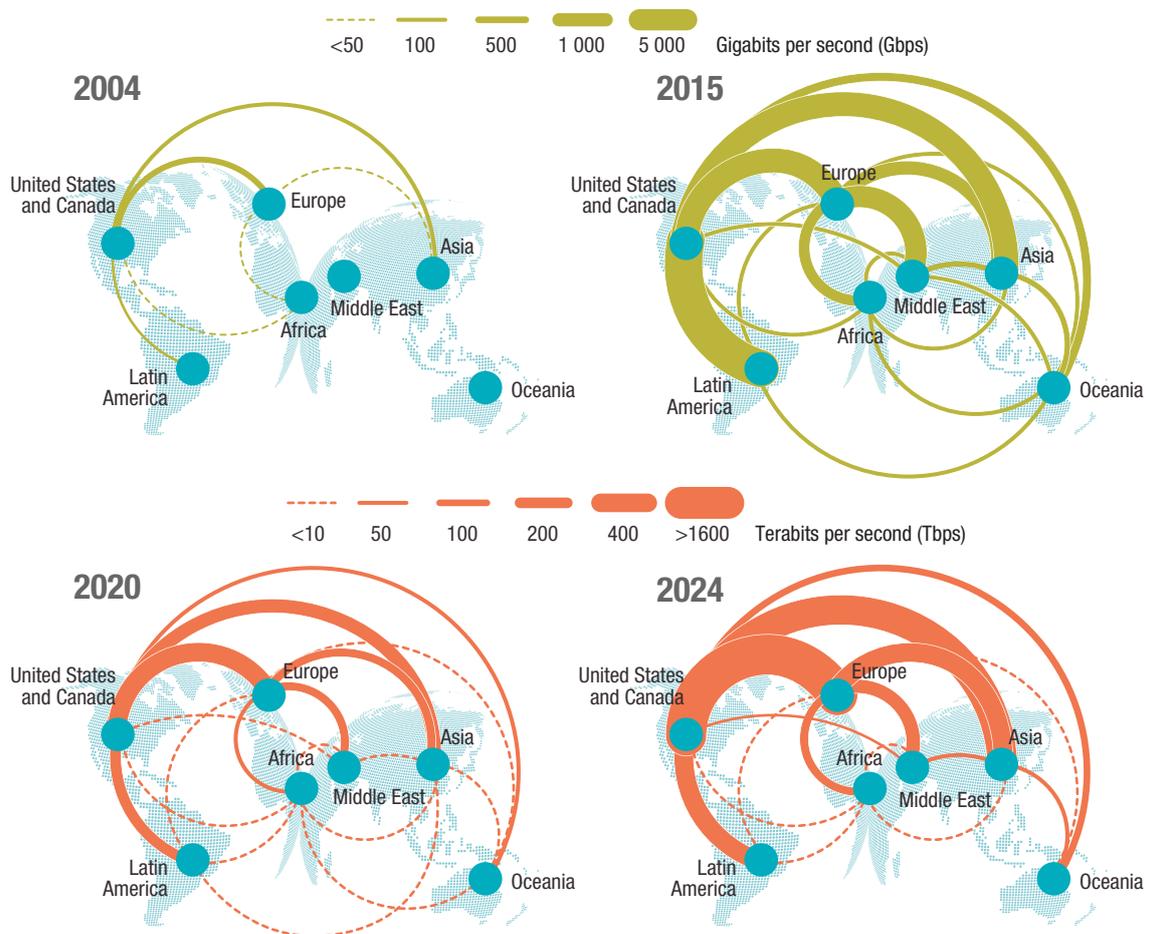
Source: UNCTAD calculations, based on ITU (2020) and ITU interactive report Measuring digital development, Facts and figures 2020, available at www.itu.int/en/ITU-D/Statistics/Pages/ff2020interactive.aspx.

Note: Country groups are those of the source. Data for 2020 are ITU estimates.

¹⁷ If the traffic is asymmetric, i.e. if there is more incoming (downlink) than outgoing (uplink) traffic, the average incoming (downlink) traffic load is used. See the ICT Development Index (IDI): conceptual framework and methodology, available at www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx.

¹⁸ This refers to information that is openly available. TeleGeography is the largest source of data and analysis on long-haul networks and the undersea cable market. Underlying data on capacity, ownership, wholesale (non-discounted) prices and other metrics are available for subscription. Thus, it could be the case that more detailed statistics exist, but they are proprietary. TeleGeography is also the source that is used by McKinsey Global Institute publications; it presents analyses with regard to cross-border data flows (which are very often quoted as an authoritative reference in the matter, but would deserve close scrutiny).

Figure I.12. Evolution of interregional international bandwidth, selected years



Source: UNCTAD, based on TeleGeography (2015, 2019, 2021b).
 Note: One Terabyte is equal to 1,000 Gigabytes. Data for 2024 are forecasts.

A Nikkei survey using ITU and TeleGeography statistics showed that, in 2019, cross-border data flows of China – including Hong Kong, China – far outstripped any of the other 10 countries/territories and regions examined, including the United States. China accounted for 23 per cent of global cross-border data flows, while the United States ranked second at 12 per cent. The source of the leadership of China lies in its connections with the rest of Asia. While the United States accounted for 45 per cent of data flows in and out of China in 2001, that figure dropped to just 25 per cent in 2019. Asian countries now make up more than half the total, particularly Viet Nam at 17 per cent, and Singapore at 15 per cent.¹⁹

While ITU and TeleGeography statistics provide interesting information and indications on the evolution of cross-border data flows, volume is not the most important aspect. It is also necessary to look at the nature and quality of the data. It is likely that a significant proportion of the data collected are of no use for economic purposes, even if they generate revenues for a few companies. Indeed, IBM estimates that 90 per cent of data generated by sensors and analog-to-digital conversions are not used. Moreover, according to Sandvine (2020), about 80 per cent of all Internet traffic is related to videos, social networking and gaming.

¹⁹ See *Nikkei*, 24 November 2020, China rises as world's data superpower as internet fractures, available at <https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures>. The methodology used in this survey is far from clear; thus, it is not an easy task to find out how the survey was done and where the statistics come from, when discussing Chinese data inflows and outflows.

From the economic perspective, it would also be relevant to have measurements on the value of cross-border data flows. In 2016, the National Telecommunications and Information Administration of the United States produced a report exploring these measures, and provided some recommendations (box I.2). In relation to the second recommendation, on the need for standard definitions, it is noteworthy that the report itself, whose purpose is to discuss the situation with regard to measurement of cross-border data flows, fails to shine any light on what cross-border data flows actually are.

Five years have passed since the publication of this report which, in the context of rapidly evolving data-driven technological development, is a very long period. However, while the data-driven digital economy has changed significantly during this time, there has been little progress in the measurement of data flows. In order for policymakers to properly take evidence-based decisions to regulate such flows, there is a need for more official statistics on data-related issues, since relevant statistics in this area are mostly provided by firms such as TeleGeography, Cisco or International Data Corporation.

In particular, for development purposes, it would be important to be able to distinguish between raw data and data products. In the conventional economy, regarding the relationship between international trade and development, the analysis focuses on the structure of imports and exports in terms of their level of skills and technology content. Increasing skills and technology content of exports against imports would be an indication of domestic value addition and, therefore, of development. Similarly, in the case of cross-border data flows, in the context of the data value chain from raw data collection to the production of digital intelligence (data products), which implies value addition, it would be important to look at the structure of data inflows and outflows in terms of whether they are raw data or data products. Currently, there are indications that most developing countries' data outflows are in the form of raw data, while their data inflows consist more of digital intelligence produced in those countries that enjoy the main data advantages and have better capacities to process raw data (see also chapter III). Thus, it would be important to find measures that allow for a distinction between outflows and inflows of data, as well as between raw data and data products.²⁰

Box I.2. Recommendations of the United States National Telecommunications and Information Administration report on “Measuring the Value of Cross-Border Data Flows”

Recommendations include:

- Improve the overall coverage and quality of Government statistics on the services sector.
- Develop a standard nomenclature or standard definitions for concepts related to cross-border data flows, distinguishing between concepts such as digital economy, digitally-intensive, digitally-enabled economy and ICT.
- Develop a greater understanding of how firms use cross-border data flows and what economic value the data flows provide. These metrics should cover the entire United States economy, as well as specific sectors.
- Develop improved and consistent macroeconomic statistics to measure the value of cross-border data flows and the digital economy, such as the contribution of data flows and the digital economy to GDP. These metrics should cover the entire United States economy, as well as specific sectors.
- Continue the dialogue between the Department of Commerce and private industry to facilitate data-sharing and the linking of public and private data sets, where legally and logistically feasible and consistent with strong privacy protections for firms.
- Continue the collaborative efforts of the Department of Commerce and international organizations, to ensure that metrics on cross-border data flows and the digital economy are widely available for countries around the world.

Source: National Telecommunications and Information Administration (2016).

²⁰ See also chapter II for a review of the literature on data measurement issues.

G. DATA COLLECTION

Data can be collected by different actors and in various ways (see chapter III). As will be shown in this and subsequent sections, global digital platforms are playing an increasingly important role in all stages of the data value chain. This section discusses their role as major collectors of data globally. It then looks at IoT developments, as the increase in Internet-enabled devices and machine-to-machine connections are expected to significantly boost data generation and flows.

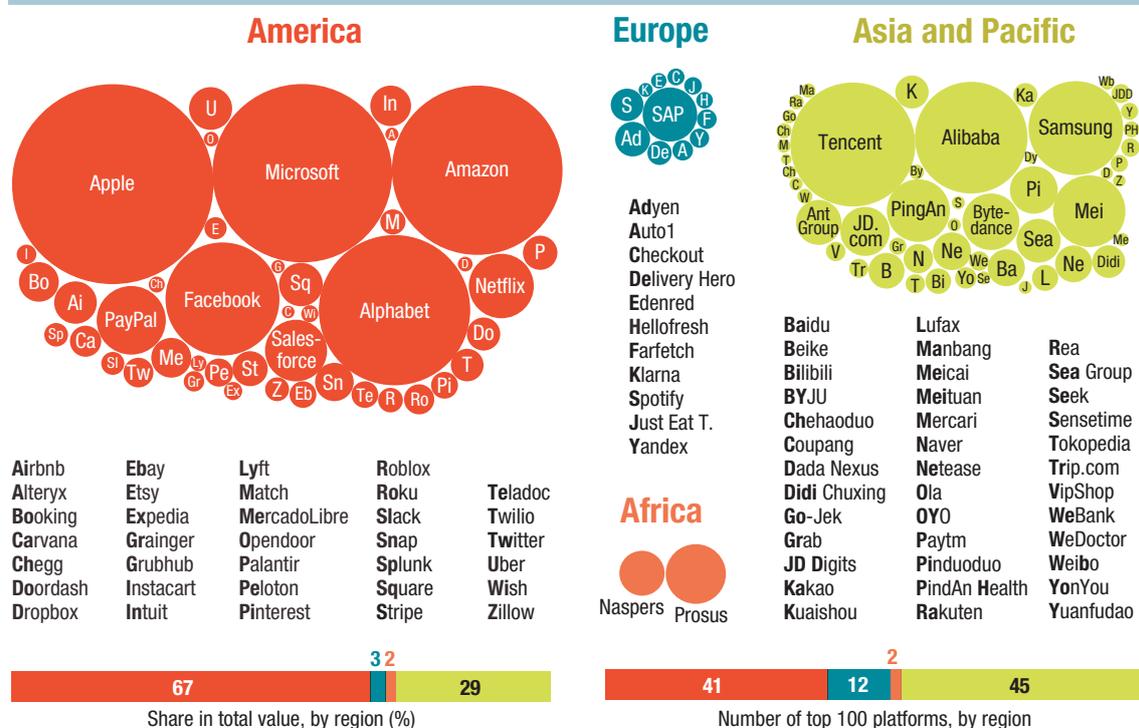
1. Digital platforms

Global digital platforms are in a privileged position to collect data at a massive scale when their many users access their services. This gives them a significant competitive advantage. In the absence of a proper international system of global data governance, this advantage in data collection directly translates in these platforms being able to capture most of the monetary gains of the data-driven digital economy and thereby also of cross-border data flows.

Network effects, combined with access to data and economies of scale and scope, have led to monopolistic trends and increased market power of the world's largest digital platforms, which are mainly based in the United States and China. The platforms reinforced their positions through strategic acquisitions of other companies by expanding their reach into new sectors, and by engaging in lobbying of policymakers (UNCTAD, 2019a, 2019b). Their position was further enhanced in 2020 during the pandemic. The worldwide distribution of global digital platforms as of 2021 is shown in figure I.13.

This section analyses the impact of the pandemic on these platforms. It then looks at lobbying trends, as some platforms aim to influence policymaking in their interests. Moreover, considering that a large part of data is used in feeding AI algorithms, and that the evolution of AI has significant consequences for the future of the global digital economy, the last part of this section looks at AI investment by leading global digital platforms.

Figure I.13. Geographical distribution of the top 100 global digital platforms, by market capitalization 2021



Source: Holger Schmidt, available at www.netzoekonom.de/vortraege/#tab-id-1 (data as of May 2021).
 Note: As a reference, the market capitalization of Apple is \$2.22 trillion, while for Mercado Libre it is \$88.7 billion, \$80.2 billion for Baidu and \$59.7 billion for Spotify.

a. Impact of the pandemic on global digital platforms

Leading digital platforms have registered significant increases in their profits and the value of their market capitalization following the pandemic. This is not surprising, since most of the digital solutions that have been used to cope with various lockdown and travel restrictions have been provided by a small number of very large firms. For example, Amazon has seen a significant push to its online retail business thanks to increasing e-commerce. Amazon has also seen a huge increase in its cloud business operations, due to increased Internet demand and traffic. This is also the case for Microsoft. Moreover, Apple has seen demand for its devices surge, as people have increasingly moved to perform their activities online.

In what follows, the recent evolution of digital advertising, profits, stock market prices and market capitalization of these companies in recent years, with particular emphasis on the impact of the pandemic, is analysed.

i. Digital advertising

One of the main ways in which some digital platforms monetize their data is through digital advertising. Global digital platforms have continued consolidating their dominant position in this market. By 2022, digital advertising spending is expected to reach 60 per cent of total media advertising spending, which is about double the share of 2013 (figure I.14a). By then, the share of top five digital platforms in terms of total digital advertising spending is expected to exceed 70 per cent (figure I.14b).

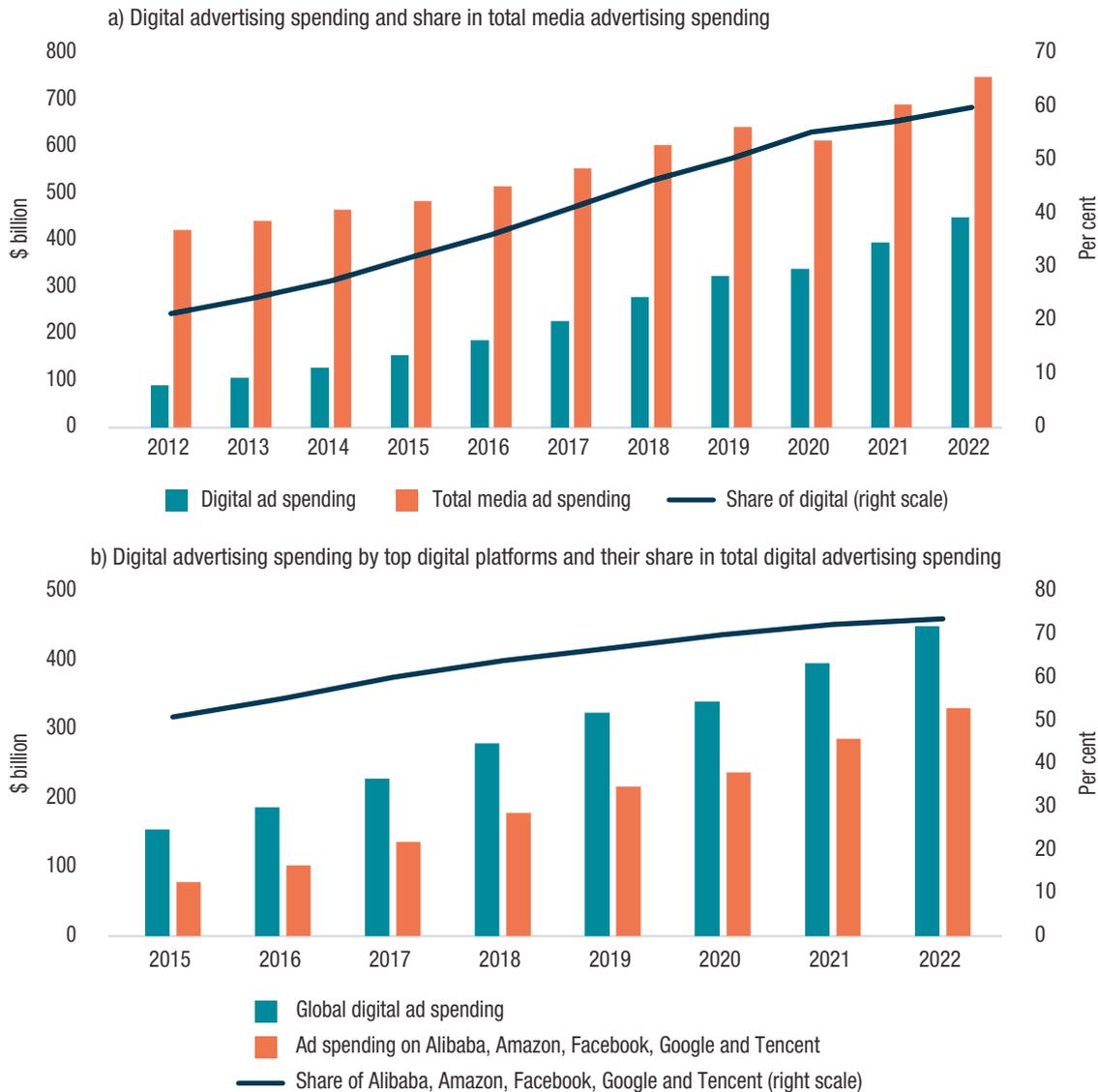
ii. Profits

Profits of leading digital platforms have experienced a rising trend since 2017, including in 2020 amid the economic crisis resulting from the pandemic (figure I.15a). Net income of the leading digital platforms in the United States reached \$192.4 billion in 2020, an increase of 21.1 per cent compared with the year before.

An analysis of quarterly profits from the second half of 2019 to the first quarter of 2021 provides additional insight into the impact of the pandemic on these companies (figure I.15b). The third quarter (Q3) and the fourth quarter (Q4) of 2019 show a pre-crisis situation with a comfortable level and growth of net incomes. In Q1 2020, these companies experienced a fall in profits, as compared with Q4 2019, as the pandemic crisis meaningfully hit the world by February and March 2020. Even if it was a dramatic fall of net income, these companies were still profitable in Q1 2020. After the initial shock, the pandemic caused an increased demand for cloud services, online shopping, videos and gaming, social networks and videoconferencing. This resulted in a positive growth of net income for these companies in Q2 2020 and, in particular, Amazon's net income more than doubled as compared with Q1 2020. In Q3 and Q4 2020, these leading digital platforms from the United States seemed to have returned to their business-as-usual path, and even beyond. Indeed, when compared with the same period of the preceding year, the combined net income of Amazon, Alphabet (including Google), Apple, Facebook and Microsoft rose by 31 per cent in Q3 2020 and 41 per cent in Q4 2020. Although the aggregated profit decreased slightly between Q4 2020 and Q1 2021, the latter more than doubled as compared with Q1 2020. These trends show that these companies have not only been resilient to the crisis, but that their business models and dominance, combined with the strong demand for digital services, have propelled them to a higher income growth path amid the worldwide economic crisis.

Leading digital platforms from China – namely Alibaba, Baidu and Tencent – also benefited, experiencing altogether a net income increase of 37 per cent, from almost \$20 billion in 2017 to \$27 billion in 2019 (figure I.16a). The increase in profits was even more remarkable in 2020, as the cumulative net income was approximately \$48 billion, a rise of 78 per cent as compared with 2019. When analysing the impact of the pandemic, which started earlier in China than in the United States, i.e. by the end of 2019, only Alibaba seems to have been affected in Q4 2019 (figure I.16b). While in Q1 2020 the profits of these companies sharply decreased (mainly because of Alibaba's lower profits), Tencent emerged as a winner, with higher profits than in the previous two quarters. In Q2 and Q3 2020, the quarterly net income increased, especially for Alibaba, making the cumulative profits of these Chinese companies in Q3 2020 similar to the level seen in Q3 2019. The explosion of the cumulative net income in 2020 is attributed to the very significant profits made by Alibaba and Tencent in Q4 2020.

Figure I.14. Digital advertising spending, 2012–2022



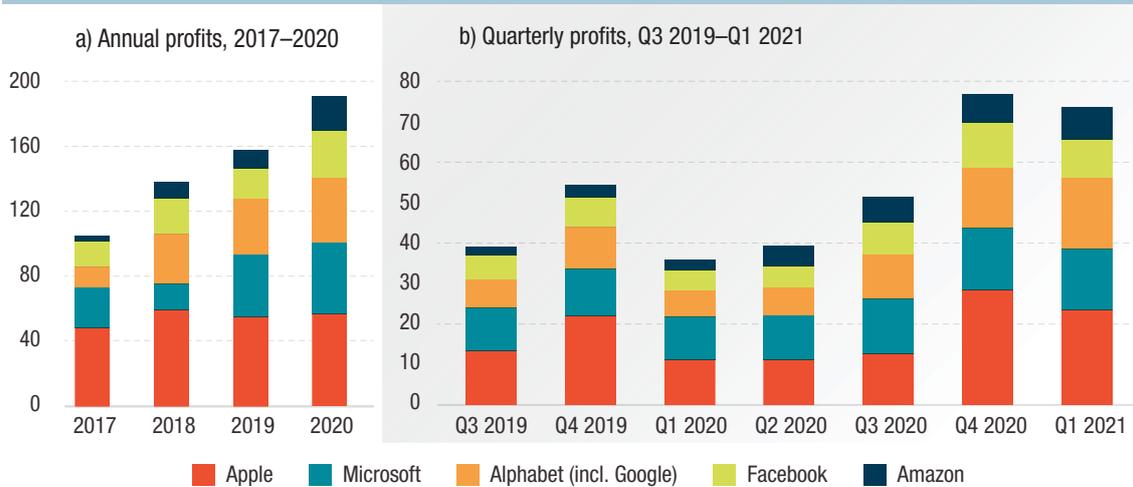
Source: UNCTAD, based on data from eMarketer, Global Digital Ad Spending Update Q2 2020, available at www.emarketer.com/content/global-digital-ad-spending-update-q2-2020.
 Note: 2020 to 2022 are estimates.

iii. Stock market prices and market capitalization

Increases in profits of leading global digital platforms have not escaped the attention of investors, as reflected in increasing stock prices. Figure I.17 compares the stock price growth of these companies from Q4 2019 to January 2021 with the evolution of the New York Stock Exchange (NYSE) Composite Index, a representative indicator of the economy's health in the United States.

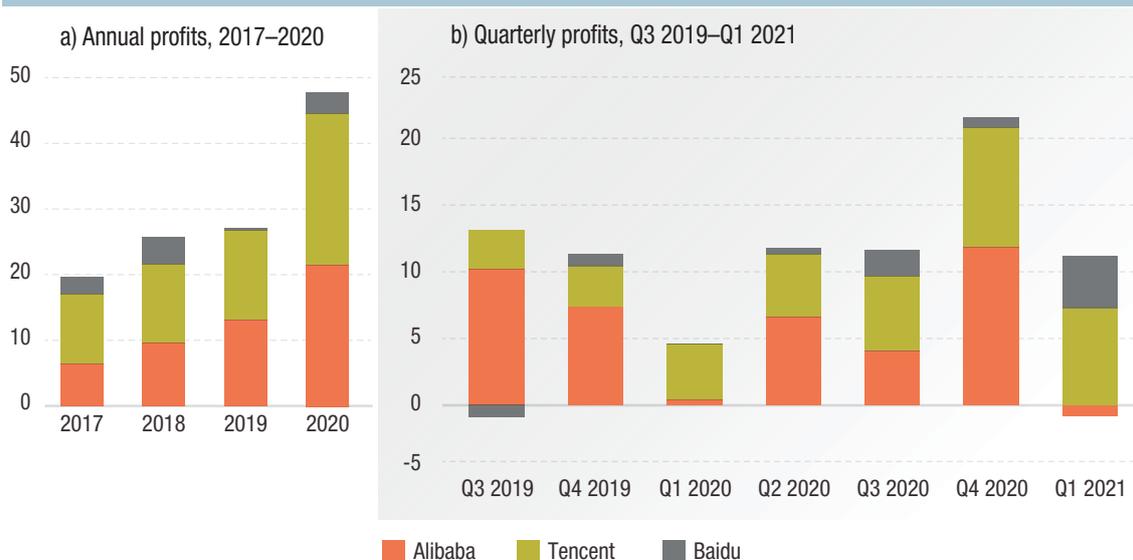
Stock prices of global digital platforms from the United States and China, as well as the NYSE Composite Index, all experienced significant falls or, at best, lower positive growth from the end of February to late March 2020, as compared with their levels on 1 October 2019. This was the result of the initial shock from the global sanitary and financial crisis. This growth hit its lowest point for Amazon on 12 March 2020 (-3.4 per cent); Facebook, Microsoft and Tencent on 16 March 2020 (-17.0 per cent, -1.2 per cent and +1.4 per cent, respectively); Baidu on 18 March 2020 (-18.0 per cent); Alphabet (including Google), Apple and Alibaba on 23 March 2020 (-12.6 per cent, -0.1 per cent and +6.8 per cent respectively); while the NYSE Composite Index hit its highest negative growth on 23 March 2020 (-31.6 per cent).

Figure I.15. Profits by major digital platforms in the United States
(Billions of dollars)



Source: UNCTAD calculations, based on the Wall Street Journal, available at www.wsj.com/market-data/quotes/company-list/ (accessed May 2021).

Figure I.16. Profits by major digital platforms in China
(Billions of dollars)

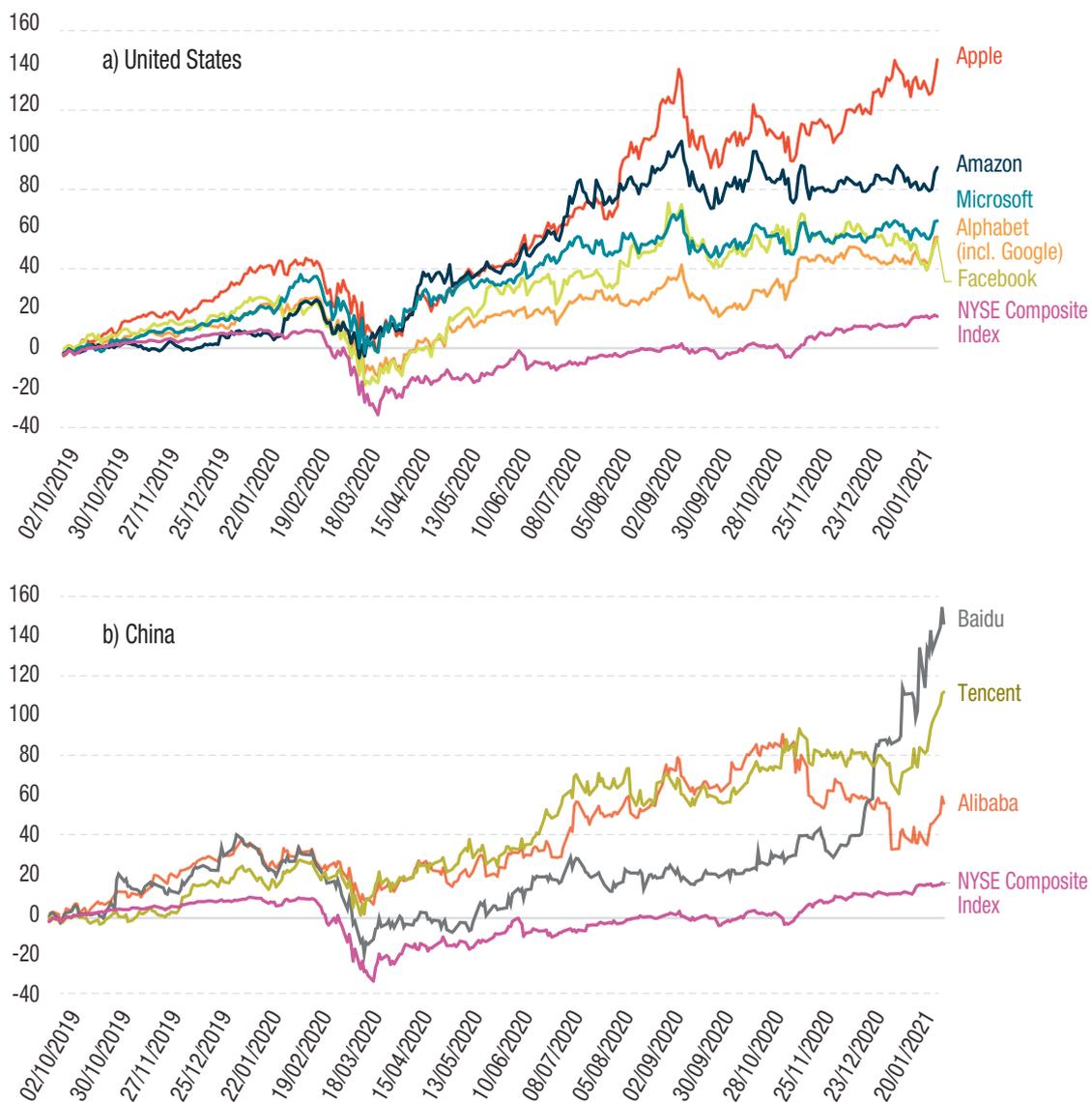


Source: UNCTAD calculations, based on the Wall Street Journal, available at www.wsj.com/market-data/quotes/company-list/ (accessed May 2021).

However, since mid- and late March 2020, the stock prices of these companies, as well as of those represented by the NYSE Composite Index, started to recover. This recovery was on average lower for the NYSE Composite Index than for the global digital platforms. Between 1 October 2019 and 21 January 2021, the NYSE Composite Index increased by 17.0 per cent. In the same period, the growth rates of stock prices for the selected companies were at least three times larger: Facebook (55 per cent), Alphabet (including Google) (56 per cent), Alibaba (57 per cent), Microsoft (64 per cent), Amazon (90 per cent), Tencent (113 per cent), Apple (144 per cent) and Baidu (147 per cent).

Overall, the NYSE Composite Index recovery in the context of a deep economic crisis points to some disconnection between financial markets and the real economy. Most significantly, the remarkable increases in stock prices of leading digital platforms show an even greater disconnection between the digital economy and the “real” economy.

Figure I.17. Stock prices of global digital platforms from the United States and China versus the New York Stock Exchange Composite Index
(Change in per cent)

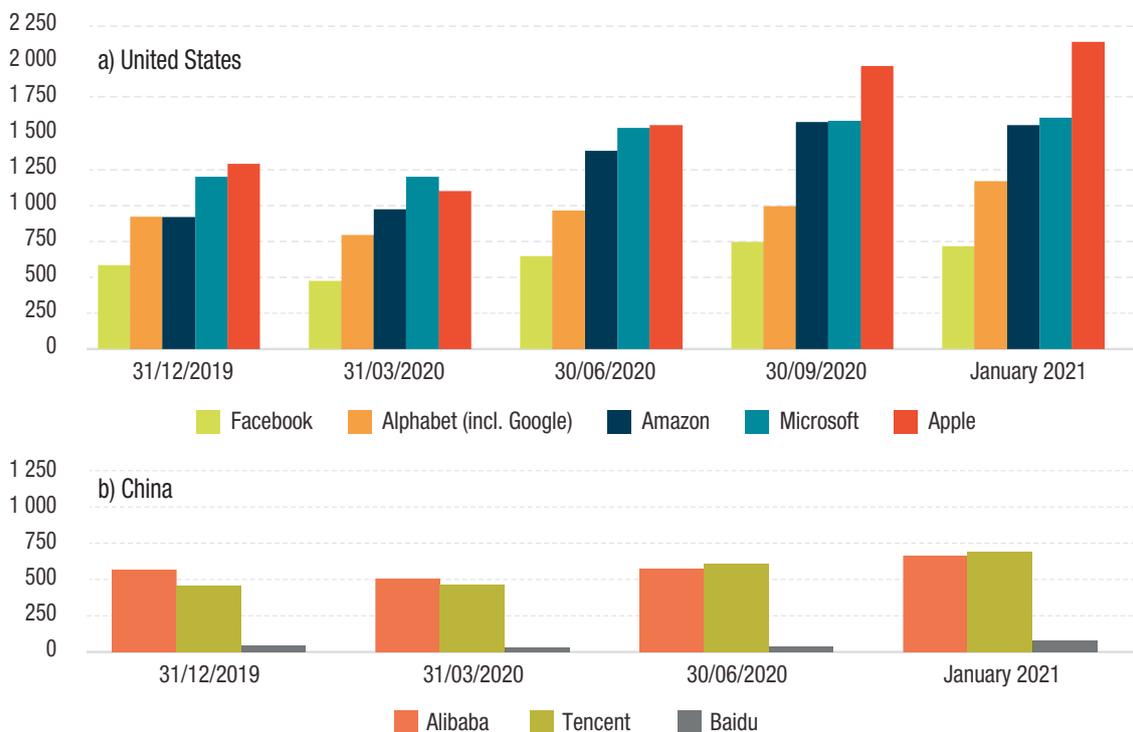


Source: UNCTAD calculations, based on Yahoo! Finance, available at <https://finance.yahoo.com> (accessed January 2021).

Note: The figures show the change in stock prices between each date and 1 October 2019.

Large increases in their stock exchange prices through 2020 translated into considerable changes in the market capitalization of leading global digital platforms (figure I.18). Concerning the American companies, by the end of 2019, the market capitalizations of Microsoft and Apple were already more than \$1 trillion each, Alphabet (including Google) and Amazon approached that mark, and Facebook was valued at more than \$0.6 trillion. Through 2020, the market capitalization of these companies showed significant increases: 22 per cent for Facebook, 27 per cent for Alphabet (including Google), 34 per cent for Microsoft, 66 per cent for Apple and 70 per cent for Amazon. As a consequence, after a year that saw many bankruptcies and heavy national State subsidies for saving industries around the globe, Facebook's market value was \$716 billion in January 2021, Alphabet's was \$1.17 trillion, Amazon's \$1.56 trillion and Microsoft's \$1.61 trillion. Apple outpaced the rest and reached a value of over \$2 trillion, becoming the first company in the United States to pass that mark.

Figure I.18. Market capitalization of global digital platforms from the United States and China, Q4 2019–January 2021
(Billions of dollars)



Source: UNCTAD calculations, based on Yahoo! Finance, available at <https://finance.yahoo.com> (accessed January 2021).

The three digital giants from China had lower market capitalization by the end of 2019 as compared with those in the United States. Baidu, with the lowest market value among them by the end of 2019, saw an increase of 86.4 per cent in 2020, to reach \$81.5 billion in January 2021. Alibaba, which had the highest market capitalization by the end of 2019 (\$571 billion), experienced a growth of 17.8 per cent, to \$672.8 billion. Tencent's market capitalization had the largest absolute increase in 2020 (51.9 per cent), and reached \$699.8 billion, thus exceeding that of Alibaba.

b. Influencing policymaking

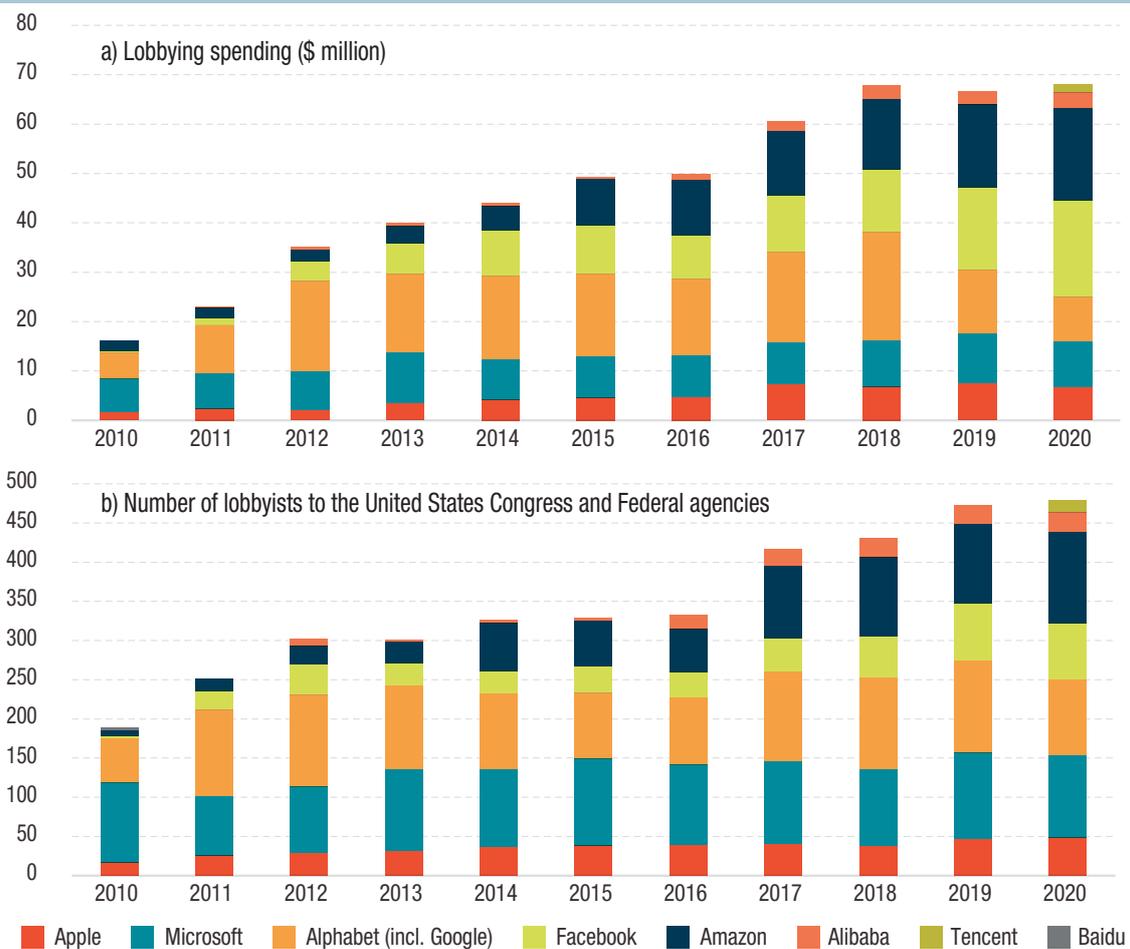
Some leading digital platforms aim to influence regulations through their lobbying efforts.

i. Lobbying in the United States

The digital platforms are highly active dealing with the United States Congress, spending large amounts of money for lobbying and hiring people with political connections. In 2020, Facebook and Amazon ended up among the top 10 lobbying spenders, bested only by the massive trade associations (Center for Responsive Politics, 2021). The United States digital platforms (Alphabet (including Google), Amazon, Apple, Facebook and Microsoft) increased their spending from \$16 million in 2010 to over \$63 million in 2020 (figure I.19a). Alibaba has been an active lobbyist to the United States Congress, but to a lower extent than the United States companies in terms of spending.²¹ Google and Microsoft were the largest lobbying spenders in the early 2010s, while Amazon, Apple and Facebook were at significantly lower levels. However, Facebook and Amazon increased their lobbying spending the most in the period 2010–2020. Facebook spending rose from \$0.35 million in 2010 to almost \$20 million, the highest level of the five companies. Not surprisingly, increased spending was also reflected in hiring more people to engage in lobbying (figure I.19b).

²¹ Tencent only lobbied in 2020, while Baidu had no registered lobbying spending in the last decade.

Figure I.19. Lobbying by global digital platforms in the United States, 2010–2020



Source: UNCTAD calculations, based on “Lobbying Data Summary”, Center for Responsive Politics, available at <https://www.opensecrets.org/federal-lobbying>.

ii. Lobbying in the European Union

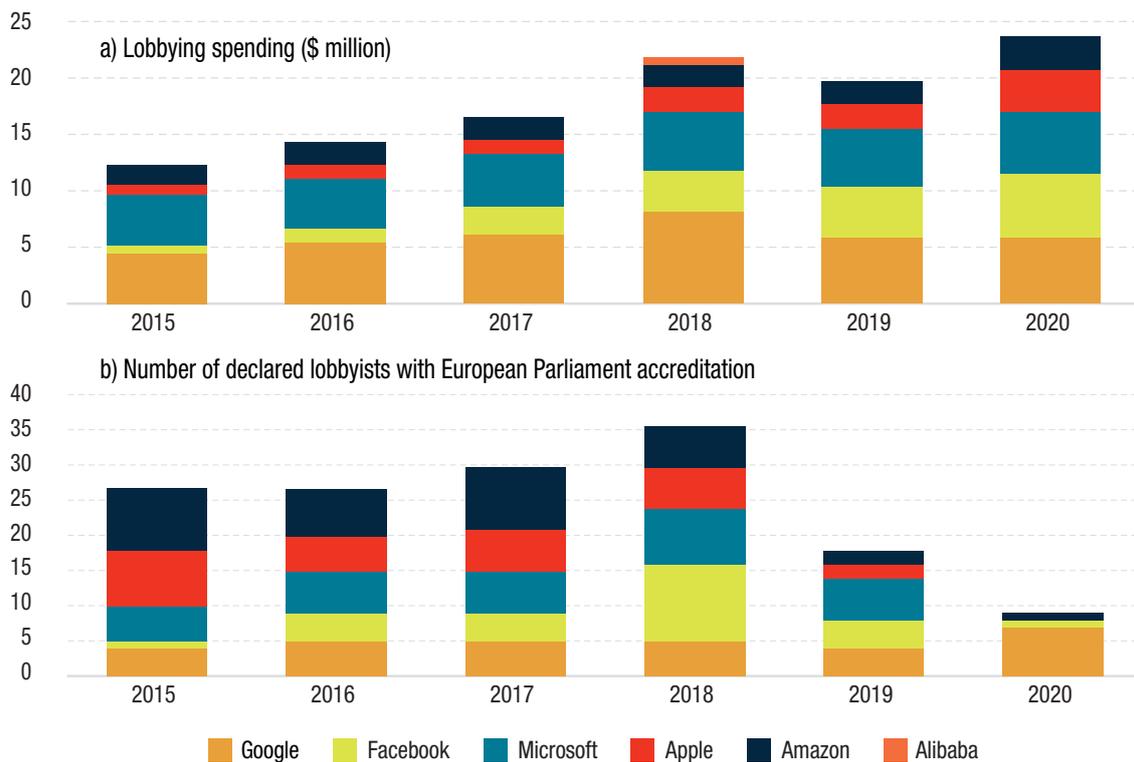
Global digital platforms from the United States are also actively lobbying in the European Union. Although their spending is lower in Brussels than in Washington, D.C., Google, Facebook (FB Ireland Limited) and Microsoft were occupying, in the same order, the top three positions on the list of companies and groups lobbying spenders in the European Union as of 15 April 2021; Apple and Amazon (Amazon Europe Core SARL) were within the top 20 and top 30, respectively, of the same category in Europe.²²

These United States companies altogether spent more than \$12 million in 2015 on lobbying activities in the European Union, and almost doubled these expenses in 2020, to reach \$24 million (figure I.20a). Among the Chinese digital platforms, spending on lobbying was registered only for Alibaba in 2018, at an amount below the levels of the United States companies. The number of hired lobbyists by the digital platforms in the European Union was significantly lower than in the United States (figure I.20b). However, their influence in the European Union also seems to be made in parallel by funding some think tanks – “organizations that can influence new regulations by publishing studies and position papers and organizing discussion forums – but these ties are often not at all clear”.²³ The increase in lobbying

²² See LobbyFacts database, available at <https://lobbyfacts.eu/reports/lobby-costs/all/0/2/2/21/0/2021-04-15>.

²³ See Corporate Europe Observatory, Big Tech Lobbying: Google, Amazon & friends and their hidden influence, available at <https://corporateeurope.org/en/2020/09/big-tech-lobbying>.

Figure I.20. Lobbying by global digital platforms in the European Union, 2015–2020



Source: UNCTAD, based on LobbyFacts database, available at <https://lobbyfacts.eu/about-lobbyfacts>.
Note: This database did not include data for Baidu and Tencent.

activities by global digital platforms in the European Union is an evident sign of their rising power, but also of their attempts to get ready for the key upcoming tech-related policies in the European Union that could shape the industry's future.

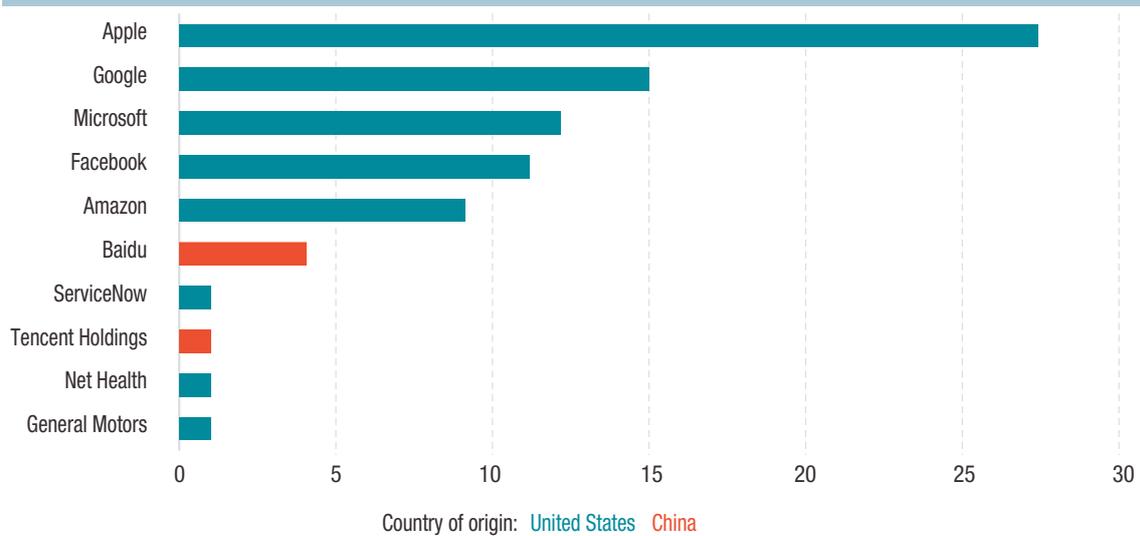
c. Investment in AI start-ups and AI-related research and development by leading digital platforms

Another way in which digital platforms are increasing their market power in the data value chain is by acquiring start-ups and investing in horizontal and vertical expansion (UNCTAD, 2019a). Digital platforms that handle massive data are also the ones having increasingly invested in artificial intelligence (AI), which in turn helps them to effectively use data, improve the user experience and attract new users (and data). Therefore, these companies, and countries where they are based, are in a better position regarding AI leadership, as well as in the management of global data, a crucial component of today's digital economy and future growth in all industries. The situation regarding AI developments at country level is discussed further below.

Regarding mergers and acquisitions (M&A) of start-ups active in the AI segment, during the period of 1 January 2016–22 January 2021, there were 308 M&A deals worth \$28.4 billion. As shown in figure I.21, the top five companies in the world, by number of acquired AI start-ups in the same period, were the Big Tech companies from the United States, followed by Baidu (sixth) and Tencent (eighth) from China. Apple led this ranking, followed by Google and Microsoft. As for now, it seems that the competition in AI is purely based on future expected profits and global leadership.

As major digital platforms enjoy the data advantage, they are also increasingly investing in AI-related research and development, which is deemed key to reaping future benefits from processing and analysing data. AI research takes place mainly in universities, research institutions and private companies. The private tech firms constantly increased their participation in major AI conferences in the

Figure I.21 Number of acquisitions of AI start-ups, top ten acquirers, 2016–2021



Source: UNCTAD, based on CBInsights, available at www.cbinsights.com (accessed 22 January 2021).

period 2000–2019 (Zhang et al., 2021) and for the most prestigious ones, they even dominate in the number of submitted papers. As shown in figure I.22, Google is by far the leading institution among the top-tier AI research institutions, while Microsoft and Facebook also feature among the top 10.

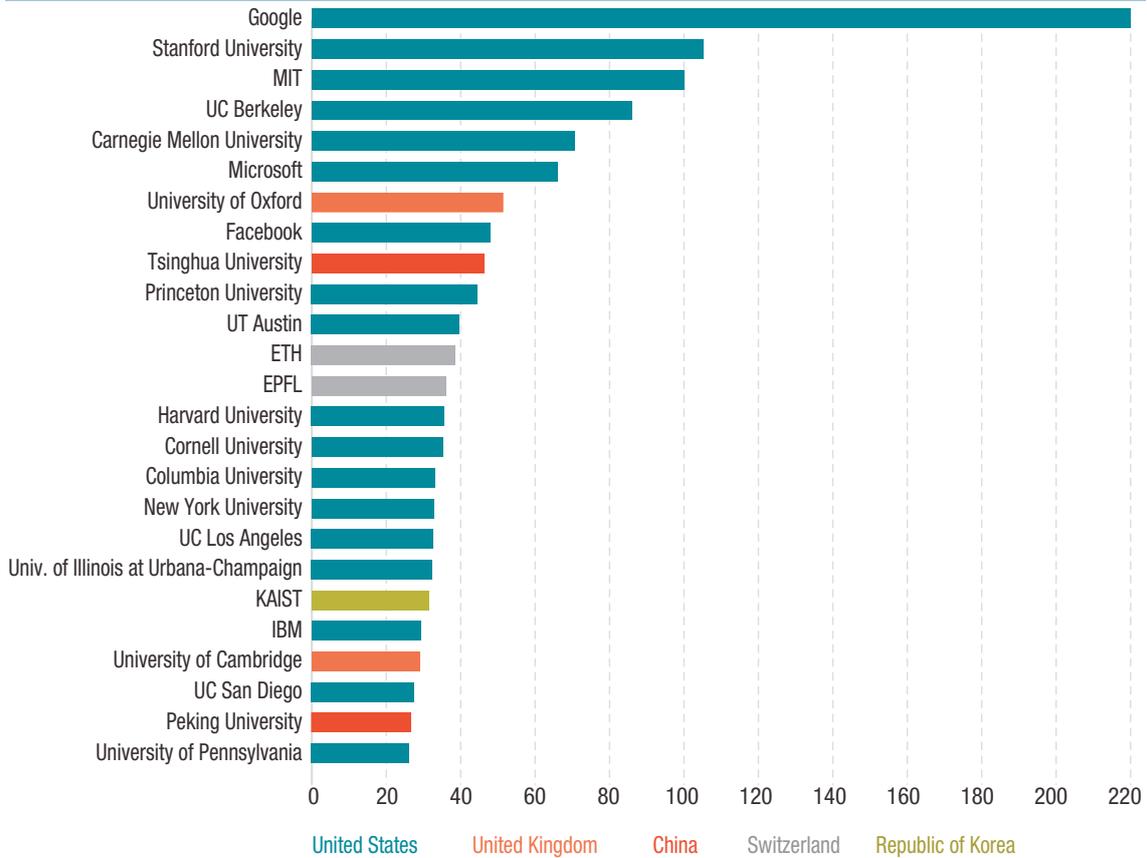
In this context, platforms in the United States and China benefit from particularly good access to talent and skills needed for the harnessing of data and AI. Most AI researchers, 59 per cent, work in the United States, while China hosts another 11 per cent, leaving the remaining 30 per cent for the rest of the world (figure I.23). In terms of the origins of researchers, China accounts for 29 per cent and the United States for 20 per cent. India and the Islamic Republic of Iran also represent important sources of such talent.

About two thirds of all students with master’s and PhD degrees in AI in the United States were foreign students in 2016–2017. Among the international PhD students who graduated in the period 2014–2018 and started to work, almost 90 per cent stayed in the United States (Zwetsloot et al., 2019). Very similar results were found by Zhang et al. (2021), who estimated for the year 2019 the share of foreign students among the new AI PhDs in United States to be 64.3 per cent, and that 81.8 per cent of foreign graduates stayed in United States.

A related issue is the professional choice of AI students after graduation. Regulators in the public sector tend to lag the leading private companies in terms of technical knowledge in AI, as they fail to attract the best talent. According to Zhang et al. (2021), the share of new AI PhDs who chose industry jobs increased from 44.4 per cent in 2010 to 65.7 per cent in 2019. By contrast, the share of new AI PhDs entering academia dropped from 42.1 per cent in 2010 to 23.7 per cent in 2019. For the remaining part of the new AI PhDs in 2019, 10.6 per cent, it may be assumed that they joined the public sector or non-profit organizations, or did something else. More detailed research on the same topic was carried out by Zwetsloot et al. (2019). They conducted a study in the United States of two groups of AI PhD postgraduates (domestic and international), and found that the United States postgraduates engaged mainly in jobs in the private and academic sectors, while only 8 per cent went to work for the Government or non-profit organizations (figure I.24). This trend was more accentuated for foreign students, as the vast majority started to work in the private sector (mainly in large companies), and only 4 per cent went to the public sector.

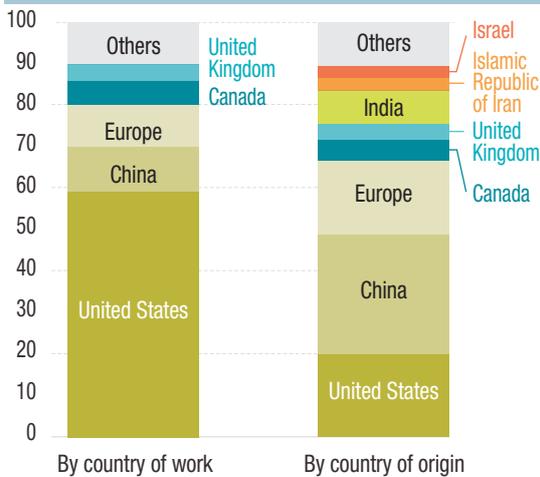
Professional career development also does not benefit the public sector. For those who graduated in 2014–2015 and switched sectors, of “the graduates who start in government or non-profit jobs, nearly 75 per cent leave for either industry or academia within four years. Around 20 per cent of the graduates who started off in academia moved to the private sector, and 10 per cent of those who started off in

Figure I.22. Top 25 institutions for top-tier AI research
(Number of papers published)



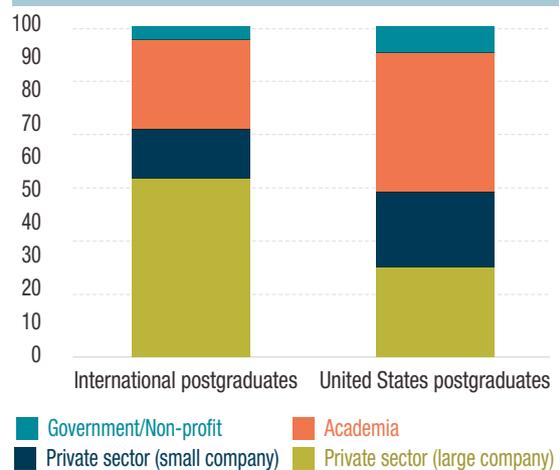
Source: UNCTAD, based on AI Research Rankings 2020: Can the United States Stay Ahead of China? Available at <https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b12116>.
Note: Data refer to papers accepted at the two most prestigious AI research conferences: International Conference on Machine Learning and Neural Information Processing Systems annual meeting 2020.

Figure I.23. Geographical distribution of AI researchers, by country of work and origin, 2019
(Per cent)



Source: UNCTAD, based on the Global AI Talent Tracker, available at <https://macropolo.org/digital-projects/the-global-ai-talent-tracker/>.

Figure I.24. First job among graduates with PhDs in AI staying in the United States, by sector, 2014–2018
(Per cent)



Source: UNCTAD, based on Zwetsloot et al. (2019).

private sector travelled the opposite path” (Zwetsloot et al., 2019:13). The AI researchers moving from academia to industry are another growing concern. This trend, driven by strong industry demand for AI researchers with advanced technical skills, may create a brain drain that shrinks the pool of talent available for public interest AI research (Jurowetzki et al., 2021). Ahmed and Wahed (2020) argue that the unequal distribution of computing power in academia, or the computer divide, is adding to inequality in the era of deep learning. Large technology companies have more resources to design AI products, but they also tend to be less diverse than less elite or smaller institutions. This raises concerns about bias and fairness within AI.

This imbalance – between the private sector on the one hand, and the public and academic sectors on the other – in attracting the best AI talent should be rapidly addressed (a similar gap, as in the United States, probably exists in other advanced economies and China). A failure on this matter will have long-term consequences. Public authorities with technically limited AI capacity will struggle, or even fail, to design and implement regulations in the fast-changing digital markets, driven increasingly by innovative developments in AI. As a consequence, global digital platforms and other private companies will continuously remain one step ahead of the regulators. Concerning the likely brain drain from academia, it will result in the AI research being biased towards these companies’ methods to reach commercial objectives, which are already creating concerns on issues such as the use of surveillance tools and their impact on people’s privacy. However, the imbalances with regard to attracting AI talent to the public sector are not the only ones that need to be addressed. There are other imbalances – for example, with regard to gender. Box I.3 looks at the role of women in AI research.

2. Internet of Things

The Internet of Things (IoT) is likely to be the main way to collect data in the near future, through the data generated by billions of connected electronic devices. Data can be collected through connected devices such as sensors, meters, radio frequency identification and other gadgets that may be embedded in

Box I.3. Women working in AI research

There is a very important gender gap in AI talent. This is seen within academia and corporate sectors, as well as among all countries actively involved in AI.

Concerning academia, among the PhD students in the AI field, there is strong male dominance. According to the Stanford University AI Index 2021 Report (Zhang et al., 2021), female graduates of AI and Computer Sciences PhD programmes in North America accounted for only 18.3 per cent of all PhD graduates in the period 2010–2019. Taking another proxy to estimate the gender gap, at one of the most prestigious annual AI conferences (Neural Information Processing Systems), between 2016 and 2019, the Women in Machine Learning workshop attendance was on average only about 10 per cent of the total.

Another study of the top 21 academic AI conferences in 2018 estimated that only 18 per cent of the conference authors were women, while this proportion was 19 per cent and 16 per cent in academia and industry, respectively, by employment sector of origin of the authors. As for the cross-country comparison, some economies are doing better than others, but the proportions are still a far way off from reaching anything close to gender balance. The list of top performers includes Spain (26 per cent), Taiwan Province of China (23 per cent) and Singapore (23 per cent). The three leading countries in absolute numbers of female researchers in AI have the following rates of female authors: United States (20 per cent), China (22 per cent) and United Kingdom (18 per cent) (Gagné et al., 2019). In 2020, based on a different methodology of counting, the ratio of female authors in AI publications was 15 per cent (Gagné et al., 2020).

At Google, the leader in AI publications in the two most prestigious AI conferences, female authors represented only 10 per cent of all researchers in AI (Chin, 2018). The issue of the gender gap in the development and deployment of AI technology is important because of the potential society-wide impact of machine learning, probably the most important one of all current technologies for the future of our societies.

Source: UNCTAD.

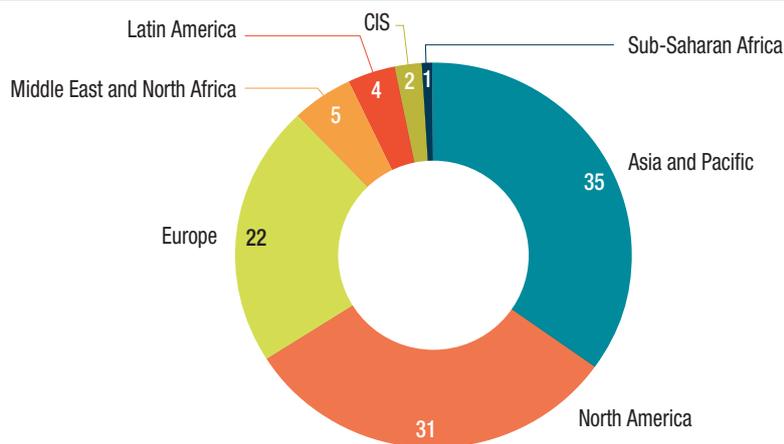
various Internet connected objects used in everyday life. With increasing digitalization of the global economy, the data value chain takes place in multiple countries, and accelerates due to decreasing costs and the easier use of more sophisticated technologies, including IoT (Nguyen and Paczos, 2020). Thus, the growing use of IoT will lead to an increase in cross-border data flows in the future without human intervention (Voss, 2020).

The key role of IoT in our lives has been highlighted during the COVID-19 pandemic. Some IoT applications that aided to fight it by providing critical data include connected thermal cameras, contact tracing devices and health-monitoring wearables. Moreover, temperature sensors and parcel tracking have helped ensure that sensitive COVID-19 vaccines are delivered safely. However, the increasing use of IoT has also raised concerns related to security, privacy, interoperability and equity (WEF, 2020a), that need to be addressed through proper governance.

The size of the global IoT market was \$308.97 billion in 2020. The market is projected to grow from \$381.30 billion in 2021 to \$1.85 trillion in 2028, which represents an annual growth rate of 25.4 per cent over 2021–2028 (Fortune Business Insights, 2021). According to the IDC (2020a) forecast for the period 2020–2024, worldwide spending on IoT has been negatively impacted by the pandemic, although a return to double-digit growth is expected in the mid-to-long-term, achieving an annual growth rate of 11.3 per cent over the forecast period. China, the United States and Western Europe will account for about three quarters of all IoT spending. Although the three regions will have similar spending totals initially, the spending by China will grow at a faster rate than the other two regions – 13.4 per cent annual growth rate, compared with 9.0 per cent and 11.4 per cent – making it the leading country in IoT spending. The fastest annual IoT spending growth will be in the Middle East and North Africa (19.0 per cent), Central and Eastern Europe (17.6 per cent), and Latin America (15.8 per cent).

In 2020, for the first time, there were more IoT connections (e.g. connected cars, smart home devices and connected industrial equipment) than there were non-IoT connections (smartphones, laptops, tablets and computers). By 2025, it is expected that there will be almost four IoT devices per person on average.²⁴ Estimations by GSMA (2019a) project that the total number of IoT connections is set to increase from 9.1 billion in 2018 to 25.2 billion in 2025. This will represent a \$1.1 trillion revenue opportunity by 2025. However, this revenue will be unevenly distributed by region, as shown in figure I.25. Sub-Saharan Africa, CIS and Latin America are expected to account for only 7 per cent of the total revenue opportunity.

Figure I.25. Geographical distribution of Internet of Things revenue by 2025
(Per cent)



Source: UNCTAD, based on GSMA (2019a).
Note: Country groups are those of the source.

²⁴ See *IoT Analytics*, 19 November 2020, State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time, available at <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/>.

It is estimated that the world economy benefited by \$175 billion in 2018 from the productivity benefits to businesses from the use of IoT; this is equivalent to 0.2 per cent of GDP. Over half of these benefits were enjoyed by manufacturing businesses, making it the sector currently gaining the most from using IoT. Productivity benefits from business use of IoT are expected to rise to \$3.7 trillion by 2025, representing 0.34 per cent of global GDP. The United States and China are leading the world in IoT productivity gains, accounting for over 50 per cent of global benefits (GSMA, 2019b).

In terms of sectors, by 2025, connected industry will represent more than half of the total revenue opportunity, followed by smart homes, which will represent 23 per cent of the total. Consumer electronics will account for 15 per cent, and connected vehicles and smart cities will represent 5 and 4 per cent of the total, respectively (GSMA, 2019a). Industrial IoT connections will lead overall growth of total IoT connections, at an annual average of 21 per cent between 2017 and 2025 (figure I.26). As a result of this significant growth, IoT connections for industry will account for over half of worldwide connections by 2025. This will imply a significant change in the way that industries work.

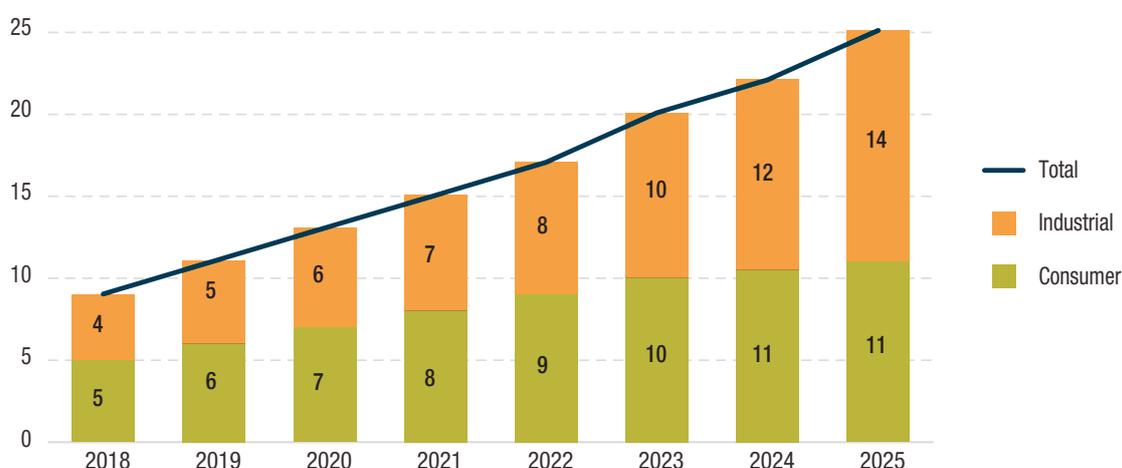
IDC (2020b) estimates that data generated from connected IoT devices will be 73.1 zettabytes by 2025, growing from 18.3 zettabytes in 2019. Most of these data will arise from security and video surveillance, but industrial IoT applications will also represent a significant share. This increase in overall data resulting from IoT will imply rising data flows across borders, as the different connected devices can be located all around the world. So far, analyses on the relationship between IoT developments and cross-border data flows are scarce, although there seems to be agreement that IoT will lead to a rise in those flows. In a study for Brazil, Indonesia and South Africa, GSMA (2021) estimates that emerging economies could reap major gains from deploying IoT. Under conditions of open cross-border data flows, they could have a considerable impact on economic output, in the form of increases in:

- GDP: up to 0.5 per cent in Brazil, up to 0.9 per cent in Indonesia, and up to 2.6 per cent in South Africa;
- Exports: up to 2.4 per cent in Brazil, up to 2.9 per cent in Indonesia, and up to 3.1 per cent in South Africa;
- Employment: up to 0.2 per cent in Brazil, up to 0.4 per cent in Indonesia, and up to 1.3 per cent in South Africa.

However, imposing restrictions on cross-border data flows would reduce the economic gains (measured in GDP) from IoT by 59 per cent for Brazil, 61 per cent for Indonesia and 68 per cent for South Africa.

Some leading global digital platforms – such as Alphabet (including Google), Amazon and Microsoft – are also major providers of IoT (UNCTAD, 2021d), which allows them to reinforce their data advantage. This, combined with the marginal share of Africa and Latin America in the expected revenues from IoT,

Figure I.26. Global number of IoT connections, by sector, 2018–2025



Source: GSMA (2019b).

points to IoT to contribute to the existing imbalances in a way similar to most other digital technologies. This will require policy interventions to address resulting inequalities, including an equitable distribution of the gains from the resulting cross-border data flows.

As IoT facilitates much higher collection and consumption of data, the use of these technologies poses increasing privacy and security concerns. As will be discussed in this Report, these considerations accumulate further in the case of cross-border data flows, as sensitive data can be transferred to a country where the jurisdiction may not apply the same standards of data protection as in the country where the data are collected. In exploring the governance landscape for IoT, WEF (2020a: 65–66): concludes that “the many risks inherent in IoT have not yet been effectively mitigated, and the state of IoT governance remains immature. At the same time, however, the effort to manage these risks can lead, in some cases, to inappropriate regulation, which in turn can threaten the value and effectiveness of many kinds of IoT applications. The issue of cross-border data exchange is a case in point... As important as it is to govern the use of many types of IoT applications, privacy and cybersecurity regulations remain fragmented across the globe.”

The development of IoT goes parallel to that of the deployment of 5G technologies, which is discussed in the next section.

H. DATA TRANSMISSION AND STORAGE

The fact that data are intangible does not mean that they are an ethereal entity. They need physical support and are transmitted through and stored in physical infrastructures. This section looks first at 5G as a key technological development for the last mile connection to the end user. Then it discusses the role of submarine cables and the potential of satellites for the long-distance connection (backbone) as major channels of data transmission. Finally, it highlights the importance of Internet exchange points (IXPs) for connecting networks and peering locally the Internet traffic, as well as of the cloud market and data centres for data storage. In many of these areas, the global digital platforms are also expanding their presence.

1. 5G mobile broadband

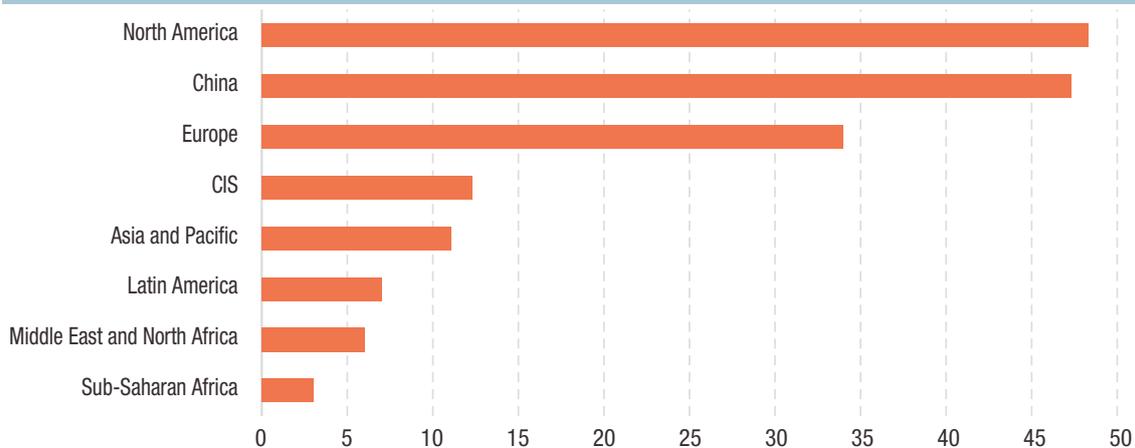
The development and deployment of 5G wireless technologies are key for the development of IoT, due to its higher capacity to handle massive volumes of data in comparison with previous generations. The 5G technologies are expected to radically change mobile networks with superfast speeds, and promises an end to congestion, by significantly reducing latency.

This technology started to be commercially deployed on the ground in 2020. However, it is mainly taking place in developed countries, and some countries in Asia, notably China. This situation is expected to remain in 2025 (figure I.27). It is forecasted that 5G mobile data traffic will surpass 4G and lower technologies by 2026 (figure I.28). Even though North America and Europe have lower shares in global mobile subscriptions in 5G technology, they have a larger share in global data consumption, because of efficient networks, high-end user devices and affordable voluminous data packages.²⁵

The 5G technology is expected to have a positive impact on customer experience of mobile devices in terms of Internet quality connection and increased data volumes. Globally, this will accelerate the trend to swap desktops (fixed broadband) for mobile devices, mainly for e-commerce shopping, videos and gaming. Messaging and social networking applications, already and widely used on smartphones, will also benefit from 5G. It will also affect cloud services. All of these will involve increased cross-border data transfers. Because of its high capacity to handle data, as well as its potential economic impact, 5G is a key element behind the technology/trade conflicts between the United States and China, with Chinese company Huawei, a leader in 5G development, at the centre.

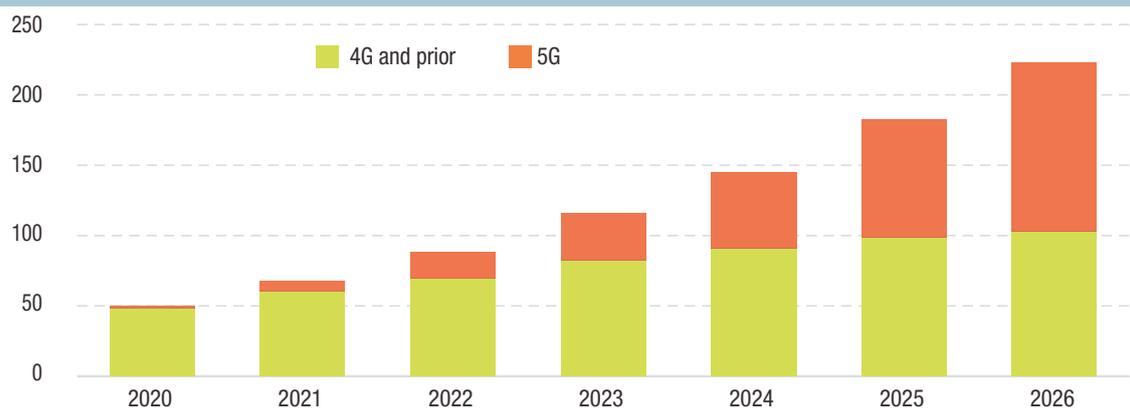
²⁵ See Ericsson Visualizer, available at www.ericsson.com/en/mobility-report/mobility-visualizer?f=8&ft=2&r=1&t=1,20&s=4&u=3&y=2020,2026&c=3 (accessed April 2021).

Figure I.27. 5G adoption, by region, 2025
 (Per cent of total connections)



Source: UNCTAD calculations, based on GSMA (2020a).
 Note: Country groups are those of the source.

Figure I.28. Global mobile data traffic projections, by technology, 2020–2026
 (Exabytes per month)



Source: UNCTAD, based on Ericsson Visualizer, available at www.ericsson.com/en/mobility-report/mobility-visualizer?f=8&f=2&r=1&t=1,20&s=4&u=3&y=2020,2026&c=3 (accessed April 2021).

2. Submarine cables

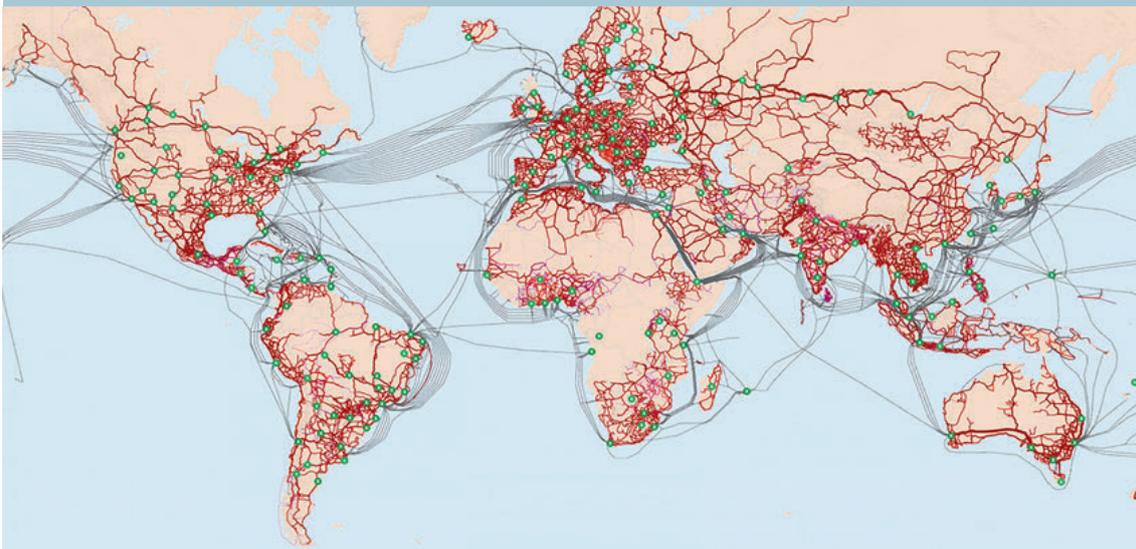
It is estimated that about 99 per cent of international traffic goes through submarine cables (ITIF, 2019). Their advantage over other channels, such as satellites (discussed below), is that cables can carry far more data at far less cost.²⁶

Submarine cable connections are shown in figure I.29, which also includes terrestrial transmissions. The ITU Interactive Terrestrial Transmission Map takes stock of national backbone connectivity (optical fibre, microwaves and satellite Earth stations), as well as of other key metrics of the ICT sector.²⁷

²⁶ See Submarine Cable FAQs, available at www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

²⁷ More detailed submarine cable maps can be found at the Global Internet Map 2021, available at <https://global-internet-map-2021.telegeography.com/>; and at Platform DIGITAL, available at https://go2.digitalreality.com/rs/087-YZJ-646/images/Map_Digital_Realty_2010_Platform_DIGITAL_Global_Map.pdf?_ga=2.119330761.1552758197.1613555008-584212833.1613555008.

Figure I.29. Internet transmission map, June 2021



Source: UNCTAD, based on ITU Interactive Terrestrial Transmission Map, available at www.itu.int/itu-d/tnd-map-public/.

Regarding interregional routes, the map shows that the highest density of the submarine cable network is in the northern transatlantic route and the transpacific routes, between the United States and Europe, and between the United States and Asia, respectively. The map also shows that the largest density of within-region connections are in Europe, East Asia and South Asia. Africa and Latin America show lower density, both on intercontinental as well as intraregional interconnections; large areas in these regions remain underserved.

The main users of international bandwidth are also the ones who are most heavily investing in cables. These include content providers such as Google, Facebook, Amazon and Microsoft, but also include carriers such as Telxius, China Telecom and Telstra.²⁸ According to TeleGeography, “Unlike previous submarine cable construction booms, content providers like Amazon, Google, Facebook, and Microsoft are taking a more active role in this recent surge. These companies alone have such incredible demand for data center traffic that they’re driving projects and route prioritization for submarine cables.”²⁹ This is illustrated in figure I.30, which shows the share of international bandwidth capacity use by type of provider.³⁰ As noted earlier in this chapter, an estimated 80 per cent of total Internet traffic relates to videos, social networking and gaming services, which are to a high degree provided by major digital platforms such as YouTube (Google), Netflix and Facebook, for instance.

3. Satellites

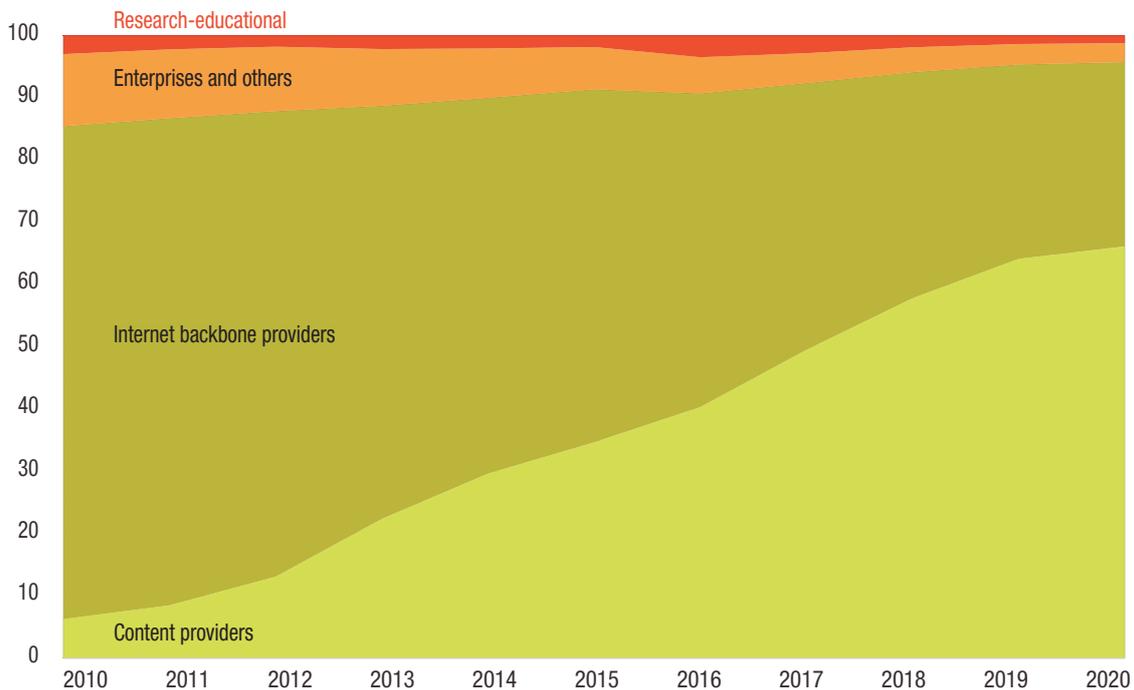
Satellites are useful in reaching remote areas that are not wired by fibre. IDC (2021b) explores the status of next-generation satellite connectivity and how it will open new connectivity use cases, not only for remote locations, but also in suburbs, cities and towns. It concludes that the operational edge, the tactical edge, and the remote enterprise and government edge will get a major boost in terms of connectivity and functionality if/when 5G device-to-satellite becomes a reality; 5G-to-satellite connectivity will open important use cases in commercial and military transportation, agriculture, oil, gas and mining, and utilities, as well as remote residential broadband connectivity.

²⁸ See TeleGeography, 8 October 2019, Is Your Planned Submarine Cable Doomed?, available at <https://blog.telegeography.com/is-your-planned-submarine-cable-doomed>.

²⁹ See TeleGeography, 9 November 2019, A Complete List of Content Providers’ Submarine Cable Holdings, available at <https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list>.

³⁰ For more details on the status of the submarine cable industry, see “Submarine Telecoms Industry Report 2020/2021 Edition”, available at <https://subtelforum.com/products/submarine-telecoms-industry-report/>.

Figure I.30. Global used international bandwidth by type of provider, 2010–2020
 (Per cent)



Source: UNCTAD calculations, based on TeleGeography.

The big players, such as SpaceX and Amazon, have been investing heavily in fast satellite broadband. They have each planned to spend approximately \$10 billion on satellite broadband.³¹ These companies seek to provide broadband to remote and underserved places, helping schools and government overseas operations, or providing Internet access to regions affected by natural disaster or conflict. Another major reason behind these investments is the possibility to improve access to data from an increased number of Internet users, and thus generate new revenues. The potential return on investment is huge. Morgan Stanley (2020) estimates that “the global space industry could generate revenue of ... \$1 trillion or more in 2040, up from \$350 billion, currently. Yet, the most significant short- and medium-term opportunities may come from satellite broadband Internet access... satellite broadband will represent 50 per cent of the projected growth of the global space economy by 2040—and as much as 70 per cent in the most bullish scenario. Launching satellites that offer broadband Internet service will help to drive down the cost of data, just as demand for that data explodes”.

4. Internet exchange points

The development of data-related domestic Internet infrastructure is as important for the functioning of the Internet as the quality of connectivity and Internet coverage, to engage more people and companies in the data-driven digital economy. This includes Internet exchange points (IXPs) and co-location data centres. IXPs are physical locations where different networks connect to exchange Internet traffic via common switching infrastructures. The networks that participate in IXPs can be Internet service providers, content providers, hosting companies, Governments, etc. IXPs are dispersed across countries, enabling local networks to efficiently exchange information, as they eliminate the need to exchange local Internet traffic overseas. It has been shown that access speeds for local content can improve as much as tenfold with an IXP, as traffic is routed more directly (Internet Society, 2015).

³¹ See *Reuters*, 30 July 2020, Taking on SpaceX, Amazon to invest \$10 billion in satellite broadband plan.

There were 556 IXPs in the world as of April 2021, with the highest number in developed economies (293), followed by developing and transition economies (220 and 43, respectively). In terms of the average number of IXPs per country in these groupings, there were 7.9, 3.9 and 2.6 IXPs per country, respectively, in developed, transition and developing countries. At the regional level, Europe led, followed by North America and Asia, in the absolute number of IXPs (figure I.31). In terms of volume of data traffic passing through these regional IXPs, Europe, with 28 per cent of all IXPs, led as well, with 60 per cent of the global domestic bandwidth production. This is partly due to the fact that there are several IXPs working as intercontinental hubs in Europe. Africa represented 9 per cent of all IXPs, but their domestic bandwidth production was only 2 per cent.

The presence of an IXP cannot always ensure more benefits to local customers. For instance, Djibouti has one IXP, which acts as a regional hub, providing services to neighbouring countries, but the monopolistic structure of its telecommunications sector results in unaffordable Internet charges (World Bank, 2021). Therefore, the presence of IXPs in a country or the greater volume of data exchanged through them does not automatically translate into faster speeds and lower charges of Internet connection for local users. Conversely, an inclusive IXP for domestic, international and diverse partners, which permits equal treatment to all participants (often competitors), can encourage the data peering of their networks. However, most developing countries lack domestic infrastructure to permit locally generated data to be exchanged via IXPs, although investment in equipment to establish an IXP is not expensive (Internet Society, 2015), stored at co-location data centres and processed on cloud platforms (World Bank, 2021). The state of co-location data centres and cloud markets in the world is presented in the next subsection.

5. Cloud markets and data centres

Cloud computing allows for the delivery of computing services over the Internet. In this way, companies can access faster innovation processes and flexible resources, and benefit from economies of scale, while they can store their data at much lower costs. Gartner (2019) predicts that, by 2025, 80 per cent of enterprises will shut down their traditional data centres (10 per cent already did in 2019), and instead move to co-location data centres and hyperscale data centres.

Co-location data centres are highly concentrated in developed countries. As of January 2021, within a total of 4,714 co-location data centres, almost 80 per cent were based in developed countries, mainly in North America and Europe. Only 897 were in developing countries, mainly in Asia, and 119 in transition economies. Africa and Latin America hosted, respectively, 69 and 153 of these data centres. It is worth noting that even though the EU27 and the United Kingdom had, respectively, 1,105 and 273 co-location data centres (compared with the 1,796 in the United States and only 154 in China), Europe has not been able to reap the benefits from data to the extent that the United States and China have. This suggests that it takes more to succeed in the data economy than investing in data centres.³²

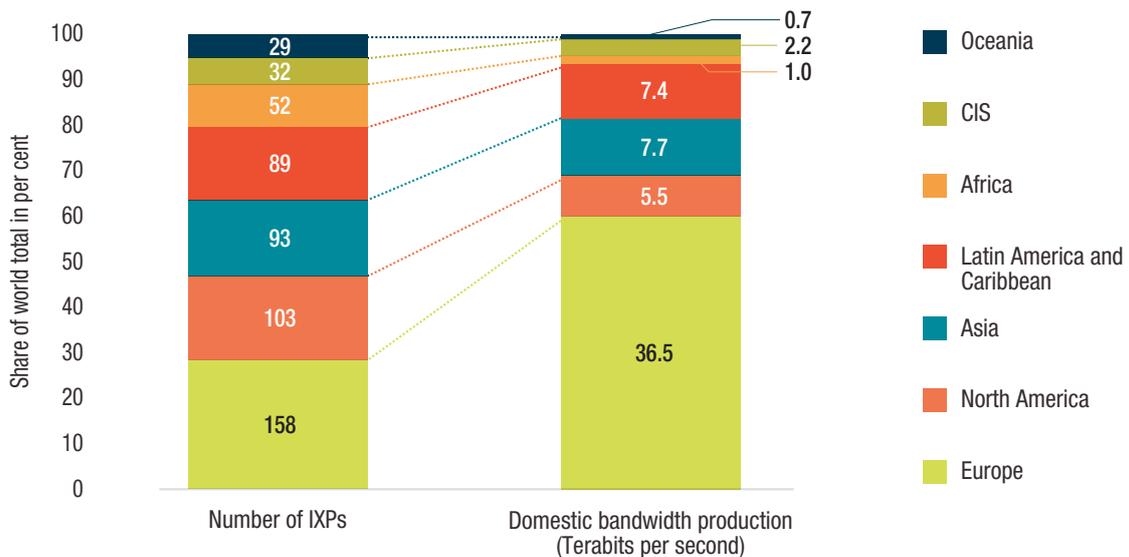
In the case of hyperscale data centres,³³ the leading position is held by the United States, which accounted for 39 per cent of the total of 597 hyperscale data centres by the end of 2020, followed by China with 10 per cent and Japan with 6 per cent. The total number has more than doubled since 2015. Amazon, Microsoft and Google collectively operate over half of all hyperscale data centres. Amazon and Google opened the most new data centres in 2020, accounting for half of the additions (Synergy Research Group, 2021a). Overall, as shown in figure I.32, two companies from the United States (Amazon and Microsoft) accounted for 52 per cent of total cloud infrastructure services revenues.

Data analysis and use, supported especially by data centres, can be very helpful for the achievement of sustainability goals, including fighting climate change. However, the digital economy, in particular the data centres, have environmental impacts that need to be accounted for (see box I.4). The location of

³² UNCTAD calculations, based on the Data Center Map database, available at www.datacentermap.com/datacenters.html (accessed January 2021).

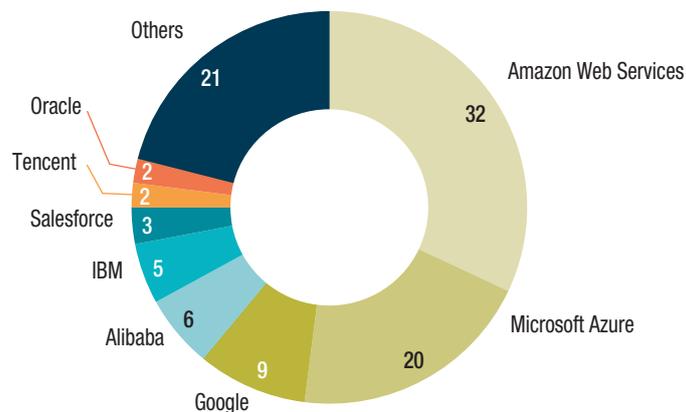
³³ According to Equinix (2020): "A hyperscale data center is a type of wholesale colocation engineered to meet the technical, operational and pricing requirements of hyperscale companies, such as Amazon, Alibaba, Facebook, Google, IBM, Microsoft and a handful of others. These 'hyperscalers' require huge amounts of space and power to support massive scaling across thousands of servers for cloud, big data analytics or storage tasks."

Figure I.31. Internet exchange points, number and bandwidth by IXPs, by region, April 2021



Source: UNCTAD calculations, based on Packet Clearing House database, available at https://www.pch.net/ixp/summary_growth_by_country (accessed April 2021).

Figure I.32. Cloud infrastructure service revenues, by provider, Q4 2020
 (Market share in per cent)



Source: UNCTAD, based on Synergy Research Group (2021b) and Statista (2021).

data centres can be driven by an environment logic (for example, in countries with moderate climate for saving energy on cooling their infrastructures); but it is also based on other factors, such as the reliability and cost of use of local energy infrastructures (see chapter III). The location of data centres is a key issue in relation to cross-border data flows. As will be discussed in detail in chapter IV, requirements to locate data storage in a particular territory are one of the measures used to regulate cross-border data flows. Growth of IoT and 5G uptake may represent an evolution in the data centre market from a predominance of hyperscale data centres to so-called “edge data centres”, since the data latency transmission needs will require data to be closer to the source.³⁴ There are indications of a move towards a multi-cloud system, which combines different types of data centres.

³⁴ See CBInsights, 11 March 2021, What is edge computing? Available at www.cbinsights.com/research/what-is-edge-computing/.

Box I.4. Energy consumption of data centres and data transmissions networks

Energy infrastructure and consumption are critical factors for the working of the data-driven digital economy. According to The Shift Project (2019:16), the digital economy's energy consumption as a ratio of global energy consumption increased from 1.9 per cent in 2013 to 2.7 per cent in 2017, and was on course to reach 3.3 per cent in 2020. Among the different segments of the digital economy, data centres and data transmission networks together accounted for 35 per cent of total energy consumption in 2017 (19 and 16 per cent, respectively). According to the International Energy Agency (IEA, 2020), the global demand for energy of data centres and data transmission networks were, respectively, 200 TWh (or 0.8 per cent) and 250 TWh (or 1 per cent), with mobile networks accounting for two thirds within the latter.

Data centres consume electricity in order to gather, store, transmit and analyse data. Although their global level of consumption has remained constant over time, what has radically changed is the structure of data centre types. The share in energy consumption of traditional data centres as a proportion of all data centres fell from 90 per cent in 2010 to 30 per cent in 2019, reflecting the rise of cloud and hyperscale data centres. IEA forecasts that the share of hyperscale data centres will increase to almost 50 per cent of the energy consumption by all data centres in 2022. As noted by IEA (2020), "If current trends in the efficiency of hardware and data centre infrastructure can be maintained, global data centre energy demand can remain nearly flat through 2022, despite a 60 per cent increase in service demand. Strong growth in demand for data centre services continues to be offset by ongoing efficiency improvements for servers, storage devices, network switches and data centre infrastructure, as well as a shift to much greater shares of cloud and hyperscale data centres. ... The shift away from small, inefficient data centres towards much larger cloud and hyperscale data centres is evident in the shrinking share of data centre infrastructure in total energy demand."

Source: UNCTAD.

I. DATA PROCESSING AND USE: ARTIFICIAL INTELLIGENCE

Benefits and costs of data emerge in large part from their use in feeding AI algorithms, to provide insights and predict behaviours. There is a bidirectional relationship between AI and data: without data, the contribution of the AI field would be limited to knowledge-based systems governed by "if-then rules"; and without AI, the value that could be extracted from data would be limited to human experience and theoretical understanding of the real-world phenomena, only enhanced with faster and more precise computation capabilities that machines could offer. Huge benefits can be derived from AI and the control of data, which provide not only economic gains, but also enormous power and capacity to control and shape the future of technology, the economy and society. This results in a highly competitive race for AI leadership among countries worldwide. There is also intense competition in the private sector among the big digital platforms, which are all very active in AI-related investment.

At the country level, the United States is leading in AI development, with China rapidly catching up. These two countries accounted for as much as 94 per cent of all funding of AI start-ups between 2016 and 2020.³⁵ The European Union is falling behind.³⁶ Developing countries are at a disadvantaged position on AI development, particularly those in Africa and Latin America. A study about the current and potential use of AI by start-ups and small and medium-sized enterprises in low- and middle-income countries in four regions – sub-Saharan Africa, North Africa, South Asia and South-East Asia – concluded that "while AI has the potential to achieve social good, positive outcomes are not guaranteed. There are many fundamental questions about data protection, ingrained bias as a result of poor data collection methods, social inclusion and the responsible use of AI. AI enables new technologies to improve efficiency and productivity, but it may also deepen inequalities, hindering the achievement of

³⁵ UNCTAD, based on CBInsights data, available at www.cbinsights.com (accessed January 2021).

³⁶ For a detailed comparison of the situation with regard to AI development in the United States, China and the European Union, see Castro and McLaughlin (2021).

the United Nations Sustainable Development Goals. Since increased use of data introduces further privacy and ethical concerns, AI solutions should be guided by sound privacy and ethical principles” (GSMA, 2020c:2).

It is estimated that global investment in AI companies has increased tremendously over the past five years. In 2019 alone, privately held AI companies attracted nearly \$40 billion in disclosed equity investment across more than 3,100 discrete transactions. Because some transactions do not have publicly disclosed values, total transaction value could have been significantly higher – as much as \$74 billion. The United States has the world’s largest investment market in privately held AI companies (Arnold et al., 2020). Global digital platforms are playing a key role, thanks to their advantage in accessing massive amounts of data.³⁷ The evolution of private investment in AI companies in recent years is presented in figure I.33, which shows the limited role of developing countries, apart from China. In terms of government spending on AI, China ranks first (at around \$22 billion), followed by Saudi Arabia, Germany, Japan (all below \$4 billion) and the United States (at around \$2 billion).³⁸

Once the situation of all stages of the data value chain has been reviewed, from data collection to data use in AI, passing through transmission and storage, an element that is present in all these stages is the use of semiconductors. They are essential for data flows and for the digital economy to work. The semiconductors market has been negatively affected by the disruption of global value chains, due to the pandemic. Semiconductors are also a major factor in the geopolitics dynamics connected to digital technology developments (see box I.5).

Figure I.33 Private investment in AI companies, by economy, 2015–2020
(Billions of dollars)



Source: UNCTAD calculations, based on the publicly available database of NetBase Quid – 2021 AI Index Report (Zhang et al., 2021), available at <https://aiindex.stanford.edu/report/> (accessed April 2021).

³⁷ See Unite.ai, 17 October 2020, Investments by Tech Giants In Artificial Intelligence is Set to Grow Further, available at www.unite.ai/the-investments-of-tech-giants-in-artificial-intelligence-is-set-to-grow-further/.

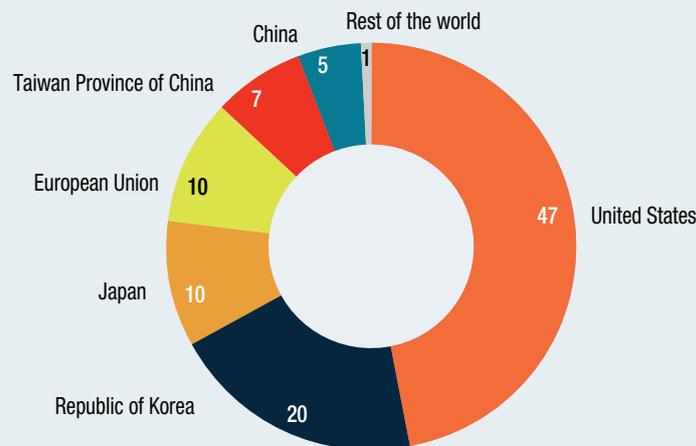
³⁸ Data are as publicly announced in the national AI strategy report. See Tortoise, “The Global AI Index, Spotlighting the G20 nations”, available at www.theglobalaisummit.com/FINAL-Spotlighting-the-g20-Nations-Report.pdf.

Box I.5. The semiconductor market

With the exponential growth of data, chips are increasingly needed for data generation, transfer, processing and storage. Contrary to most of the digital technological developments, which are mostly led by the United States and China, the latter does not play a prominent role in the semiconductor market. The United States accounted for 47 per cent of total sales in 2020, and the Republic of Korea for another 20 per cent (box figure). China ranked only sixth, with 5 per cent of total sales.

In 2021, the semiconductor market has been experiencing a situation of scarcity due to the pandemic. The boom in consumer electronics led to a surge in demand and the global semiconductor value chain experienced difficulties, resulting in a shortage of supply (Varas et al., 2021).

Box figure. Semiconductor sales, by economy, 2020
(Share of world total in per cent)



Source: UNCTAD calculations, based on 2021 Factbook, Semiconductor Industry Association, available at www.semiconductors.org/wp-content/uploads/2021/05/2021-SIA-Factbook-FINAL1.pdf.

J. DATA IN RELATION TO HUMAN RIGHTS AND SECURITY

Data are not just an economic resource. They are also closely related to issues of privacy and human rights in general, as well as security. Data can be abused or misused in ways that can affect political systems and democracy. Some high-level events have served as reminders of the need for these issues to be carefully addressed. Some of the most well-known incidents include: in 2013, the disclosure by Edward Snowden of global surveillance programmes; in 2018, the information that consulting firm Cambridge Analytica had obtained the personal data of users without their consent; and, in 2020–2021, concerning revelations and investigations into data protection issues with regard to the facial recognition company Clearview. The data-driven digital economy has also given rise to significant cases of misinformation and disinformation. The digital world is filled with “fake news”, which allow for the manipulation of society. This phenomenon became highly evident with the COVID-19 pandemic, giving rise to what the World Health Organization qualifies as an “infodemic”.³⁹

The 2020 Ranking Digital Rights Corporate Accountability Index evaluates “26 of the world’s most powerful digital platforms and telecommunications companies on their publicly disclosed commitments and policies affecting privacy and freedom of expression and information. These companies held a combined market capitalization of more than \$11 trillion. Their products and services affect a majority of the world’s 4.6 billion internet users. In 2020, we saw improvements by a majority of companies

³⁹ See World Health Organization, Infodemic, available at www.who.int/health-topics/infodemic#tab=tab_1.

and found noteworthy examples of good practice. But these things were overshadowed by findings demonstrating that the global Internet is facing a systemic crisis of transparency and accountability. Users of the world's most powerful digital platforms and telecommunications services are largely in the dark about who has the ability to access their personal information and under what circumstances. People lack basic information about who controls their ability to connect, speak online, or access information, and what information is promoted and prioritized".⁴⁰ The results for digital platforms are presented in table I.3.

While human rights and security are of a more qualitative nature and cannot be easily quantified, this section provides some information about trends that point to increased societal concerns that need to be addressed.

1. Privacy and surveillance

With the explosion of data flows, a large proportion of which are personal data, privacy issues have become a major concern globally. Several surveys reflect the increasing concerns of individuals about their privacy as digitalization increases. For example, according to the 2019 CIGI–Ipsos–UNCTAD Global Survey on Internet Security and Trust, 78 per cent of the people surveyed were concerned about their online privacy, with over half being more concerned than they were a year ago. This marked the fifth year in a row that a majority of those surveyed said they felt more concerned about their online privacy than in the previous year.⁴¹ In the United States, another 2019 survey revealed that the majority thinks "their personal data is less secure now, that data collection poses more risks than benefits, and believe it is not possible to go through daily life without being tracked".⁴²

Company	Total	Governance	Freedom of expression	Privacy
Twitter	53	47	60	51
Verizon Media	52	64	40	51
Microsoft	50	65	40	51
Google	48	54	46	48
Facebook	45	62	35	46
Apple	43	49	22	54
Kakao	42	42	38	44
Mail.Ru	27	23	19	33
Yandex	27	24	20	33
Alibaba	25	7	17	36
Baidu	25	11	13	37
Samsung	23	29	15	25
Tencent	22	4	15	32
Amazon	20	6	14	28

Source: UNCTAD, based on 2020 Ranking Digital Rights Corporate Accountability Index, available at <https://rankingdigitalrights.org/index2020/>.

⁴⁰ See 2020 Ranking Digital Rights Corporate Accountability Index, available at <https://rankingdigitalrights.org/index2020/>.

⁴¹ See www.cigionline.org/internet-survey-2019.

⁴² Pew Research Center, 15 November 2019, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, available at www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

During the pandemic, in order to trace the contagion and prevent social contact with people having the virus, a number of contact tracing applications were developed. These raised a debate with regard to privacy issues and data protection. It appears that these have been more successful in Asia than in Europe or the United States. Indeed, in a 2020 Cisco survey on privacy in the pandemic, 60 per cent of people expressed concern about their data being protected in the tools they were using.⁴³

The Snowden scandal was a wake-up call around the world about the activities of Governments to survey the population. However, surveillance is equally practiced by the public as well as by the private sector, as companies control a lot of data on individuals. The difference is that Governments' surveillance is mainly for security and political control, while private companies' surveillance focuses on commercial exploitation of data. This can have significant implications in terms of human rights. According to the analysis of Feldstein (2019) on the global expansion of AI surveillance, a growing number of States are deploying advanced AI surveillance tools to monitor, track and surveil citizens. AI surveillance technology is spreading at a faster rate to a wider range of countries than experts have commonly understood. At least 75 out of 176 countries are actively using AI technologies for surveillance purposes. This includes countries with smart city/safe city platforms, facial recognition systems and smart policing. China is a major driver of AI surveillance worldwide, and companies in the United States are also active in this space. AI surveillance technology supplied by these firms is present in 32 countries.

A key technological development for surveillance purposes is facial recognition. This has been very controversial all around the world, and is leading to debates about banning it. In total, there are now 109 countries that are either using or have approved the use of facial recognition technology for surveillance purposes. Meanwhile, in 2019, Belgium found a pilot project using facial recognition technology at an airport to be in breach of federal law, and France and Sweden recently banned the use of facial recognition in schools. In the United States, San Francisco became the first city in the country to ban facial recognition technology outright in 2019. Since then, several other cities, including Oakland and Northampton, have voted to ban it.⁴⁴ The European Union data protection authorities have also called for a ban on the use of these technologies.⁴⁵

2. Security

There are plenty of security threats related to data on the Internet, including data breaches, identity theft, malware, ransomware and other types of cybercrime. The analysis of the recent evolution of data breaches shows that, as a general trend, the number of security incidents decreased between 2015 and 2019. However, incidents that resulted in confirmed disclosure of data to unauthorized parties (data breaches) were fairly constant (about 2,000 cases) in the 2015–2018 period, and in 2019 surged to 3,950 cases. North America was by far the most affected region by the number of incidents and data breaches, followed by Asia and the Pacific, which had a higher frequency of data breaches in proportion to all incidents. These two regions are followed by Europe, the Middle East and Africa. The coverage for Latin America and the Caribbean was limited, so the numbers of incidents and data breaches are small, but do not reflect a better defensive system against data breaches.⁴⁶

Data breaches have become more prevalent due to cloud computing and increased digital storage. As a result of the pandemic, 2020 was an exceptional year, with industries being severely impacted in every corner of the globe. This eased the way for cybercriminals targeting vulnerable victims in the health care industry, as well as those who were unemployed or working remotely. For example, scams

⁴³ Cisco, 2020 Consumer Privacy Survey: Protecting Data Privacy During the Pandemic and Beyond, available at www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-infographic-2020.pdf.

⁴⁴ For more details, see the Facial Recognition World Map, available at <https://surfshark.com/facial-recognition-map>; and *Nature*, 18 November 2020, Resisting the rise of facial recognition.

⁴⁵ See European Data Protection Supervisor, 21 June 2021, EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination, available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en.

⁴⁶ See Verizon, Data Breach Investigation Reports (several years).

increased by 400 per cent in March 2020, making the pandemic the largest-ever security threat. In 2020, the United States saw the highest average cost of a data breach, at \$8.64 billion. It is estimated that, by 2025, cybercrime will cost the world \$10.5 trillion annually.⁴⁷

Investment in cybersecurity companies reached more than \$11 billion in 2020, the highest level since 2016, amid the worldwide economic crisis. The average amount per deal in cybersecurity more than doubled between 2016 and 2020 (from \$10 million to \$23 million). This rise could largely be explained by the increased risk of incidents and data breaches resulting from the accelerated digitalization process of society and the attacks targeting the health sector after the start of the sanitary crisis in 2020. The leading economy in terms of the investment amount in cybersecurity companies is by far the United States (almost three quarters of the global level), followed by China and Israel, for the period 2016–2020 (CBInsights, 2021).

3. Internet shutdowns

In spite of the increased need for Internet use due to the pandemic, there were 155 documented Internet shutdowns in 2020. While this represented a decline from 196 in 2018 and 213 in 2019, the smaller number should not be seen as an indication of the lessened impact of a shutdown or an overall increase in digital rights. In fact, the number of countries that shut down the Internet was 25 in 2018, 33 in 2019 and 29 in 2020. In 2020, out of the 29 countries, 10 were in sub-Saharan Africa, 8 in the Middle East and North Africa, 6 in Asia and the Pacific, 3 in Latin America and the Caribbean, and 2 in Europe. India had by far the largest number of Internet shutdowns, at 109 (Access Now, 2021).

These Internet shutdowns have a disruptive effect on lives and livelihoods – damaging human rights, and hurting public health and safety – and affect the right to development (Nyokabi et al., 2019). Moreover, the total cost to the world economy of Internet restrictions since 2019 was estimated at \$14.5 billion.⁴⁸ The negative impact of shutdowns was augmented during the pandemic.

K. CONCLUSIONS AND ROAD MAP TO THE REST OF THE REPORT

In setting the stage for this Report, this chapter has addressed basic issues related to the definition and characteristics of data, before providing an overview of recent developments in the data-driven digital economy, in which cross-border data flows take place. It has analysed global developments with regard to ICT and data infrastructure, data traffic, value and markets, as well as in the different stages of the data value chain. The traditional digital divide, understood in terms of Internet connectivity, access and use, remains high, and it is a recurrent challenge for development. Moreover, as the role of data as an economic resource, and that of cross-border data flows, have been increasing, new dimensions of the digital divide have emerged in connection to the collection, transmission, storage, processing and use of data. Thus, a data-related divide is adding to the long-standing digital divide.

— A data-related divide is adding to the long-standing digital divide.

Rapid developments in digital technologies can offer opportunities in terms of value creation and capture, but they also raise significant challenges. The data-driven digital economy is characterized by major power imbalances and inequalities between and within countries. A few global digital platforms from the United States and China are getting most of the benefits. The pandemic has aggravated this

⁴⁷ See Varonis, 16 April 2021, 98 Must-Know Data Breach Statistics for 2021; it also gives details of the main recent data breaches.

⁴⁸ See Top10VPN, 4 January 2020, The Global Cost of Internet Shutdowns.

situation with the acceleration of digitalization trends. These global digital platforms have been able to strengthen their dominant positions while the rest of the economy fell into an economic crisis.

Global digital platforms are increasingly investing in all parts of the global data value chain: data collection through the consumer-facing platform services, data transmissions through submarine cables and satellites, data storage (cloud and hyperscale data centres), and data analysis (AI). Overall, the trends shown in this chapter also suggest a need to change the denomination of global digital platforms. Although they have the data advantage through their platform component, they are no longer just digital platforms. Their businesses span across many sectors, and they are present at all layers of the digital economy (from the core digital sector to the narrow scope of the digital economy and the broad scope of the digitalized economy).⁴⁹ They should be considered as global digital corporations. Hence, it becomes increasingly difficult to consider regulations of cross-border data flows without also considering the governance of these digital corporations.

The rapid pace of digitalization before 2020 had already sounded the alert about the need to regulate the digital economy in order to maximize its benefits and minimize its risks and challenges, so that it can contribute to development (UNCTAD, 2019a). The acceleration of digitalization as a result of the pandemic has made digital divides even more evident and the imperative to regulate – at national, regional and international levels – even more urgent. Data governance is critical in this context, including the governance of cross-border data flows, which is the topic of this Report.

As cross-border data flows become increasingly prominent in the global economy, there is a growing need to properly regulate them at the international level, within the broad context of global data governance. Currently, those that can extract or collect the data – and have the capacity to further process them, mainly global digital corporations from the United States and China – are in a privileged position to appropriate most of the value of data. By contrast, those who can be considered as producers or source of the data in raw form – i.e. the users of the platforms, with a large number of them in developing countries, who are also contributing to that value – do not receive development gains. There is a need for a new international system to regulate these flows, so that the benefits of cross-border data flows are equitably distributed.

• The acceleration of digitalization as a result of the pandemic has made digital divides even more evident and the imperative to regulate the data-driven digital economy – at national, regional and international levels – even more urgent.

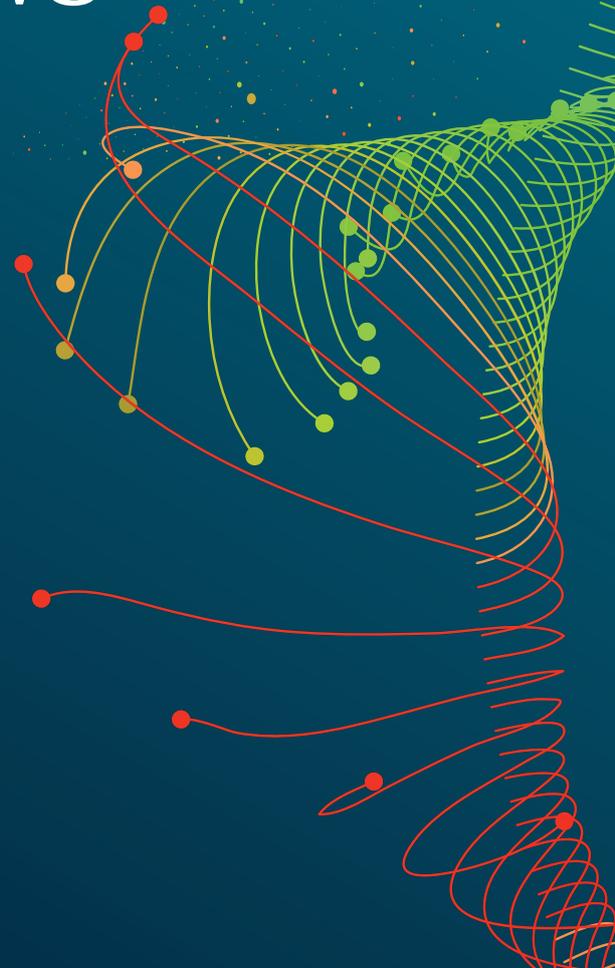
Against this background, focusing on the international dimension of data, the rest of the Report is structured as follows. Chapter II reviews the literature on cross-border data flows, and reveals some gaps that would need to be filled, providing a motivation for this Report in contributing towards meeting such needs. Chapter III takes a step back by looking at the main issues at stake on cross-border data flows and development. Chapter IV discusses the approaches towards the data-driven digital economy in major areas of influence in the world, which have a bearing on the global governance of data flows, or run the risk of fragmentation in the digital space, with potential implications for developing countries. Chapter V provides a mapping of the main measures used at the national level to regulate cross-border data flows, while chapter VI reviews regional and international policy approaches on cross-border data flows. Finally, chapter VII concludes with a discussion on potential policy options to move forward towards a consensus in the governance of data and cross-border data flows, in a way that ensures that potential benefits generated support global development goals, while preventing data abuse and misuse.

⁴⁹ See the representation of the digital economy in figure I.1 of UNCTAD (2019a).

Before turning to a more detailed analysis of the role and implications of data flows for development and related policies, this chapter provides a review of the literature dealing with cross-border data flows. It seeks to identify major issues and gaps, as well as areas for improvement, that are highly relevant for the international policy debate.

The chapter shows that there is generally a lack of common definitions on data and cross-border data flows. This hampers their measurement, as well as constructive discussion and consensus-building on their governance. Few studies discuss the development implications of cross-border flows of different types and taxonomies of data. Moreover, most of the literature focuses on the trade dimension of data, often neglecting the multidimensional character of data. Most studies are from anglophone countries and very few deal with developing countries.

A REVIEW OF THE LITERATURE ON CROSS-BORDER DATA FLOWS



Literature on **cross-border data flows** has various limitations and gaps

Commonly agreed definitions of data and cross-border data flows are missing, hampering their measurement as well as constructive discussion and consensus-building on their governance

Few studies discuss the **development implications** of cross-border data flows

Most recent studies on cross-border data flows mainly look at them from a trade angle, and few consider them in a **multidimensional manner that factors in economic and non-economic dimensions**

Many studies have clear **ideological leanings** reflecting certain interests

Few studies are for developing countries and most are **anglophone**

There is little hard evidence to support free data flows or strict data localization policies

Research gaps

Priorities for future research

Working on definitions and the **measurement** of data and data flows

Focusing on the **development implications** of cross-border data flows

Stronger emphasis on the **multi-dimensional nature of data**

More balanced assessments of cross-border data flow policies, pondering the pros and cons

A. INTRODUCTION

The growing role of data in the evolving digital economy, following rapid progress in digital technologies, has resulted in a parallel surge in the literature on cross-border data flows in recent years. Early literature that used the term “cross-border data flows” was concentrated in banking documents and publications on information technology (IT) topics. The international debate on cross-border data flows is not new. These flows were already high on the international agenda in the 1970s and 1980s, when “transborder data flows” were considered. For example, the Organisation for Economic Co-operation and Development (OECD) adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 (Kuner, 2011).¹ The focus at that time was mainly on personal data protection and privacy issues. Over the past decade, as the role of data as an economic resource increased, debates have moved towards economic-related aspects.

With the expansion of the Internet, which changes information, goods and service flows, cross-border data flows have gained in importance, and the number of publications has risen. As illustrated in figure II.1, the number of search results on Google Scholar for scientific publications containing “cross-border data flows” per year surged from 1994 to 2020.

This chapter reviews the legal, economic, civil society and private sector literature² assessing the current status of research on cross-border data flows and their regulation.³ In particular, it looks at relevant definitions currently in use, the measurement of data flows, the focus of research and perspectives of countries at different levels of development. In doing so, the chapter identifies a number of issues that require further investigation. A key issue is defining and measuring cross-border data flows, to better understand where the debates stand; this is difficult, as the importance of data is growing in diverse contexts.

Another relevant aspect is the dominance of research on and from developed countries, which tends to leave out the role and needs of developing countries in this evolving area of the digital economy. Moreover, many studies tend to rely on implicit assumptions and ideological leanings, without considering all the arguments.

This literature review is not intended to be exhaustive or systematic. Its purpose is to highlight major issues and gaps, as well as areas for improvement, that are highly relevant for the international policy debate on cross-border data flows and development. This Report, then, aims to address and contribute to filling in some of these gaps. Moreover, this chapter mostly reviews the recent literature, as it is more relevant for informing the existing international policy debate on this matter.

Figure II.1 Number of publications on cross-border data flows, 1994–2020



Source: UNCTAD, based on Google Scholar, available at <https://scholar.google.com> (accessed 18 January 2021).
Note: Based on keyword searches for “cross-border data flow” and “cross-border data flows” for publications dated from 1994 to 2020. The figure aims to be indicative, and does not claim to be a comprehensive systematic keyword search of associated topics.

¹ See chapter VI for details on the OECD Guidelines.

² This review does not cover literature by Governments, because views of Governments are mostly reflected in the policy discussions presented in chapters IV to VI.

³ A table with details of the literature reviewed is presented in the online annex to chapter II, available at https://unctad.org/system/files/official-document/der2021_annex1_en.pdf.

B. DEFINING DATA AND CROSS-BORDER DATA FLOWS

While cross-border data flows are becoming more important in research and policy literature, consensus on the most basic elements – the definitions of data and of cross-border data flows – remains elusive.

Data are often taken as given, assuming a common understanding as the basis of many studies. They can, however, refer to different concepts or dimensions. Krotova and Eppelsheimer (2019) undertake a literature review on data governance using text mining; they distinguish between data and information. Information is defined as being made up of refined and processed data to increase their value, whereas data describe the characteristics and properties of events or objects. Similarly, the OECD defines data as a collection of unprocessed points which, through processing and analysis, become information (Casalini and López González, 2019; Nguyen and Paczos, 2020; Tomiura et al., 2019).

In relation to data governance, Ciuriak (2020) considers data the new capital asset to capture rents in an economy. Aaronson (2019a) elaborates on how often a too-limited view of what defines data is taken; data cannot simply be treated as other economic resources – such as infrastructure, labour or capital – as much data arise simply as a by-product of life, which consequently has implications on how to regulate and govern data flows.

Similarly limited is a workable definition of what constitutes a cross-border flow of data – a definition that allows for measurement, and forms a common ground for discussions. Basically, it is an unimpeded transfer of data across international borders or different international markets (Linden and Dahlberg, 2016; WEF, 2020b). However, as data do not cross borders via customs, more specificity in the definition would be beneficial. The Business Software Alliance (BSA, 2017) makes the definition slightly more operational in terms of defining a start and end point of a flow, by defining a cross-border data flow as a transfer of data between servers located in different countries.

Many other authors just do not define these flows. Those who support the free flow of data across borders focus on their possible positive impacts, such as contributing to innovation, productivity, research and social interactions (BSA, 2017; Spiezia and Tscheke, 2020).

Overall, taking the definitions of data and cross-border data flows as a given makes many authors zero in on a specific aspect of data, predominantly trade-related, without considering other domains that rely on data flows and might have other characteristics – and, consequently, different implications for data governance, regulation and countries at different levels of development.

C. QUANTIFYING CROSS-BORDER DATA FLOWS AND THEIR IMPACT

The relatively high-level definitions of cross-border data flows leave wide open the question of how to measure the actual flows, as discussed in chapter I. Technically, data flows can be measured in bits and bytes per unit of time (Nicholson and Noonan, 2017). This leaves out where this measurement should take place to be able to determine whether a certain data flow is cross-border and whether it constitutes an inflow or an outflow. Nevertheless, a growing body of literature aims to quantify the impact of these flows.

Some research circumvents measurement issues by defining them narrowly, such that they become tractable and quantifiable. McKinsey (2014, 2016, 2019) largely defines these flows as cross-border data and communication flows. Hence, they are measured using Internet bandwidth, Internet penetration and Internet call minutes. At the same time, these reports try to differentiate cross-border data flows from other flows, such as financial ones (McKinsey, 2014), even though banking is associated with large data flows. Overall, they find that the contribution of data to increasing global gross domestic product (GDP) overtook that of trade in goods (McKinsey, 2016). However, even mobile operators appear to consider measuring these flows to be sufficiently complex. A publication on cross-border data flows of their business association, GSMA, refrains from quantifying international data flows (GSMA, 2018a).

Others refer to case studies to demonstrate the growing role of data, particularly in business, health and research. Castro and McQuinn (2015) illustrate how firms such as airplane manufacturers collect terabytes of data during international flights to support maintenance and repair services. Similarly, a manufacturer of trucks and buses has established a data-driven arm to analyse driving data to optimize fuel efficiency, reduce transport's environmental impact, and use aggregated data to monitor the fleet and detect problems earlier (Castro and McQuinn, 2015).

As measuring the volume of data flows remains difficult and approximations dominate, some economic analyses attempt to measure them indirectly. The approaches fall into three broad categories: first, approximations using digital components in trade; second, surveys and observations of changes in behaviour when faced with regulatory changes; and third, assessments of the impact of data flow restrictions.

One approach to quantifying the role of cross-border data flows is looking at the contribution of digitally-enabled services trade to overall trade, or to GDP. Nicholson and Noonan (2017) seek to determine an upper limit estimation of these kinds of services in the overall international service trade of the United States of America between 2002 and 2011. They identify five categories of trade statistics from the Bureau of Economic Analysis, which are enabled by information and communications technology (ICT), and are thus likely to involve data flows. This leads to an approximation, as there is no available information on which share of these services was actually delivered digitally. The authors estimate that, in 2011, digitally-enabled services had a trade surplus of \$136 billion, with digitally-enabled exports amounting to \$357 billion, which accounted for 60 per cent of overall services exports. In addition, they estimate that these services contribute a third of the value added of total exports. Consequently, their value to the economy of the United States is sizable. In turn, the cross-border data flows involved are likely highly valuable. The drawback of this approach is that it can only measure flows for which there is an associated monetary value. Data crossing borders prior to processing that transforms them into products of commercial value cannot be accounted for. Hence, this approach is likely underestimating the importance of cross-border data flows, given that many flows do not appear in official trade statistics.

Tomiura et al. (2019) surveyed large- and medium-sized enterprises in Japan on their data transfers abroad after the introduction of the European Union General Data Protection Regulation (GDPR) on the transfer of personal data; and the cybersecurity laws of China and India. They assess changes in firms' behaviour in a descriptive analysis. Of the respondents, 5 per cent were adversely affected by the introduction of GDPR, and 8 per cent by the cybersecurity laws. Of those affected, a third changed the location of their data storage and processing. Also, 40 per cent of firms tightened their data protection measures in response to GDPR, while more than half of the 8 per cent affected did not react to the cybersecurity laws. Overall, only 1 per cent of respondents transformed or stopped their business with the European Union following the introduction of GDPR. In reaction to cybersecurity laws, around 5 per cent of firms changed their data transfer practices to the countries concerned. In the case of GDPR, this impact of new data flow regulation appears comparably smaller than in some other studies (Gupta et al., 2020; Ferracane and van der Marel, 2020). Moreover, the survey finds a surprisingly low share of businesses transferring data internationally on a daily basis, which may indicate a measurement issue.

Another strand of the literature measures cross-border data flow value implicitly by simulating or estimating the impact of restrictions on data flows, such as GDPR or data localization⁴ laws elsewhere. Bauer et al. (2013) measure these flows indirectly through a reduction in trade, GDP and overall welfare, using a general equilibrium model to simulate the impact of GDPR prior to its introduction. Their estimations show that limiting the free flow of data, with the associated loss in competitiveness, would lead to a contraction of GDP of the European Union of between 0.8 and 3.9 per cent. The negative impact on per capita income could amount to between \$340 and \$1,140. The authors estimate that this loss would wipe out any gains from trade achieved through the European Union–United States Free Trade Agreement (FTA), implying a significant value of cross-border data flows in a trade context.

⁴ Data localization refers to a policy measure in the context of cross-border data flows regulation that imposes requirements to locate data in a particular territory.

Similarly, Bauer et al. (2016) measure the impact of countries' data flow regulation on their industries in terms of productivity, by constructing an index for data regulatory measures. This index is based on subindicators of the OECD Product Market Regulation Index, and country-specific policies, in addition to measures of data intensity in various sectors. They find that restricting the flow of data has an increasingly adverse effect in terms of productivity and prices on industries that are relatively data-intensive. Their estimates show that there would be a reduction in medium-to-long term real GDP of between 0.1 and 0.58 per cent due to the data restrictions – a sum of several billions of dollars in the case of the European Union. Similarly, Badran (2018), Ferracane and van der Marel (2020), and Ferracane et al. (2020) measure the lost value of cross-border data flows from data restrictions in terms of reductions in firms' and sectors' innovation potential and productivity for different sets of countries. An analysis of CUTS International (Gupta et al., 2020) finds that data restriction policies would limit exports of digital services from India such that GDP could decline by 0.2 to 0.34 per cent. For the 2025 target size of the economy of India, this would imply a gap of \$9 billion to \$17 billion.

By contrast, Spiezia and Tscheke (2020) analyse the impact of removing restrictions through pairs of countries becoming signatories to the same data privacy agreements. They find that being a signatory to Convention 108 of the Council of Europe or the United States Safe Harbour agreements with the European Union and Switzerland increases trade in goods from 6 to 8 per cent. Ratifying Convention 108 is associated with growth of trade in services of 12 per cent for country pairs. However, no significant effect is estimated for the United States Safe Harbour agreements.⁵ Hence, the cost of higher compliance rules is outweighed by the benefits of facilitated flows of data within the parties of the agreements; this impact is both statistically and economically significant.

In addition to the challenge of measuring these flows quantitatively, there is also a legal question on what constitutes cross-border data flows, which can impact their measurement. For instance, a transfer of ownership of data from an entity in one country to one in another, without moving the data out of their data centre, could constitute a flow of data across borders without an actual flow of data having occurred and being measured (Nguyen and Paczos, 2020).

At this point, the literature aiming to quantify these flows is filled with proposed steps towards a better understanding of the topic. However, as large gaps remain for providing a comprehensive picture, there is a need for more work on measuring cross-border data flows, to develop different options and eventually identify approaches that can contribute to national statistics on the topic.

D. TYPES OF DATA

Data can be characterized along a multitude of dimensions. The types of data covered in most of the research tend to fall into three categories: trade, business and personal. A significant part of the literature focuses on data in relation to trade. Research covers trade in services, goods and digital services, often trying to quantify the data flows in some manner. Many analyses belong to two categories: first, attempts to quantify current flows of data in the form of service components in trade (McKinsey, 2014; Nicholson and Noonan, 2017); and second, estimations of the impact of data flow restrictions or their lifting (Badran, 2018; Bauer et al., 2013, 2016; Gupta et al., 2020; Ferracane et al., 2020; Ferracane and van der Marel, 2020; Spiezia and Tscheke, 2020).

Alternative types of data in quantifying exercises are volume of communication flows in bytes (Bughin and Lund, 2017; McKinsey, 2014). As the value of communication flows is challenging to determine – making them hard to compare with values of goods and other international flows – these comparisons remain relatively rare.

Legal research in this area falls into three broad, non-exclusive categories of data: trade, personal versus non-personal data, and comparisons of various regimes addressing data flows. Arguments against free data flows are often linked to personal data being outside the control of responsible entities. Hence, a significant part of the literature investigates different global data restriction regimes (Chander

⁵ For a discussion on Convention 108, see chapter VI. The Safe Harbour was replaced by the Privacy Shield, which is also discussed in chapter IV.

and Lê, 2015). Several studies note that regulations often distinguish between personal and non-personal data (Chander and Lê, 2015; Aaronson, 2019a; Aaronson and Maxim, 2013; Meltzer, 2020; Casalini and López González, 2019; Daza Jaller et al., 2020; Mattoo and Meltzer, 2018; WEF, 2020b). Other legal studies investigate the role of data in trade, especially in the context of regulating data flows within the trade regime (Burri, 2016; Daza Jaller et al., 2020; Mattoo and Meltzer, 2018; Hilbig, 2018; BDI, 2017; Aaronson and Maxim, 2013). However, Aaronson (2019a) points out that a large proportion of data is not associated with any trade, which makes regulating data via trade agreements problematic.

In the context of business data, Nguyen and Paczos (2020) analyse the use of data in augmenting existing business models by making them more data-driven, and their value in new business models. Linden and Dahlberg (2016) assess the role of free business data flows in the context of freedom of movement in the European Union.

Another block of literature investigates different types of data in the context of data governance. At the macro level, this concerns questions of regulation both at the national and international levels, and of compatibility and interoperability of various regulatory approaches (Aaronson, 2019a; Ademuyiwa and Adeniran, 2020; GSMA, 2018b; Mattoo and Meltzer, 2018; Microsoft, 2018; WEF, 2020b). At the micro level, the focus is on businesses' data management and the value of data (Engels, 2019; Krotova and Eppelsheimer, 2019).

The World Bank (2021) characterizes data using two dimensions: public or private intent data and, in terms of its data collection methods, new or traditional. Thereby, traditionally collected public intent data often have a broad population coverage, but lack in timeliness, while new private intent data can be highly granular and timely, but are rarely representative of the population, especially minorities.

In addition to these broad categories, Coyle et al. (2020) mention additional dimensions that can help to differentiate between different kinds of data:

- Characteristics: for example, by sensitivity or purpose.
- Origin: provided, observed, derived or inferred (OECD, 2013a).
- Usage: for instance, for human resources, corporate, business-to-consumer or technical purposes (Rentzhog and Jonströmer, 2014).
- Feature: for example, public versus private, proprietary or open, actively or passively created (Nguyen and Paczos, 2020).

These dimensions help increase understanding of the nature and purpose of data, while also illustrating that, depending on the type of data used, they can be described in a multitude of ways. At the same time, this multidimensionality highlights that establishing straightforward rules in connection with data is challenging, as it is difficult to narrowly define data (De La Chapelle and Porciuncula, 2021).

E. POSITIONS TOWARDS CROSS-BORDER DATA FLOWS

Four major groups – civil society, academia and think tanks, the private sector, and international organizations – contribute to the literature on cross-border data flows. Within each group, overall positions towards these flows broadly align.

Academia and think tanks⁶ mostly tend to support the free flow of data, while many also favour clear rules around them (Aaronson, 2014, 2019a; Aaronson and Maxim, 2013; Badran, 2018; Bauer et al., 2013, 2016; Chander and Lê, 2015; Chen et al., 2019; Ciuriak, 2020; Ferracane et al., 2020; Ferracane and van der Marel, 2020; Kimura, 2020; Meltzer, 2020; Tomiura et al., 2019). Economic aspects primarily motivate the studies that are in favour of free data flows, by making the case against data localization and privacy regulations that make international transfers more burdensome. These studies favour cross-border data flows, as these lower costs of doing business and expand international trade, consumer

⁶ Several think tanks – such as the European Centre for International Political Economy, the Information Technology and Innovation Foundation and the Hinrich Foundation, among others – strongly support free flows of data, predominantly motivated by economic and trade arguments.

welfare and GDP (Bauer et al., 2013; Badran, 2018; Hinrich Foundation, 2019; Tomiura et al., 2019; Ferracane et al., 2020; Ferracane and van der Marel, 2020). Another argument against data localization relates to possible inefficiencies. First, keeping data within national borders and establishing a data storage industry are not associated with large increases in employment, as data centres are mostly automated (Chander and Lê, 2015). Furthermore, data localization does not contribute to data security. Keeping data in a single location makes them more vulnerable to destruction due to (natural) disasters, but also because of hackers, when the security is not up to the most recent standards (Chander and Lê, 2015). In addition, Taylor (2020) notes that the opportunity cost from data localization is too high, even for developing countries, as a fragmented Internet will have adverse effects on emerging technologies, such as making them more biased if they rely on a limited and homogenous set of data for transforming data into insights.

However, while supporting free flow of data on the basis of the assumed cost of data localization, the authors do not consider distributional effects of the gains from free data flows, which is a critical aspect for development. Gains, for instance from e-commerce, are likely to accrue especially in sectors and to people that are already privileged in terms of international market access or skills. This could exacerbate existing inequality within and across countries (Hill, 2018; Avila, 2020).

While overall in favour of the free flow of data, Mitchell and Mishra (2019) propose a revised World Trade Organization (WTO) framework with rules that allow for staggered implementation. This would enable developing countries to develop their capacities to enforce new rules on data regulation and to build digital infrastructure before being bound by WTO rules. Furthermore, their proposed framework would require developed countries to provide technical assistance to build this missing capacity. Moreover, some research argues towards free data flows to support human rights, freedom of speech and democracy (Bauer et al., 2013; Chander and Lê, 2015).

Similarly, some international organizations – especially the OECD, the World Bank and the World Economic Forum (WEF) – support the free flow of data, particularly with a focus on trade and as a means to create value (Casalini and López González, 2019; Daza Jaller et al., 2020; Mattoo and Meltzer, 2018; Nguyen and Paczos, 2020; Spiezia and Tscheke, 2020; WEF, 2019; World Bank, 2021). The motivation for relatively free flows of data across borders is supporting economic growth and international cooperation (World Bank, 2021) which require a system of data exchange that is as frictionless as possible – and ideally does not lead to further fragmentation between countries. While a lot of the work is relatively focused on trade, Spiezia and Tscheke (2020) point out that, beyond trade data, there is limited insight on what types of data cross borders. Non-trade-related types of data might require a reconsideration of attitudes towards them flowing freely.

Private sector actors that publish on cross-border data flows are a select group. They mostly have international business interests and hence are generally in favour of free data flows. Their perspective is motivated by maintaining and growing their businesses. Limiting these flows is associated with protectionist measures (BDI, 2017). An additional commonality is the support for a certain level of data security and privacy rules (BSA, 2017; Global Data Alliance,⁷ 2020; GSMA, 2018a, 2018b; Microsoft, 2018). This is likely driven by a need for trust, both from consumers and regulators. Publications in this context consist mainly of statements that emphasize the importance of free cross-border data flows, with little analytical background (BSA, 2017; Global Data Alliance, 2020; International Chamber of Commerce, 2021).

Civil society perspectives are more nuanced in their attitudes towards the free flow of data. Some authors based in the United States argue strongly in favour of cross-border data flows to support the economy, and advocate for trade negotiations to impose binding rules on data flows (Castro and McQuinn, 2015; Cory, 2017, 2019). Others put a stronger emphasis on the need for rules and regulation to accompany these flows. These take different forms, such as common technical standards to ensure security (McLaughlin and Castro, 2019); and/or an appropriate regulatory environment, including data protection, cybersecurity, legal accountability and interoperability between countries (WEF, 2020b). Thus, they are motivated by enabling exchange of data within clear guidelines to protect individuals.

⁷ The Global Data Alliance was created in early 2020 to advocate for free cross-border data flows. See *Medianama*, 23 January 2020, Cross-industry global coalition launched to advocate for free flow of data across borders.



Civil society actors with a focus on developing countries are more cautious towards free data flows. If free flow of data is imposed on countries through trade agreements, developing countries may be taken advantage of (Hilbig, 2018). These agreements may then limit the scope for national policymaking and country-specific approaches to development (Our World is Not for Sale, 2019). Moreover, for developing countries to benefit from the digital economy, they need to find means to localize the economic value of data, which could require temporary protectionist measures or an improved framework for data ownership and remuneration (Gurumurthy et al., 2017; Hill, 2018; James, 2020). In the absence of better domestic rules, including on taxation of international technology firms, gaps in income and privacy issues are likely to grow, entrenching dependencies (Kilic and Avila, 2019; Raghavan, 2018). Consequently, a slower pace in policymaking could ensure a fairer distribution of gains from data (Trade Justice Movement, 2020).

Mayer (2020) supports a cautious approach towards free outflow of data on consumer preferences from developing countries. From a data-driven industrial policy perspective, domestic firms could use data on consumer preferences in manufacturing to develop new products that serve new internal market segments. This type of industrial policy would limit outflows of certain data, and thereby aim to support economic development with less reliance on export-oriented industrialization. Similarly, Singh (2019) highlights the need for an industrial policy to ensure that domestic data contribute to value creation within the country to support digital industry development. Foster and Azmeh (2020) and Ciuriak (2018) also emphasize the relevance of industrial policy for development in the data-driven digital economy.

By contrast, Mitchell and Mishra (2019) question whether the digital divide can be bridged if developing countries have no access to international, relatively cheap digital services. They acknowledge, however, the skewed distribution of intellectual property and enabling technologies to benefit from data that are predominantly owned by firms in developed countries, which might make industrial policy in a data context attractive.

F. SCOPE OF RESEARCH

Trade and business concerns are at the centre of a large share of the current literature. Consequently, it is relatively narrow in focus and analysis, as it does not consider other dimensions of data. As this research often aligns with free trade support and integrated global markets, the arguments regarding cross-border data flows are equally geared towards these outcomes.

Spiezia and Tscheke (2020) analyse the effect of joint membership to international data agreements on trade in services and goods. While focusing on trade in their empirical analysis, the authors acknowledge the limitations, as data are not only linked to trade. They weigh the challenge of identifying value associated with data flows and measuring it appropriately, while acknowledging the difficulty of putting a correct valuation on other factors, such as privacy. In line with the concern for privacy, Mattoo and Meltzer (2018) analyse different regulatory options to determine the best one to allow for free flows of data, while protecting personal data privacy. They favour country-specific privacy regulations. Hence, the authors are against the inclusion of data privacy components within FTAs. Rather, they favour specific international cooperation agreements between regulators, such as the now-ineffective European Union–United States Privacy Shield. Similarly, Nguyen and Paczos (2020) set out to assess the economic value of data flows, which shapes their arguments towards the positive impacts of these flows.

The T20 policy brief on the free flow of data finds its discussion on microeconomic theory, where the invisible hand of a market contributes to its equilibrium (Chen et al., 2019). Hence, without market failures, free flow of data would be the optimal path to take. Any policy intervention that prevents free flows of data is only justified to address market failures, such as imperfect competition; or non-economic arguments, such as social issues, including privacy and security concerns. Accordingly, the policy brief first outlines how free data flows represent the best option, and as a second-best, regulations might have to be considered.

Tomiura et al. (2019) set out to survey the effect of regulations of cross-border data flows on Japanese firms. They take no apparent position towards restrictions. The survey's aim is to determine the

importance of data flows for the surveyed firms. However, the phrasing of the survey suggests an implicit favouring of free international data flows. It only assesses negative impacts of regulation on data transfers, by asking whether business with regions under regulation was reduced, deviated elsewhere or stopped. Given the adequacy status of Japan with the European Union, it might also have led to more data exchange, in line with findings in Spiezia and Tscheke (2020).

Some empirical analyses seem to assume at the outset that data regulations have adverse effects on trade and GDP, and that measures to limit data flows constitute a threat to the foundational idea of the Internet (Chander and Lê, 2015; McLaughlin and Castro, 2019). A number of studies also refute the point that restricting international data flows is a way to support the development of a local data industry; it would instead tend to raise costs for local firms, in particular smaller ones; limit choices for consumers; and threaten data security (Badran, 2018; Chander and Lê, 2015; Cory, 2017; McLaughlin and Castro, 2019; Castro and McQuinn, 2015). Overall, the discussion is too focused and limited towards emphasizing negative effects.

Business associations and private sector players focus their arguments even more, presumably with a view to support their interests. The premise is that cross-border data flows need to be supported in the best manner possible. Consequently, they present policy briefs, often providing limited empirical evidence or analyses, rather than weighing advantages and disadvantages. The Federation of German Industries sees data as the key enabler of Industry 4.0, for which frictionless data flows are essential to maintain their members' competitiveness. Thus, any FTA should limit data restrictions, which the Federation considers a new form of protectionism (BDI, 2017). Similarly, the Global Data Alliance outlines policy areas – cybersecurity, privacy and law enforcement – that it supports to build consumer trust and enable businesses, innovation and growth in all sectors (Global Data Alliance, 2020). GSMA, the association of mobile network providers, sets the direction of its argument in the title of one of its publications, “Cross-Border Data Flows: Realising benefits and removing barriers” (GSMA, 2018a). It posits that data flows give individuals, businesses and organizations more options, by increasing consumer choice and reducing operational costs of network operators working across borders. However, mobile operators are subject to specific rules that limit their possibilities for using these economies of scale across borders, due to data localization measures for network data (GSMA, 2018b). In a similar vein, Microsoft puts forward reasons why a sound cloud infrastructure supports many of today's major societal, economic and environmental challenges, and outlines a policy road map (Microsoft, 2018). One common missing point in these perspectives is that they do not look at the distributional impacts of the benefits of cross-border data flows.

However, while a lot of the research favours free cross-border data flows to support trade – and in turn productivity, innovation and GDP – Aaronson (2014, 2019a) takes a broader approach by considering the value of an open Internet in itself to be part of human rights, foreign policy and security issues (Aaronson, 2014). Furthermore, Aaronson (2019a) looks at the role of data as an economic resource more broadly than the often-used analogy of “data is the new oil”. Additionally, she illustrates how data governance is still a patchwork, which requires that Governments develop a new approach to tackle the governance of these flows. This could then provide a framework to advance Internet freedom through clearer guidelines, which most regulation and FTAs to date neglect (Aaronson, 2014).

In conclusion, most of the literature fails to broadly assess the role of cross-border data flows in the economy and society, and their possible benefits and disadvantages in a balanced manner. Instead, most studies seem to be aligned with a predetermined outcome, which is sometimes specifically stated, but often left for the reader to identify.

G. DEVELOPMENT PERSPECTIVE OF CROSS-BORDER DATA FLOWS

Thinking about cross-border data flows is closely entwined with supporting businesses with large data flows. This is reflected in the geographical and linguistic origin of frontier thinking on the issue. It is strongly dominated by anglophone authors from developed countries. Regulations are driven, to some

extent, by the need to secure a competitive advantage of national players (Aaronson and Maxim, 2013). Research correlates with this need.

As developed countries dominate the research, there are relatively few examples of publications that focus on the development perspective on data flows. To date, developing countries have been more consumers than producers in the data-driven economy (Aaronson, 2019a) or are likely to be taken advantage of (Hilbig, 2018). Remaining digital divides, in particular with respect to capacity to use data-driven approaches in economic development, give developed countries a head start in creating data insights and value while data flow freely across borders (Mayer, 2020).

Investigating five African countries, Badran (2018) estimates that the impact of data localization is sizably smaller than for European Union countries. Although this sounds positive initially, it is likely driven by fewer links and trade relationships with other countries, which is not ideal for long-term economic development. Additionally, adverse effects of data localization in Africa might be particularly high because unreliable energy supply makes local data centres costly to run.

Aaronson (2019a) notes that contributing to the development of data governance frameworks at the global level can be challenging for developing countries, as many are still missing the appropriate norms, rules and regulations, as well as infrastructure, for a data-driven economy. Without a national level plan, it is difficult for policymakers to take a stand in the international debate and, for instance, support the development of interoperable standards that allow countries to pursue their own strategies (Aaronson, 2014; Cory, 2017, 2019; Hill, 2018; Mattoo and Meltzer, 2018; Meltzer, 2020; Microsoft, 2018). With the United States and the European Union putting forward strong rules on either free flow of data or data protection, respectively, developing countries may be caught in the middle, feeling obliged to fall in line with either of the approaches, as they have less bargaining power (Aaronson and Maxim, 2013). The World Bank (2021) emphasizes the need for low-income countries to be better included in digital trade and data governance negotiations; the outcome should not put too much regulatory, financial and capacity burden on countries, to ensure that new rules can be enforced.

Some studies, however, consider the opportunities for developing countries. The implicit development angle in Cory (2019) is that innovation is spurred by the exchange of ideas and data, as well as access to cheaper solutions, such as cloud software. Hence, developing countries would benefit from regulations that maximize innovation potential by allowing the free flow of data. This view aligns with Chen et al. (2019). The authors point out that, as people in developing countries increasingly make use of data-intensive communications technology, their need for a regulatory framework is rising in order for them to harness this potential for economic growth.

Regarding developing countries, most of the debate around cross-border data flows and development focuses on India, which has a relatively large digital service industry, with strong links abroad. The Indian states with larger information technology sectors have higher standards of living and attract more foreign direct investment. Likewise, higher digital services exports are associated with more innovation in terms of patents filed and number of start-ups. Hence, India is an illustration of benefits arising from free data flows. Modelling data restrictions, CUTS International (Gupta et al., 2020) concludes that they are adverse to development, leading to a sizable loss in digital service exports and GDP. However, using India as an example to derive insights on development of other countries might have limited validity. The country's large size and well-educated and English-speaking middle class are key factors that prevent replication of the Indian experience in many other countries. These countries may be limited by their small internal market, which hinders them from building a modern domestic digital economy (Deardorff, 2017; World Bank, 2021).

Some research acknowledges that there are differences between countries' readiness, but does not go into any discussion on how developing countries might be differently affected by certain data governance approaches to these flows, or how they can be effective drivers of development (BSA, 2017; McKinsey, 2014).

As long as developing countries are not able to drive their own development in the digital sphere, limited capabilities and financial means create a new dependency. This so-called digital colonialism involves

actions by major technology firms to shape the policy debate in their favour through lobbying, investments in infrastructure, and donations of hardware and software to developing countries (Avila, 2020).

Consequently, the ability of a country to make its own decisions in shaping policies on data and data flows – their data sovereignty – is gaining in importance (Hilbig, 2018; McLaughlin and Castro, 2019; Avila, 2020; Taylor, 2020), although the definition and motivation of data sovereignty can vary widely across countries (De La Chapelle and Porciuncula, 2021). To put this independence into practice, several authors propose policy road maps to build better data governance and enabling environments (Aaronson, 2019a; Ademuyiwa and Adeniran, 2020; Chen et al., 2019; GSMA, 2018b; WEF, 2020b). Moreover, within countries, there is the suggestion of multistakeholder approaches to shape the governance framework along the priorities of businesses and other actors. Consequently, several publications focus their road maps on privacy frameworks, cloud-enabling environments and globally facilitating the flow of data across borders (GSMA, 2018b; Microsoft, 2018; WEF, 2020b). Their angle on development is to acknowledge that the journey towards the best regulatory environment is country-specific. A major concern in realizing benefits from up-to-date rules and regulation is limited capacity in terms of relevant expertise, as confirmed by policymakers surveyed in Asia (GSMA, 2018b). By contrast, WEF (2020b) proposes a very high-level road map, leaving out details on its implementation. Ademuyiwa and Adeniran (2020) specifically analyse data governance concerns that African countries should address to build digital sectors, digitalize their economies and integrate into the global data value chain, to benefit from the digital economy. They emphasize the role of rules and regulation on antitrust, competition, taxation, data privacy and security, as well as skills.

International cooperation on cross-border data flows is also a key issue. While it is important for countries to have regulatory space to develop rules that fit their individual needs, the international nature of data flows calls for cooperation. Aaronson (2019a) calls for an international organization that supports cross-border data flows and helps develop common standards that facilitate them across countries. This is echoed by GSMA (2018a), which suggests that legislating these flows might be better done at a regional level, to create areas with few limitations, such as in the European Union.

Most of the limited literature that includes a development perspective is in English, and mainly produced by experts from advanced countries. For instance, in the case of Latin America, studies that consider cross-border data flows in the context of analyses on digital trade have been produced by Cory and Castro (2018), Meltzer (2018) and Suominen (2018). Aguerre (2019) conducts one of the few studies by a Latin American expert. Perspectives from other languages and domains could also be helpful in extending the reach of the debate. For example, there are some interesting works in relation to the geography of data in French, such as that by Cattaruzza (2019).

H. DRAWBACKS OF THE CURRENT LITERATURE

While there are positive trends in the literature that can contribute to policy discussions, there are also certain weaknesses. One concern is implicit assumptions that many authors make before they argue their case based on these assumptions. The foremost assumption is that restrictions of data flows are undesirable. For instance, Tomiura et al. (2019) survey only adverse effects of data regulation. While this would be correct based on economic theory, with the underlying assumption that the market leads to efficient outcomes, it neglects the presence of market imperfections – such as monopolistic tendencies or societal values – that might generate other outcomes. From a more technical perspective, the assumptions underlying general equilibrium models and their calibrations may limit the generalizability of the findings to different country samples (Badran, 2018; Bauer et al., 2013, 2016; Ferracane and van der Marel, 2020; Ferracane et al., 2020).

Defining data better – and the areas of economies, societies and the overall environment they touch upon – is important to further the discussions on measurement, as well as on their policy implications. One of these discussions relates to data flows as a form of trade, and whether FTAs should legislate internationally the flow of data across borders. A sizable share of research focuses on data and trade, especially with respect to shaping international rules within trade negotiations (Aaronson, 2014; Bauer

et al., 2013; BDI, 2017; Castro and McQuinn, 2015; Cory, 2017; Microsoft, 2018; Nicholson and Noonan, 2017). This is certainly an important topic for cross-border data flows. However, both Burri (2016) and Mattoo and Meltzer (2018) reject the idea that these flows should be negotiated within the realm of trade negotiations, as they are either too one-sided or leave out relevant actors, such as the Internet governance community.

Defining data rights is also relevant to making data and data flows more tractable. With the growing role of cross-border data flows, Linden and Dahlberg (2016) analyse whether the free movement of data should become one of the “free movements” that are at the centre of the internal market of the European Union. This would put data on the same footing as freedom of movement for goods, services, capital and people. While they conclude that free data flows might be more of a subsidiary freedom, having these open discussions on the nature of data flows is vital to better delineate the topic.

Furthermore, as outlined above, the development perspective is not well covered in the literature. This comes with the added challenge that certain propositions for data governance might not be easily implementable for every country. McLaughlin and Castro (2019) and Hilbig (2018) call for countries’ sovereignty in legislating on data, without offering ideas on how this could be achieved. Similarly, the call for an appropriate amount of data protection leaves out the answer to how one might assess this amount (Global Data Alliance, 2020). Finally, some of the policy road maps might be difficult to implement, as they require ideas on how to bridge the gap in capacity to introduce and guide the policy process (Ademuyiwa and Adeniran, 2020; Microsoft, 2018; WEF, 2020b).

I. CONCLUSION AND OUTLOOK

The review of the literature presented in this chapter reveals several limitations and gaps:

- The current literature is still struggling to define data and cross-border data flows, hampering constructive discussion on their governance.
- There are significant problems of measurement of cross-border data flows.
- There is little literature on the different types of data, and taxonomies used do not properly address the implications that different categorizations may have with regard to cross-border data flows.
- Most of the literature analyses cross-border data flows from a trade perspective. Some of it looks at cross-border privacy issues, but there is a general lack of studies that address cross-border data flows in a multidimensional manner.
- Balanced analyses pondering the advantages and disadvantages of different policy options regarding cross-border data flows are rare. Many studies have clear ideological leanings and implicit assumptions upon which they base their arguments. Studies tend to start with a predetermined position towards free data flows on the one side, or data localization on the other. In those cases, the objective of the research is mainly to justify the position taken.
- From a development perspective, there is little evidence that backs positions in support of either free cross-border data flows or strict data localization policies. Most studies favouring free flows seek to estimate the negative impact of data flow restrictions in terms of opportunity cost. However, such an approach may fail to incorporate equity and distributional issues related to who appropriates the gains. They may also fail to factor in the non-economic dimensions of data, such as privacy and security.
- At the same time, the case for strict data localization policies in support of domestic development is weak. It is not evident that keeping data inside national borders results in economic or social development.
- The lack of evidence in either direction is partly related to measurement problems, and partly to the fact that the data-driven digital economy and the exploding cross-border data flows are relatively recent phenomena.

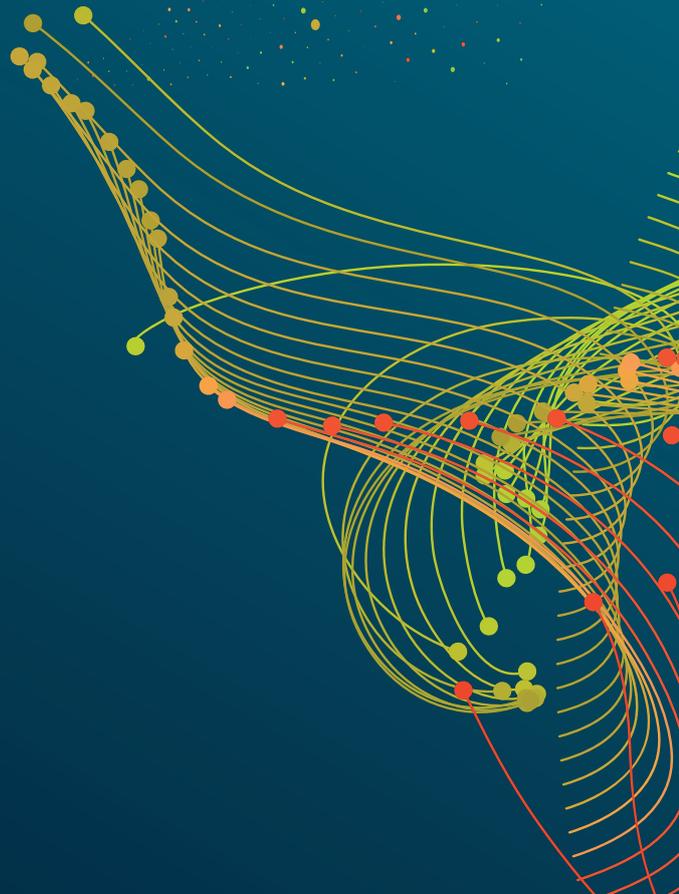
- The literature comprises mainly anglophone studies, published predominantly in developed countries or, when focusing on the developing world, mostly on India.
- Last, but not least, there is little focus on the relationship between cross-border data flows and development. And quite often, when the development perspective is introduced, it is analysed by experts from developed countries. Apart from India, there are few studies on the topic produced in developing countries.

Overall, these conclusions indicate significant gaps in the literature on cross-border data flows and development, which also influence the policy debates. Against this background, the next chapter takes a step back, and seeks to lay some foundations for a broader and more inclusive analysis of cross-border data flows.

In view of the gaps in the literature and debates on cross-border data flows highlighted in chapter II, this chapter goes back to the basics of data and their flows across borders. This means revisiting their definitions, concepts and characteristics. Without a common understanding of what data and cross-border data flows are, and the complex interconnections involved in the data economy, it is difficult to agree on their implications, or on what policies should be put in place, with a view to harnessing data for development.

The chapter underlines that data are multidimensional, which calls for a holistic approach to their governance. Building on the trends analysis in chapter I, it notes that data can generate both private and social value, but that value creation requires access to large quantities of data, and the necessary capacities and skills to develop them into digital intelligence. The outcome depends on, among other things, the type of data involved, and how they are collected, analysed and shared. Existing power imbalances and inequalities regarding cross-border data flows raise concerns about the possible implications for developing countries.

BACK TO BASICS: ISSUES AT STAKE



CHAPTER III WHAT DATA AND CROSS-BORDER DATA FLOWS ARE AND THEIR IMPLICATIONS FOR DEVELOPMENT

Data are multidimensional

Economic dimension

Collect



Store



Analyse



Private value

(e.g. through targeted online advertising, digital platforms, data services)

Social value

(e.g. climate change, health)

Non-economic dimension



Privacy



Other human rights



Security

Data are **different from goods and services**, and their flows are different from trade

Rather than data ownership, what matters are **rights to access, control and use data**

Data access and use are key for **development**

Countries are at **different levels of readiness** in terms of capacity to harness data for development

Issues at stake

Implications of cross-border data flows vary by **data type**

Where to **locate data** depends on various factors that need to be assessed

A few **global digital corporations** have **privileged access** to data and **unique capabilities** to turn data into digital intelligence

Developing countries risk becoming **mere providers of data**, while having to pay for digital intelligence produced with their data

Maximize the gain from the data economy, while **minimizing the risks** involved

Ensure an **equitable distribution** of benefits

Consider the **complex policy trade-offs**

Public policies are needed

Oversimplification by calling for free data flows or for strict data localization is unlikely to be useful: **Middle-ground solutions** are needed

Global data governance needs to take a holistic, multidimensional, whole-of-government and multi-stakeholder approach

A. INTRODUCTION

The relationship between data and development can be understood in two different, but interconnected and equally important, ways. First, data can be used to inform decisions and processes towards the attainment of economic, social and environmental goals. From this perspective, the relationship between the use of data and development is quite straightforward. Increases in the availability of data resulting from progress in digital technologies can significantly help in advancing towards the achievement of the Sustainable Development Goals, by providing enhanced evidence for decision-making. This is illustrated in different cases related to poverty reduction, health, environment and climate change issues, transport, energy or agriculture (World Bank, 2021).

Second, data can be part of the economic development processes themselves, as part of the data value chain, as they have become a key economic resource. In this sense, development occurs as a result of value addition to data through processing the raw data to convert them into digital intelligence (data product). Data for development here are about the role that data can play as an engine for development, in terms of domestic economic value addition in developing countries, which is what economic development is. In this context, ensuring development gains from data becomes a more complicated task.

In terms of economic development, it is important to ensure that developing countries are able to properly capture the value of the data extracted from their citizens and organizations.

As data have become the lifeblood of the digital economy, and they can provide significant developmental benefits to different economic agents – but most importantly, due to their nature as a public good, for society as a whole – the sharing of data is desirable for strengthening their positive effects, while addressing possible risks (OECD, 2019a). Sharing of data in the form of increased access for most citizens to maximize the potential gains to the extent possible implies that data need to flow, not only domestically but also internationally. In this context, it is important to look at various types of data that may have different implications in terms of access, including for data crossing borders.

In terms of economic development, it is important to ensure that developing countries are able to properly capture the value of the data extracted from their citizens and organizations. The economic benefits of data and cross-border data flows are not automatic, nor evenly distributed, between and within countries (UNCTAD, 2019a); the free play of market forces does not lead to efficient and equitable outcomes. Thus, public policies have an important role to play. In the absence of a proper international system of regulations on cross-border data flows, global digital platforms and lead firms of global value chains have privileged access to and control of huge amounts of data, and are in a particularly good position to appropriate potential gains; they can also foreclose potential social gains by limiting data access. This has significant impacts on inequality, and affects development prospects. Thus, from the economic perspective, it is important to look at private as well as social value from data, but also at the distribution of the value created from data, within and between countries, so that it is equitable.

Data have significant impacts not only in terms of economic value; it is also necessary to look at non-economic aspects related to data which, having important effects on individuals and society, cannot be delinked from the economy due to the particular nature of data. Cross-border data flows have many complex implications in various domains that need to be deeply explored and understood in order for them to be addressed for development purposes. There may be legitimate reasons for data to remain within national borders, in addition to ensuring that the domestic economy can properly benefit from these flows, including the protection of privacy and other human rights, as well as security issues. There are also significant challenges emerging from abuse and misuse of data that need to be taken into account. The need to minimize these risks and challenges, which largely affect users' trust, points in the direction of protecting data through different safeguards and policies to control cross-border data flows.

Data and data flows, both domestic and international, can therefore bring many benefits, which should be promoted and distributed in an equitable manner, instead of being captured by a few firms and countries. At the same time, there are many risks and challenges that need to be carefully addressed. All of these affect individuals, who are increasingly at the origin of the data, and private firms, both big and small, as well as Governments and civil society. It is therefore important for all to deeply reflect on what the main issues at stake are in relation to data and cross-border data flows from the development perspective, and what the implications for policymaking are. Exploring the multiple interconnections and underlying links between data and development is crucial to enhancing policy-relevant understanding of cross-border data flows.

• Data and cross-border data flows can bring many benefits, which should be equitably distributed, instead of being captured by a few firms and countries, while many risks and challenges need to be carefully addressed.

Against this background, and in view of the gaps in the literature and debates on cross-border data flows highlighted in chapter II, the present chapter takes a step back, with a view to deepening the understanding of major issues of relevance in connection with cross-border data flows and development, starting from the basics. In fact, the starting point is the definition and characteristics of data presented in chapter I, which the present chapter develops further. Section B looks at the ways data are collected and used. Section C then discusses the different dimensions of data that add significant complexities to the analysis of data and cross-border data flows. Issues related to ownership of, access to control of and rights over data are explored in section D. Section E discusses the way data flow and the relevance of the location of data storage, while section F looks at different types of data and their implications for cross-border data flows. Section G discusses power imbalances and inequalities resulting from cross-border data flows. The position of developing countries in the international data value chain is explored in section H. Sovereignty issues that emerge in connection with these flows, at different levels, are addressed in section I. Section J highlights the conflicting interests and policy trade-offs that emerge in this context. Section K then looks at the capacities needed to benefit from data, before the conclusions are presented in section L.

B. DATA COLLECTION, PROFILING AND USE

Any data flowing over the Internet can be collected. As discussed in chapter I, data can be collected through different channels, including through web browsers, mobile applications or Internet of Things (IoT) devices. These can include personal data, but also geospatial data, weather data, sensor data (machine-to-machine) and traffic data, among others. These data can be volunteered, as in the case of personal information for registration for a web service, or data from a web survey. However, often the data collected and analysed are observed data, such as web visits, location or Internet Protocol (IP) address, but they may also include technical information about the connected device, such as its operating system or media access control address. With the right access, it is also possible to intercept any data sent over the Internet, such as emails or other text messages, voice or video messages, or communication from IoT devices, such as connected refrigerators or doorbells.¹

For some purposes, it is important to collect data that can be used as identifiers (something to tie information to a particular person). Identifiers are data that point to a specific person or device (unique), do not easily change (persistent) and are easily accessible (available).² Not all identifiers will check all three

¹ This is why data transfers are increasingly encrypted – for example, with the move from non-secure HTTP (Hypertext Transfer Protocol) to the more secure HTTPS (Hypertext Transfer Protocol Secure).

² See Electronic Frontier Foundation, 2 December 2019, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, available at www.eff.org/wp/behind-the-one-way-mirror.

boxes, but some that do might be a name, an email address or a phone number. Identification is critical for determining the degree of anonymization of the data, which is relevant for the distinction between personal and non-personal data. However, although the technology for anonymizing data is progressing, the extent to which data can be anonymized remains a controversial question, as discussed below.

Data can be collected for different reasons – such as product and service development, targeted advertising and surveillance – and its authorization may be based on service agreements, use policies, legal requirements or requests. Without relying on any other party, data can be collected by entities that own, control or have access to key Internet infrastructure (for example, Internet exchange points (IXPs)), websites, web servers, or software (operating systems and applications). These entities include website owners, e-commerce or social media platforms, application developers, operating software developers, Internet service providers (ISPs), Governments and hackers. Data can also be obtained indirectly through, for instance, data brokers, court orders or other legal requests, or be bought on the dark web.

In the context of the data economy, a new vocabulary emerges and a whole new plethora of relevant actors appears. These include data subjects, who can be defined as the identified or identifiable living individual (or entities) to whom personal data relate;³ and data brokers, businesses that aggregate information from a variety of sources, process it to enrich, clean or analyse it, and license it to other organizations.⁴ Other data-related actors are data aggregators, data analysts and data controllers, who determine the purposes for which and the means by which personal data are processed.⁵

A relevant question that arises in connection to data collection and tracking is to what extent the massive amounts of data collected are necessary for the operation of the services, or whether there is overcollection of data.

In terms of data collection for commercial purposes, a distinction can be made between first-party and third-party data collection and tracking. The biggest online platforms collect vast amounts of data whenever their services are used. The collection of data by companies through their own products and services is called “first-party tracking”. These data may be collected as part of implicit or explicit consent. However, data may also be collected by parties other than the website or service the user directly interacts with, known as “third-party tracking”. For instance, Facebook also collects information about users of other websites and apps with its invisible “conversion pixels”, and Google uses location data to track user visits to brick-and-mortar stores.⁶ In fact, there are many data brokers and online advertising agencies that track day-to-day web browsing and device use. Most third-party tracking is designed to build profiles of people and entities that can be used for targeted advertising. Some of the more common ways in which Internet tracking takes place are detailed in box III.1. Certain major digital platforms are undertaking revisions of tracking practices, which may have implications in terms of privacy and competition; the positive impact of these changes on privacy remains to be seen.

A relevant question that arises in connection to data collection and tracking is to what extent the massive amounts of data collected are necessary for the operation of the services, or whether there is overcollection of data. This is important because a large part of the data is observed data, often collected without the consent or knowledge of the user. It may be argued that, by accepting the conditions of

³ This concept has been generalized with the General Data Protection Regulation. Other regulations may use different terms. For example, in India, the data subject is the data principal.

⁴ See definitions, available at <https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/#subject> and www.gartner.com/en/information-technology/glossary/data-broker.

⁵ See European Commission, “What is a data controller or a data processor?” Available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en.

⁶ See footnote 58.

Box III.1. Internet tracking

The tracking of online behaviour can take many forms, and tools and techniques are constantly evolving. The following are some of the most common methods currently in use:

Tracking cookies

A cookie is information saved by a web browser when someone visits a website, so that it can recognize the device in the future. Cookies can have different purposes, one of which is to track a user's online behaviour – for example, to customize the browsing experience or to deliver targeted advertisement. Tracking cookies can be placed by the target website (first-party cookies) or by its partners (third-party cookies) and contain identifications that allow them to identify users and track them online. Every time a user reconnects to a website, the browser will send back the cookie's information, such as clicks, shopping preferences, device specifications, locations and search history. In recent years, the use of third-party cookies has come under scrutiny and is being blocked by some of the most-used browsers, including Mozilla Firefox, Safari and soon Google Chrome as well.

Web beacons

Web beacons are tiny, single-pixel images that track user behaviour on websites or emails. When opening a webpage or email that has such beacons embedded, the browser or email reader will download the image, requiring the device to send a request to the server where the image is stored. This automatic request will provide information that can be used to obtain information about the user's device, such as its IP address, the time the request was made, the type of web browser or email reader that made the request, and the existence of cookies previously sent by the host server. The host server can store all of this information and associate it with information from other trackers or identifiers.

Device fingerprinting

An even more intrusive form of tracking is browser fingerprinting or device fingerprinting. This refers to the collection of information about the hardware and software of a particular device. This information is collected through a script (a list of commands that are executed by a certain programme) that runs in the background when visiting a website. These scripts can determine the operating system of the device, the browser or other installed software, the use of an ad blocker, time zone, language, the screen's resolution and colour depth, installed browser extensions, and even more granular technical specifications about graphics card and drivers. All these different attributes taken together will provide a unique fingerprint with which the device can be identified and tracked, even without using cookies, or when the IP address is hidden.

Mobile devices

Similar techniques are used to track the use of applications on mobile devices. Even though mobile apps cannot access cookies the same way web-based trackers can, they can take advantage of the way mobile operating systems work and access unique identifiers that let them tie activity back to a specific device. Moreover, in mobile apps, it is not possible to grant privilege without granting the same privilege to all of the third-party code running inside it. Some mobile operating systems, such as Apple's iOS 14.5 update, have recently started to include an option for users to block application tracking.

ISP tracking

Apart from tracking by first- and third-party websites, online activities can also be monitored by ISPs, as all of a user's traffic is routed through its ISP's servers. By analysing NetFlow information, an ISP can gather information about the website that is being visited, the time spent on a website, and other basic information about the connection and type of data that are being transferred. Deep packet inspection (DPI) can give the ISP even more information. As long as a website does not use encrypted communication, the ISP can monitor basically everything – including username and passwords, products that are being purchased, and credit card numbers and addresses – when entered for payment and delivery. Even when one visits a website using encrypted communication, the ISP will still be able to know the target website. Additionally, an ISP can analyse the Internet traffic and its metadata, such as the size, type, timing and destination of data packets. This means that ISPs can potentially collect more personal data than Facebook or Google.

Source: UNCTAD, based on Electronic Frontier Foundation, 2 December 2019, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, available at www.eff.org/wp/behind-the-one-way-mirror; TechCrunch, 19 June 2020, Oracle's BlueKai tracks you across the web. That data spilled online, available at <https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/>; Avast, 14 May 2021, Data Brokers: Everything You Need to Know, available at www.avast.com/c-data-brokers; United States Federal Trade Commission Consumer Information, May 2021. How To Protect Your Privacy Online, available at <https://www.consumer.ftc.gov/articles/how-protect-your-privacy-online>; Goodwill Community Foundation, Understanding browser tracking, available at <https://edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/>; Proton Technologies AG, How to protect your data from your ISP, available at <https://protonvpn.com/blog/is-your-isp-selling-your-data/>; StackExchange, My ISP uses deep packet inspection; what can they observe? Available at <https://security.stackexchange.com/questions/155057/my-isp-uses-deep-packet-inspection-what-can-they-observe>.

service, the user has agreed to such data collection. However, this supposedly “informed” consent is highly debatable, given the opaque way in which the conditions of services are usually presented, very often in long and complex language. Moreover, the consent is presented in a take-it-or-leave-it manner, so that the user has no other choice but to accept the conditions. In principle, the conditions of service should be simpler and clearer for users to know what they have agreed to, and they should work in such a way that there is not excessive collection of unnecessary data. The latter is, however, rather difficult, because data have “option” or potential value, which only materializes once the data are processed and used. Thus, some data collection is speculative and done without the exact knowledge of how they can be used later. There will always remain a trade-off between consent practices and innovation in data-driven services.

While data collection and tracking already raise questions, what matters most is their purpose – what the data are used for – which is what will determine their value, as well as both their positive and negative effects for individuals and society. As mentioned above, data can be used for developmental purposes, including for overall increases in efficiency and productivity. Data are an essential ingredient to feed artificial intelligence (AI), and are used to create profiles on people or entities. The data, the insights generated from them and the profiles created can be used by companies and organizations to improve their products and personalize their services, enhancing the experience of the customers, as well as for advertising purposes. In this way, companies collecting the data can generate significant profits by monetizing data. On the negative effects side, companies, as well as Governments, that control the data can manipulate experiences and opinions through the use of attention and behavioural economics tools, which can lead to undesired impacts for society. In this way, these profiles can involve abuse and misuse of the data. This can have an impact, for example, in terms of discrimination, as these profiles can be used for different activities – such as hiring, insurance, bank lending and social services – in very opaque ways. Discrimination may also emerge in terms of gender and race, as data and algorithms may be biased. Indeed, the availability of huge quantities of data is key for producing valuable digital intelligence, but the quality of this digital intelligence also hinges on the quality of the data on which it is based.

Overall, by being “converted” into data as more and more of their activities and events become digitalized in what has come to be called the “surveillance economy” (Clarke, 2019), people become the product. The digital intelligence derived from the data becomes merchandise and, as data reflect the activities and behaviours of the people, the latter also become in a way assimilated to merchandise. Thus, through digitalization, the world is moving from a market economy to a market society, as it allows the market to extend to more and more aspects of life.

C. THE MULTIDIMENSIONAL CHARACTER OF DATA

A proper understanding of the role of data in the economy and society, and their fundamental properties, requires looking at their different dimensions. This section highlights the multidimensional character of data, not only as an economic resource, both for private and social value, but also in relation to non-economic aspects – such as privacy and other human rights, and security. In all their dimensions, which are interconnected and need to be seen as a whole, data have become a strategic resource for individuals, firms and countries. Since they cannot be disentangled, proper policymaking implies avoiding addressing data issues with a silo approach, although different policy emphases may be put on each of the dimensions according to policy choices, while considering cross-dimensional impacts.

1. The economic dimension of data

A key idea underlying much of the discussion on data is that they have become a key *economic resource*. The digital economy is increasingly being defined by intangibles, where new aspects of organizations – such as knowledge, intellectual property and digital code – are now central to competitive advantage (Haskel and Westlake, 2017). This encourages organizations to collect, combine and process ever more data to generate economic value (UNCTAD, 2019a; Mayer-Schönberger and Cukier, 2013). Data

have emerged as a particularly important resource to key business models in the digital economy. For example, platform business models rely on data, and through analysis lead to virtuous circles of data-driven improvements and further production of data (Gawer, 2014). Business models revolving around AI and algorithms cannot exist without data that drive models and systems.

From this perspective, there can be different emphases on the fundamental economic aspects of data. Data can be seen as a *commodity* that can be traded; however, the potential tradability of data is highly debatable, particularly in what concerns raw data. There are difficulties in establishing property rights or data ownership, *inter alia*, because data are of a non-rival nature, which implies that many people can use them at the same time, and they are often a reflection of people and their behaviours (see below). Moreover, as individual raw data have only potential “option” value – because economic value in the data-driven digital economy materializes only after the raw data are aggregated and processed into data products and monetized through their use – there is no proper price discovery mechanism of the market for raw data. In addition, the value of data when used, once processed, is highly contextual. Thus, there are not properly developed and formalized raw data markets, which implies that these data cannot be directly bought or sold, and that there is no proper demand and supply. As the World Bank (2021:32) puts it, “although private bilateral market exchanges of data are well established in certain niches (specifically, trading personal data to target advertising), there are as of today no open multilateral markets for data, and many attempts to create such data markets have failed”. It is the digital intelligence resulting from the processing of data that can be monetized and commercialized; thus, references to data markets usually relate mostly to markets for these data products.

Beyond the private economic value of data, from the development perspective, it is also crucial to look at the social value of data.

Data can also be seen as *capital* (Sadowski, 2019; Tang, 2021), but once again it is mainly the digital intelligence that can be considered as capital, as an asset that can enhance the functioning of a firm and lead to wealth. Given the role that data are playing as a core aspect of decision-making in organizations and society, data may also be regarded as *infrastructure*, which is increasingly crucial to operations at the organizational, sectoral, regional or country level (OECD, 2015); this is highly related to the social value of data, discussed below (Kawalek and Bayat, 2017). Data can also be considered as *labour*, as they frequently represent activities undertaken by humans (Arrieta-Ibarra et al., 2018). While individuals generate much data, these are often captured, aggregated and processed by private firms. This mismatch between individual creation and firm control has led to a discussion about whether individuals receive fair compensation for their “free labour” of data creation. Such discussions have intensified as user data have become the foundation of profitability for many of the largest global digital corporations. The labour perspective on data might then lead to a closer consideration of individuals/producers of data – for example, by examining if they have sufficient bargaining power to gain a fair share of value for their labour (Aaronson, 2019a). This also has implications for taxation in the digital economy in terms of indicating where value is created and taxable, as digitalization complicates taxation of activities, given that physical presence is not necessary to carry out the activity.

Beyond the private economic value of data, from the development perspective, it is also crucial to look at the social value of data.⁷ As discussed in chapter I, data have special characteristics because they are non-rival, although they can have varying degrees of excludability. Data often involve externalities, which may be positive or negative. Most of the value of data is relational, resulting from the comparison or aggregation of data; individual data have no value. Due to data externalities, markets are likely to provide too little of those data that produce positive effects, and too much of those that create harmful

⁷ For a more detailed discussion on the social value of data, see the project of the Nuffield Foundation on “Valuing data: foundations for data policy”, available at www.nuffieldfoundation.org/project/valuing-data-foundations-for-data-policy. On the public good nature of data, see also MacFeely (2020a).

effects on society. Moreover, data are co-produced between the individual or entity that is at the origin of the data and the owner of the technology that collects the data. Thus, the value of data to the economy and society as a whole is different from the commercial value for private firms collecting and exploiting them: some types of data have public good characteristics. Treating data as a public good would also be justified by the fact that a large part of the technology used by digital corporations was the result of public research, and from network effects, which are collective. It would allow to shape the digital economy in a way that meets public needs (Mazzucato, 2018).

Moreover, as explored further below, data provide competitive advantages and strong market power to digital corporations, resulting in power imbalances and inequality. Consequently, market mechanisms are not likely to result in efficient or equitable outcomes for society, which leads to the need for public policymaking. Policies should aim to ensure that the creation of value from data, both private and social, is maximized and fairly distributed in society, nationally and internationally, while avoiding the potential risks that may be involved.

• Data provide competitive advantages and strong market power to digital corporations, resulting in power imbalances and inequality.

While maximizing the social value of data calls for increased sharing of data, and for public policies to enable it, data for the public good/interest can be collected or generated by both the private and public sectors. Public sector-generated data are normally shared with the wider society, through multiple open data initiatives around the world. When designing policies for data-sharing, as well as to regulate cross-border data flows, it will be important to distinguish whether it is the private sector or the Government that collects the data, because the treatment of the data and consequences differ.

In terms of cross-border data flows, what matters is whether the public good nature of data has implications beyond national borders. This implies that data generated in one country can also provide social value in other countries, which would call for sharing of data at the international level. In this context, different examples can be identified in relation to development challenges that are of a global nature. The COVID-19 pandemic situation has clearly shown the importance of sharing health data globally for coping with its consequences, and for research purposes in finding the vaccine. International sharing of data can also be useful for environmental purposes.⁸ Using data for addressing this kind of global challenges would call for enabling cross-border data flows. It should be taken into account, however, that at the international level, tackling the risks associated with data-sharing may become even more complicated. Moreover, at the international level, there is a need for public policies to address imbalances among countries that result from cross-border data flows.

2. Non-economic dimensions of data

The non-economic dimensions of data relate mainly to respect for human rights as well as to national security issues. The *human rights dimension* of data emerges by looking at the origin of data, and linking them to fundamental rights and protections, as data often represent activities and behaviours of users or entities. Wherever more swathes of data are held by organizations, the important question is how this interacts with fundamental human rights and the protection of individuals (Singh and Vipra, 2019). Specifically, there are underlying declarations on human rights, such as the United Nations Declaration of Human Rights, that include the right to privacy (Article 12), among others that are relevant to data (Heeks and Renken, 2018). In addition to privacy protection, the Secretary-General's Roadmap for Digital Cooperation (United Nations, 2020a) includes surveillance, repression, censorship and online

⁸ See, for instance, Jha and Germann (2020), and the Royal Society (2021) for health data, and UNEP (2020) on environmental data.

harassment as important human rights-related aspects with regard to data-driven digital technologies.⁹ Other human rights that are of relevance include freedom of opinion and expression (Article 19).

As data about individuals are generated in ever more granular ways, tensions can emerge between these fundamental rights and data held about individuals. Privacy should also be seen from a collective perspective, as data from an individual can reveal information about other people.¹⁰ A rights perspective on data would then focus on these human rights issues more prominently, exploring how fundamental human rights can be protected within the handling of an individual's data, and how individuals can assert their rights and control such processes. This human rights perspective is also reflected in issues related to discrimination – for example, in terms of gender and race – that AI, surveillance and manipulation of data techniques may create. Moreover, surveillance and data manipulation can affect democratic human rights and even influence political systems. Influence in politics can in turn translate into impacts in the economy, as economic policies applied depend on the elected political authorities and the political regimes.¹¹

The fact that data can be abused and misused by the organizations that control them, and affect human rights, be it by the private sector or by Governments, affects the trust of users and limits the potential benefits that may be derived from the data-driven digital economy. For example, doubts in connection to respect for human rights have been a factor limiting the use of contact tracing digital applications to help in fighting COVID-19 contagion.¹² Policies would do well to ensure that respect for human rights is guaranteed so that trust is increased. Moreover, from the private sector perspective, an approach that protects human rights in dealing with data may provide for a competitive advantage in terms of reputation.

• The multidimensional character of data, from the economic and non-economic perspective, highlights important aspects and views on data and data flows, which cannot be addressed in a disconnected manner.

Data also have a *security dimension* that needs to be considered. Data may represent activities that are of concern for national security and law enforcement, as well as national culture and values. As more and more activities become encoded within data, the nature of data flows therefore becomes a concern for those focused on security and enforcement. Ensuring security and protection of data produced by key organizations (such as the military or within critical infrastructure) increasingly plays a central role in national security. This perspective on data can often overlap with the economic perspective. For example, national security rules within countries with a stronger geopolitical focus might be concerned with protecting trade secrets and intellectual property of domestic organizations as much as with critical national activities.

As data become more prevalent, they also provide a means to track criminality and enforce laws. Therefore, accessibility and jurisdiction of data are becoming more important in law enforcement. Data can also overlap with domestic security questions. In some countries, data flows (for example, those that embed certain media or applications) might be counter to cultural or moral norms, or of a politically sensitive nature that leads to censorship.

⁹ See the work of the Office of the United Nations High Commissioner for Human Rights (OHCHR) on “the right to privacy in the digital age”, available at www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx. For other major international and regional human rights instruments in which the right to privacy is recognized, see Privacy International, 23 October 2017, What is Privacy? Available at <https://privacyinternational.org/explainer/56/what-privacy>. See also the OHCHR annual reports on Freedom of Opinion and Expression, available at www.ohchr.org/en/issues/freedomofopinion/pages/annual.aspx.

¹⁰ See, for instance, Véliz (2019) and Viljoen (2020), for more details on the collective nature of privacy.

¹¹ For a comprehensive account of the relationship between data and human rights, see Ebert, Busch and Wettstein (2020).

¹² See, for instance, Lewis (2020); Algorithm Watch, Digital contact tracing apps: do they actually work? A review of early evidence, available at <https://algorithmwatch.org/en/analysis-digital-contact-tracing-apps-2021/>; and Back et al. (2021).

In sum, this multidimensional character of data, from the economic and non-economic perspective, highlights important aspects and views on data and data flows, which cannot be addressed in a disconnected manner. Policymakers therefore need to look holistically at cross-border data flows, considering all the different dimensions. Certainly, different emphasis may be given to the various dimensions according to policy priorities, but it is important to recognize the impacts that any measure can have on each of the dimensions. For example, regulating cross-border data flows from only the trade perspective will not account for other factors related to privacy or security, which may most likely lead to inappropriate regulation. Understanding how different dimensions of data complement or come into tension with each other is crucial to a holistic analysis of data and data policy, including for cross-border data flows. While accounting for the multidimensional nature of data, it is important to ensure that the non-economic dimensions are not used as an excuse for implementing policies that have economic impacts and affect the development prospects of developing countries.

The multidimensional character of data also highlights the fact that it is difficult to come to tidy conclusions on cross-border data flows as a net positive or negative to developing countries. Data are rapidly copied, moved, aggregated and reused in different settings, having multiple uses at the same time. Data generated from a medical device, for example, might be used both to enhance an individual's treatment and feed into global health observatories supporting development; but at the same time, the same data can support the building of firm risk models that exclude the marginalized from health coverage.

D. OWNERSHIP, ACCESS, CONTROL AND RIGHTS OVER DATA

To understand the particular nature of data, it is also important to discuss issues of ownership, rights, access and control of data. While there is a wide debate on “ownership” of data, this is not the concept that really matters in relation to data. There are significant complications in establishing the legal regimes that apply to data (Correa, 2020)¹³ given their specific characteristics, including that they are intangible, non-rival, co-produced and their value is relational. In economic terms, this implies that there is a need to be careful about thinking of data as akin to conventional economic goods and drawing uncritically on models of economic scarcity, supply and demand. Indeed, as mentioned before, there is an absence of proper multilateral data markets in the case of (raw) data. These properties are also central to how data are defined; as a representation of a fact or idea in the world, data should not be seen as a conventional economic good that can be owned. However, data can be instilled within a set of rights – of use, of distribution, of modification – which should be shaped by norms and policy (Heverly, 2003).

More than ownership, what matters is the data rights – that is, the right to access, control and use the data.

Moreover, in relation to personal or collective data, data represent the individual (or the community for collective data) actions and behaviours. It may therefore be more important to think in terms of data rights, which are inalienable from or intrinsic to the individual (or the community). Thus, more than ownership, what matters is the data rights – that is, the right to access, control and use the data (UNCTAD, 2019a). Data rights offer the “right to access, to change, to move or to delete data; the right to know who's collecting it, where it is, where it's going, who has access to it, for what purposes”.¹⁴ In addition, the difficulties in applying ownership or property rights to data mean that they cannot be traded or exchanged, they can just be shared.

¹³ See also Cofone (2020) and Scassa (2018).

¹⁴ See Privacy International, 6 February 2019, We don't want to sell our data, we want data rights! Available at <https://privacyinternational.org/news-analysis/2683/we-dont-want-sell-our-data-we-want-data-rights>.

Key frameworks typically outline three major overlapping domains of data that are associated with different types of rights and control (Correa, 2020; OECD, 2020a): *public data*, used for public purposes, cover data that are intended to be used more openly and thus may be subject to fewer rights and control to support use and sharing;¹⁵ *personal data*, as a representation of facts or behaviours about individuals, overlap with fundamental human rights. Frameworks for personal data therefore look to determine how individuals can control and gain access to data collected about them (Duch-Brown et al., 2017); and *private corporate data*, which are proprietary data associated with organizations, are less defined by rights and more by control. Typically, organizations may control data through restricting access or use of data, retaining the scarcity of this economic resource. Where organizations trade, purchase or use data products from other organizations, they may be subject to commercial contract and licensing. As data have become more of an essential organizational resource and part of large investments in data-related capital, there has also been pressure to instil stronger “ownership” style rules on data to protect private investments.

Tensions can emerge at the intersection of these three core domains of data (OECD, 2015). Personal data that are gathered by the private sector are particularly challenging. On the one hand, broad swathes of online data embed identifying information about citizens, with individuals often voicing concerns about privacy and consent for gathering that data (Floridi, 2020). On the other hand, as proprietary data are core to firms’ competitive advantage, those firms wish to control the data in which they have invested. Similarly, there might be tensions emerging from commercial firms that have collected environmental data, with claims that such data should be in the public domain, given that they are representing facts about the world.

E. CROSS-BORDER DATA FLOWS, TRADE AND THE LOCATION OF DATA

Cross-border data flows refer to the transmission of data from one country to another. For this transmission to happen, data are divided into packets, which follow different routes inside the networks that form the Internet. As the Internet is a global network of networks, such data packets flow through a global, distributed infrastructure – that is, the transfer of data packets is “cross-border” in nature (Mishra, 2019). What determines that a data flow is cross-border is the origin of the user/client and the destination server. This may be the case of a Google search (request) by any user outside the United States, which is the origin, to Google in the United States, which is the destination. The global and distributed nature of data flows often complicates understanding of cross-border data flows; for instance, even if data are transferred between two digital devices within the same country, they may be routed through foreign server(s) for the purposes of economic or technological efficiency. Understanding how the Internet works is therefore essential when considering the relationship between cross-border data flows and development, and their policy implications. The annex to this chapter provides more details on how data flow across borders.

In order to gain a better picture of cross-border data flows, two key aspects are also discussed in this section: the similarities and differences between cross-border data flows and international trade, and issues related to the location of data.

1. Cross-border data flows versus international trade

The conceptual framework for measuring digital trade by the Organisation for Economic Co-operation and Development (OECD), the World Trade Organization (WTO) and the International Monetary Fund (IMF) highlights the ways that trade and data interact and differ. It notes that “Data flows that are not directly monetised are not generally considered as trade flows in current statistical standards; for example, personal information provided on social networks or data captured by firms within the ‘Internet of Things’” (OECD, WTO and IMF, 2020:24); thus, non-monetary information and data are not considered digital trade.

¹⁵ There appears to be a certain lack of clarity in the literature about the term “public data”. It may refer to data produced by the public sector just for use by policymakers, or for the use of society as a whole, becoming open data. Moreover, as mentioned in the discussion on data as a public good, data collected by the private sector can also be shared with the wider population and used for the public interest.

The particular characteristics of data discussed previously imply that they require a different treatment from conventional goods and services, including in what regards the international flow of data. Data can be better understood as shared rather than as owned or exchanged (Coyle et al., 2020), or traded. Traditional trade can be undertaken without significant data flows, but trade in goods or services is increasingly linked to cross-border data flows in some respects. In goods trade, the ordering and payment of goods or services may be done digitally. In the case of goods and services that become digitalized, these may not only be ordered, but also delivered online. Cross-border data flows can, however, be more loosely coupled to trade. Data flows may not be clearly associated with transactions and/or may be monetized in more indirect ways. Users may be able to use a foreign online service for free (such as search engines, social media, video streaming and web browsing), but during this process, data generated about them are extracted, processed and monetized – for example, through targeted advertising. Moreover, as products and services become integrated, enduring cross-border data flows may also be related to facilitating services on devices such as phones and sensors.

Whether they are coupled with trade flows or not, cross-border data flows differ vastly in their character, speed, regularity and ability to track. Cross-border data flows are often much less clearly associated with commercial transactions, and in many cases they are not. A mobile device, for instance, may transmit or receive data flows about its user over a long period simply by being switched on. The speed and regularity of cross-border data flows also lead to a very different character compared with international trade. A single user interaction in an app might result in a cascade of different cross-border data flows, including captured user data, data being requested from cloud storage, and data flows related to advertising and other uses, sometimes between a set of intermediate services and organizations. As data flows are “fluid and frequent, and location is hard to determine in a borderless network... trade in the same set of data can occur repeatedly in nanoseconds. Researchers and policymakers may find it hard to determine what is an import or export. They also struggle to ascertain when data are subject to domestic law... and what type of trans-border enforcement is appropriate” (Aaronson, 2019b:546–547).

In view of the different characteristics of data in comparison to goods and services and their multidimensional nature, cross-border data flows require a different treatment from trade in terms of their regulation.

International trade and other international economic flows are part of well-established systems of monitoring and measurement. But there is no clear way that trade approaches can be applied to those flows. Governing international trade is informed by statistics that rely on the types, values and locations of trading (source and destination) as a core way of regulating flows. Such approaches are challenging, if not impossible, to apply when tracking data flows, for which no official statistics exist. The technical characteristics of data flows – their frequency, their routing as packets across the Internet, and the role of intermediaries (such as platforms) involved in facilitating data flows – make it difficult to establish the origin and destination of data flows. Similarly, assessing the value of data and data flows is a daunting task, given that this value is mainly a potential “option” value, materializing only at use, and it is highly contextual. Moreover, data are most often the unpriced by-product of the production and consumption of goods and services, making it difficult to determine where value is created and captured (Slaughter and McCormick, 2021). Therefore, well-established approaches applied to international trade (for example, rules of origin) across different territories would not lend themselves to work well in the case of data, given the nature of data and cross-border data flows.

In view of the different characteristics of data in comparison to goods and services and the multidimensional nature of data, cross-border data flows require a different treatment from international trade in terms of their regulation. As opposed to trade, in many countries, certain types of data (such as non-personal or non-sensitive data, as discussed in the next section) can be sent through the Internet without registration, approval or permissions. Transmitting other types of data, including personal data, will link to legal accountability regimes. In this case, there will be no technical barriers to free flows,

but organizations will be expected to follow rules and are legally accountable if issues arise. Within recent personal data regulations, for instance, organizations are often required to formally register with regulators (see also chapter V).

2. The location of data

The location of data can be determined by a number of factors, which can be of a technical, economic, security, jurisdiction or privacy-related nature; it is also dependent on the availability and reliability of data-related infrastructure and energy to support it.¹⁶ Whether data flows are cross-border or not is often determined by the location of data storage. When interacting with a website or an application, the server where the content or application is hosted can be located anywhere in the world. Some of the online services own and operate their own data centres; others rent server space from other companies, such as Amazon Web Services, Microsoft Azure, Google or others. A server could also be located at an ISP, a small business or at home. In turn, the Internet server might store the data locally on its disk drives, or it might send the data to another server – usually, but not always, in the same location. As discussed in chapter I, increasing volumes of data are stored within a limited number of hyperscale data centres (linked to the concentration of key cloud servers, infrastructure and data warehousing), a large part of them in developed countries and China.

Technically, data travel over fibre at the speed of light and for many applications, and data storage is not required to be in a specific location. There can be queries rapidly transmitted within applications or services. The business models of large technology firms tend to build on this location independence of storage. Core data infrastructure provides services globally or to a broad region, with a strong dominance of data centres in North America and Western Europe, which together account for almost two thirds of all co-location data centres (see chapter I).¹⁷

While data storage does not need to be location-specific, there are technical arguments for data and storage infrastructure becoming more globally spread. Having a more local source of data may benefit local firms in terms of cost. Moreover, lower latency, or time response to the request, works in favour of locating the data closer to their origin (World Bank, 2021). Other technical risks, such as sporadic fibre cuts and lack of redundancy, are reduced with an increasing diversity of data centres. These arguments are less important to low bandwidth or non-real-time data, but become more of a challenge for a newer generation of real-time applications where users require data flows that are highly sensitive to delay or highly interactive (such as cloud applications or real-time monitoring in industry).

In these cases, proximity becomes important in ensuring that large-scale data flows are viable. This does not necessarily imply the need for national data localization requirements, but highlights that there are potentially subtle barriers embedded in cross-border data flows in some regions that can impact on economic development. Large tech firms' infrastructure, for example, has neglected certain regions, such as Africa, which suffers from a lack of data infrastructure, including key application servers, data centres and content delivery networks (Fanou et al., 2017; Weller and Woodcock, 2013). Even if the state of affairs has improved in recent years, it can have an impact, for example, by downgrading the performance of specific cloud applications or increasing overall costs for data providers (Chetty et al., 2013). This reason for storing data locally has been discussed less often in terms of policy in developing countries. Reasons related to security and economics are more often found to justify it.

A common reason for storing data locally concerns questions of jurisdiction and security. In cases where data are stored outside a State's borders, the argument is that accessing such data for legal reasons can be a challenge. Mutual legal assistance treaties exist to allow nations to access data outside a jurisdiction, but these are not in place between all countries, and such requests are reported to take

¹⁶ Data location, which is the actual place where data are, is to be distinguished from data localization, which is a policy measure in the context of cross-border data flows regulation that imposes requirements to locate data in a particular territory.

¹⁷ Low-cost data warehousing and cloud computing depend on economies of scale, and firms decisions around locating such data facilities are highly structured based upon different reasons, such as risk situation and availability of infrastructure, including energy, costs, and political and regulatory considerations (Azmeah et al., 2021).

between 6 weeks to 10 months, even when the United States is the requestor (Brehmer, 2018). There are high-profile examples where data access for security reasons was less than forthcoming. Relevant to cross-border flows is the well-publicized case of the *United States versus Microsoft* in 2017, where United States courts supported Microsoft in denying access to data due to their storage in Microsoft data centres in Dublin, Ireland (Daskal, 2017).

Cybersecurity implications might also be used to justify storing data locally. Cross-border flows and international storage have been linked to perceived risks, where nations fear cross-State surveillance and/or unwarranted mining of national data (Meltzer, 2015). These security arguments are, however, much debated. While there is evidence that such surveillance occurs, localizing the storage of data is unlikely to offer a better outcome in terms of cybersecurity. Indeed, domestic storage of data across multiple countries poses risks of many small, poorly managed and costly data centres (Chander and Lê, 2014). Moreover, for citizens concerned with the security of their personal data, localized storage in countries with autocratic Governments may also pose higher risks of surveillance than international storage (Meltzer, 2015). In terms of security, firms tend to place data in diversified locations in order to minimize risks.

Keeping data stored locally may also be justified for economic reasons. Such arguments mirror those made in conventional trade debates, which argue that local production plays a key role in supporting skills, the emergence of domestic firms and development more broadly (Foster and Azmeh, 2020). Following a similar line of argument, local data storage (and the reduction of cross-border data flows) has been argued to potentially support local data capacities and infrastructure, and drive the digital economy. The limitation of these arguments is that, as opposed to localizing the production of goods or services, even if data centres are domestically located, activities associated with data may still be done remotely. Therefore, the direct local benefits of domestic data centres will lead to the creation of a relatively small number of direct jobs. These will mainly be in the initial construction of buildings with a limited number of network engineers, technicians and security required on the ground (Chander and Lê, 2014).

• The decision on where to locate data depends on different technical, economic, security, jurisdictional and privacy-related factors, as well as on infrastructure and energy availability and reliability, which may play in different directions and need to be assessed in a holistic manner.

There are, however, arguments that spillovers from data centre investments can be more significant, highlighting how other types of data-related capital and capacity emerge with the presence of data centres. Such arguments are less well researched in developing countries, but evidence in developed countries suggests that data centres can complement other investments in data infrastructure, and have important spillover effects in the economy – for example, by supporting joint public–private upgrading of energy and transport infrastructure (NVTC, 2020; Washington State Department of Commerce, 2018; UNCTAD, 2019a). Therefore, while the direct economic gains from localizing data centres are limited, in some instances the presence of data centres might be an important part of a broader package of planned investments that build data capacity and capital in a country. Moreover, while arguments for domestic localization of data are gaining ground, there is limited evidence of this relationship.

The strategy of requiring data to be stored domestically may only pay off in large countries that can achieve the necessary critical mass and scale to be able to create value from the data. In addition, keeping the data inside borders can lead to economic development only when the capacities to transform the data into digital intelligence and monetize them exist in the country, as will be discussed below. Data use skills are more important, and can be developed locally, even if the data centre is located elsewhere; the connectivity infrastructure is also more relevant than the data centres themselves. For smaller countries, little value can be generated from data when they are not allowed to flow across borders, given that the value of data emerges from aggregation of data.

Thus, it is more important to focus on the location of the value created from data (and its capture), from the processing of data into data products, which does not necessarily match the place where data are

generated. It is in the location of the use of data where real economic value is added; thus, it is the flow of data value that matters more than the flow of data themselves. In this sense, the physical location of the data storage may not be such an important factor for development. However, this may also depend on the needs for processing data, since the strongest capacity for data processing is found in the hyperscale international data centres, which are rarely located in developing countries, except for China.

It may be argued that, as long as access to the data is ensured, there should not be any relation between the location of the data storage and economic development since, with guaranteed access, domestic actors can use the data for economic purposes. This would be the case for a firm that stores its data in a data centre outside a country (leading to a cross-border data flow), which, as long as it can use the data for its purposes, will be able to benefit from the data.

A different case is when a global digital platform extracts the data from the users in a particular country, using them for its private benefit, without any compensation or possibility for domestic firms to productively use those data. Indeed, foreign entities are likely to have a first-mover advantage in data analysis and processing that may be challenging to bridge by latecomer developing countries, even with access to their data. A proper international framework regulating cross-border data flows should ensure access, and guarantee that the income gains from data are equitably shared when access is restricted. This should be complemented by improvements in the capacity to process the data in developing countries. Overall, the decision on where to locate data depends on different technical, economic, security, jurisdictional and privacy-related factors, as well as on infrastructure and energy availability and reliability, which may play in different directions and need to be assessed in a holistic manner. Policymakers in developing countries will need to assess the different costs and benefits involved in the decision about physical data location, considering the specific characteristics in the country and their development strategy needs.

F. DIFFERENT TYPES OF DATA: IMPLICATIONS FOR CROSS-BORDER DATA FLOWS

Data can be categorized in different types according to various taxonomies. Different types of data have already been introduced in previous discussions in this Report, such as volunteered and observed data; structured and unstructured data; and personal, public and private data. Other possible categorizations include data for commercial purposes or governmental purposes; data used by companies, including corporate data, human resources data, technical data and merchant data; instant and historic data; sensitive and non-sensitive data; and business-to-business (B2B), business-to-consumer (B2C), government-to-consumer (G2C) or consumer-to-consumer (C2C) data. Distinguishing among different types of data is important, because it may have implications on the kind of access that would need to be given to each type, both at national and international levels, as well as on how to handle the data.

This section discusses some key categories of data flows. These categorizations are important, as they might be the basis for differential treatment of data as they flow across borders. It may offer some potential insights for more granular regulation of cross-border data flows. However, given existing significant challenges in measuring and differentiating such flows, there may be limits to how these can be applied in practice.

An important distinction is who the producers and consumers of data are. This implies exploring whether cross-border data flows are associated with B2B, G2C, B2C or C2C exchanges. It is also relevant to discuss additional cross-cutting issues, which may involve different treatment of data related to personal and sensitive data.

1. Types of producers and users of data

a. Commercial data

As outlined earlier, proprietary data flows resulting from B2B and B2C interactions are likely to be associated with firms' legal agreements, which determine what data are transmitted and how data flow

across borders. Where flows are not linked to personal data, they are likely to be determined by internal rules of the firms, inter-firm agreements or contracts.

For cross-border organizational data associated with the transfer between internal businesses or in global value chains or B2B exchanges, a key concern is preserving the control and confidentiality of data as a core of competitive advantage in a data economy. For example, ensuring that machine-to-machine or IoT data can be exchanged securely and rapidly is an increasingly important aspect of the operation of global value chains (Foster et al., 2018).

b. Government and open data

Governments often integrate their data services with the private sector in their use of data sources, services and storage. Government-initiated cross-border data flows may therefore also depend on contracts and agreements that shape the data flow. Government data are often seen as more sensitive than other data, especially if they are part of critical national infrastructure. Thus, cross-border flows of such data may be subject to additional requirements, including national regulation. For example, certain government data may be allowed to cross borders only under certain requirements (for example, only using specific standards or encryption norms; or requirements of use of storage within the private cloud, as opposed to public cloud, for security). In some cases, cross-border data flows may be prevented when data are especially sensitive, as discussed later in more detail.

While internal government data may be subject to stricter treatments, there is also a trend for governmental and other non-profit organizations to share data as a means to create economic and social value. Appropriately shared data can drive regional or international cooperation. At a governmental level, cross-border data flows in areas such as harmonized trade, business databases, regional governance platforms, and national security and crime systems, are becoming more common.

Data flows can also integrate with more open resources, which might also be seen as a category of data with the goal of open use and sharing. Specific organizational groupings or areas may come together to agree on how to share data at national or international levels. One example of a success in this area is activities that have promoted building standards, platforms and the promotion of sharing of aid data. Led by the International Aid Transparency Initiative, this has supported Governments and non-governmental organizations in opening up their aid data, which can then be globally combined and used for broader understanding of this sector (Pamment, 2019).

c. Consumer data

Cross-border data flows involving consumers may be subject to specific treatment. Most crucially, consumer data will likely include personal data, and as such, data flows may be subject to additional rules. As personal data might also be associated with other sources of data, this is dealt with as a cross-cutting issue below. Cross-border interaction between consumers and foreign businesses, or between a consumer and a foreign consumer, have principally emerged at scale as a result of digital technologies. There are a number of questions about how such data flows might potentially be treated. With foreign enterprises being outside the jurisdiction of Governments, significant foreign B2C data flows pose risks around national adherence to a range of international and domestic rules, such as standards, labour and taxes (Aaronson, 2019a). The growth of C2C data flows across borders also poses questions about relevant treatment and jurisdiction. For example, large-scale C2C interactions in e-commerce and C2C data flows associated with the gig economy have been enabled by online platforms. These allow certain activities that sit outside existing regulatory frameworks, which may need to be reviewed.

2. Cross-cutting issues for personal and sensitive data

a. Personal data

Personal data are an important category of data whose flows need to be subject to additional regulation. A range of different types and sources of data can include personal data. Data involving consumer interactions are likely to embed personal data associated with an individual, but other data flows are

also likely to contain personal data. Firms and other organizations may, for example, exchange records about users, which may be part of cross-border data flows related to internal organizational or B2B processes.

The type of personal data present in such data flows is diverse. It may include volunteered data that users provide as part of their interaction with applications and services, such as demographic information or credit card details. It may also include a wider range of observed data captured as part of product or service use – for example, e-commerce apps may keep a record of products a user has looked at, and potentially more granular data about location, interactions and so on may be collected (OECD, 2020a). Other types of inferred data¹⁸ may also be generated related to specific individuals, including inferences based upon the collected data (such as risk and credit scores), and potentially also combined with other external data sources, both personal and non-personal. For example, an insurance firm may combine personal data provided by an individual with other data about the same individual from external sources, as well as other data, such as location and demographic risk, to determine risk levels (GSMA, 2018c).

Cross-border flows of personal data are likely to require being subject to a range of agreements and regulations. For one, the sender and receiver of data will likely need to adhere to norms and commercial agreements on how data are collected, transmitted and reused. More broadly, this will be orientated by data protection regulations. At present, different core approaches are emerging globally to personal data protection that do not well align, as will be discussed in chapters IV and V.

An important issue with these different rules is the determination as to what types of data flow are classified as containing personal data. While volunteered personal data such as demographic information are clearly personal data, there can be a lack of clarity around whether observed data are personal data or not, when it may not directly identify a specific individual. Stricter personal data rules that have been emerging have looked to enhance data protection by including broader definitions of personal data, including where anonymized and volunteered data might still indirectly identify an individual – for example, data associated with IP addresses or web cookies (Bird and Bird, 2017).

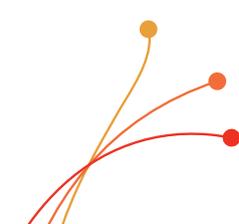
Given the risks and potential regulatory burden of capturing and resharing personal data, firms often look to undertake approaches to anonymize data that will allow more flexibility in data flows. Common approaches look to delink observed data from a specific individual, use pseudo-anonymization, or share data only in aggregation. Such techniques can be effective, but as the volume of data on individuals grows, there are questions as to whether such approaches truly result in anonymized data. As data protection is becoming stricter globally, technical research has looked to new techniques to allow data to be useful but better anonymized. Examples of this include newer techniques such as data perturbation, where random noise is added to data to provide individual anonymity while maintaining structure; and synthetic data, where artificial data are algorithmically generated to reflect the character of real data, but without representing individuals (PDPC, 2018). In an era of machine learning, it is likely that trained data models and algorithms also become more prevalent as an alternative to personal data. Once models have been trained satisfactorily, model data can be shared for applications with lower risks. Such approaches to anonymizing data can be important from a human rights view, by reducing the risk of data identifying users. They might also potentially support the sharing of personal-derived data as digital public goods in the future.

b. Sensitive data

An important segmentation for data arises when data are categorized as “sensitive”, and thus their flows are subject to additional rules or regulations, including on the ways they can be transmitted across borders. Key tensions in cross-border data flows emerge in differential ways that sensitive data are categorized – what is classified as sensitive data varies by country and over time.

Data associated with specific sectors might be subject to additional rules outside mainstream data regulation. For example, sectors such as financial or telecommunication services may have stricter

¹⁸ According to OECD (2019a), “Derived (or inferred or imputed) data are created based on data analytics, including data created in a fairly ‘mechanical’ fashion using simple reasoning and basic mathematics to detect patterns”. Thus, this should be considered as a “data product”, as it implies processing of the raw data.



data rules that do not allow cross-border data flows, or have specific requirements on storage or flows. The categorization of sensitive data flows may sometimes cause confusion and contradict other rules, as they emerge from a broader array of ministries, including those of health, trade and industry, and finance. In other countries, data rules define broader “tiers” of data flows that are considered sensitive.

3. Technical aspects of data flows

Data might also be categorized by technical features and subject to different treatment. One technical aspect that might lead to varying treatment of cross-border data flows is related to the format of data. Cross-border data flows associated with certain types of applications – such as audio, video, messaging, IP telecoms protocols and encrypted data – can lead to them being treated differentially. One way this might occur is through technical blocking of specific data flows at national Internet gateways, or where all national ISPs are requested to block these formats. Such technical treatment needs not necessarily come in the form of blocking data flows; countries may simply deprioritize such data flows. For example, deprioritizing audio or video streams across borders might result in a decline in quality of an international service. This has often been used informally as a way of prioritizing local context producers and firms. Other potential technical categorizations of data flows could be treated differentially, although there is less evidence of these being common. For example, treatments that differentiate between raw or processed data (which may imply whether data embed intellectual property) or encrypted data (which may imply data that follow stronger cybersecurity protocols) might be important categories in the future.

In sum, this section has provided some illustrations to highlight that there is a broad range of categories of data, which might imply different treatment of cross-border data flows according to the type of data. In practice, there may be significant challenges to identifying and separating these different categories of data. Differentiating data flows according to specific services or goods, or highlighting where personal data are embedded in data, is very difficult without considerable cooperation of data producers and consumers. Identifying the producers and users of data flows is also difficult, as many intermediaries in cross-border data flows exist, such as platforms, virtual private networks and content delivery networks. These play an essential part in the infrastructure of the Internet, but can also complicate the identification of the source and destination of data flows. However, a question that arises in this context, in which sophisticated algorithms are capable of creating highly personalized profiles for targeting advertising, is whether it would be possible to similarly design sophisticated algorithms that can track the different types of data.

Beyond technical challenges in identifying them, political and cultural challenges are also important for cross-border data flows. For many of the categorizations outlined (such as services, personal data and sensitive data), there are no globally agreed definitions; these vary across different regions and even among countries within a region. This will lead to challenges in deciding how cross-border flows are to be dealt with. As shown in the discussion of personal data, this is not a minor issue. Differing definitions can lead to very large differences in the volume of data flows that are categorized as personal data.

Notwithstanding the difficulties of having proper data categorization, there are clear benefits to be derived from having it, given that different types of data have different implications in terms of their flow, including across borders. It would allow the establishment of the kind of access required for each type of data, and facilitate the sharing of data under the necessary safeguards. This could take the form of conditions of access for different agents, at national or international level. Therefore, there is a need for stronger efforts and research to arrive to some common understanding on a data taxonomy that may be useful in the context of cross-border data flows and their international regulation.

G. POWER IMBALANCES AND INEQUALITY RESULTING FROM CROSS-BORDER DATA FLOWS

As discussed in UNCTAD (2019a), market dynamics in the data-driven digital economy lead to information asymmetries, market concentration and power imbalances that increase inequalities between and within countries. While enormous wealth has been generated in record time, it has been

concentrated around a small number of individuals, companies and countries. Value capture from data through the processing of raw data into digital intelligence (the data value chain) is increasingly in the hands of a few global digital platforms (see also chapter I). This is also reflected in the unequal exchanges in cross-border data flows. And, under current policies and regulations, this trajectory is likely to continue, further contributing to rising inequality and power imbalances. This section revisits these issues in terms of private sector dominance and aspects of data justice. These have significant implications for development policies, as it is important to ensure that the income gains for the data-driven digital economy, including through cross-border data flows, are equitably distributed, and that there is data justice.

1. Concentration of market power

The data value chain is dominated by global digital corporations and companies controlling global value chains. From a production perspective, even if Governments, small firms or citizens build capacity for data collection or application, most data flows are captured by or take place between private enterprises, often between subsidiaries, services and partners connected to the few large technology companies dominating various parts of the data value chain. Development challenges around data flows emerge in how these large firms extract and control the data, allowing them to create and privately capture value from them. As these firms grow and invest, there are limits to the ability for new firms to compete, due to the challenges of investing in human capabilities and capital to compete at scale. There is a risk of highly unequal “divisions of learning” opening up, where a small number of experts in tech firms, who have appropriate computing and data processing infrastructure and access to data, are central to the creation of value.

Value capture from data through the processing of raw data into digital intelligence (the data value chain) is increasingly in the hands of a few global digital platforms, which is also reflected in the unequal exchanges in cross-border data flows.

Firms in different countries are at varying states of preparedness to create value in the data-driven digital economy. Information asymmetries arise as a result of the competitive advantage that data provide to first movers. Although about 20 per cent of all firms in OECD countries in 2017 participated in e-commerce transactions, large firms are more than twice as likely as small and medium-sized enterprises to participate in e-commerce in a majority of countries, and this gap is widening in absolute terms in many countries (OECD, 2019b). For smaller businesses in most developing countries, the use of e-commerce is generally much lower. Moreover, giant digital platforms such as Google, Alibaba, Amazon and Tencent already have large troves of data, which they can transform into new value-added data products and services. These firms also have funds to purchase significant computing power and data expertise (Ciuriak, 2018). New products and services developed from data in turn generate even more data, which thereby further accentuates the market power of the digital giants (Weber, 2017). Firms that benefit from such information asymmetries tend to be large and, in general, they are concentrated in the United States and China (UNCTAD, 2019a). There are some successful digital platforms at the regional level in developing countries, such as Mercado Libre in Latin America and Jumia in Africa. However, these regional digital platforms usually follow similar practices on data as those of the global digital corporations, albeit at a smaller scale.

Command of data leads to information advantages, adding to the sources of potential market failure in the economy built on data, including economies of scale and scope, and network effects. All of these tend to promote market concentration (and thus market share capture for the leading firms). The information asymmetry inherent in the data economy seems irreducible – there are no market

solutions to correct for it. The exploitation of these information asymmetries – together with the fact that investment in the collection and cleaning of data often has a high up-front cost, but low or zero marginal cost (like other digital or intangible goods and assets) – implies that the large corporations controlling the data can capture significant rents from data extraction.¹⁹

There are also significant structural challenges for development in the global data economy. Unlike other technologies where there has been a global diffusion of innovation, the intersecting demands of high skills, capital-intensive resources and a massive amount of data together make it much more difficult for these structural challenges around data to be resolved by the market. Key platforms and devices that enhance data value chains are moving towards a situation of “winner-takes-all”. Successful big tech firms also tend to grow through integration across different stages of the data value chains, and may expand across different sectors. Successful big tech firms are also likely to make further investment in data collection infrastructure, as well as in AI research and development, cementing their dominance (UNCTAD, 2019a; Srnicek, 2016; see also chapter I).

Command of data leads to information advantages, adding to the sources of potential market failure in the economy built on data, including economies of scale and scope, and network effects, and reinforcing market concentration and inequalities.

Given the partial excludability of data, private data holders have strong incentives to accumulate data to bolster their current and future economic rents, using data as a barrier to entry. As a result, they can reinforce their market power and inequalities; significant power imbalances emerge between large digital corporations versus individuals, smaller companies and Governments. These are also reflected in asymmetries among countries when data flow across borders. In view of the huge size and power that these corporations have reached, it is likely that no country alone, particularly developing countries, will be able to tame their power. As the reach and influence of these global digital corporations increase internationally, there is a growing need for cooperation among countries to arrive to equitable development outcomes for the benefit of people and the planet.

2. Data justice and inclusion

Broader thinking around data and development also implies considering unbalanced data economies within countries. It is important not to underplay the broader tensions around evidence of the uneven impacts of data in economies that tend to provide benefits concentrated among the educated elite (IDC and OpenEvidence, 2017). When looking beyond economic indicators of development and focusing on broader social development and justice, identifying data injustices – the different dimension of data collection, handling, processing and societal structure that might lead to inequality – will be important in ensuring that data policy helps foster inclusion and sustainable development (Heeks and Renken, 2018). Examples of data injustices are also linked to the potential for discrimination based on data on different grounds, such as gender or race, which affect human rights.²⁰

For developing countries, there have been concerns, for example, about the way that data infrastructure is being introduced, as it generates data about low-income groups and communities, potentially leading to exploitation and new frontiers of economic and social exclusion (Arora, 2016; Flyverbom et al., 2017). To build digital intelligence about low-income users in such markets, users become attention objectives for systems and infrastructure of data (Arora, 2016). For example, provision of free Internet in developing countries through schemes such as Facebook’s Free Basics/Discover can provide low income groups online access at a low cost, but critical voices suggest it serves as a source of online behavioural data

¹⁹ For extended discussions on the extraction of rents in the data-driven digital economy, see Mazzucato et al. (2020), Ciuriak (2020) and Rikap (2021).

²⁰ For more detailed discussions of data justice, see Global Data Justice, “A globally inclusive dialogue about the future of data”, available at <https://globaldatajustice.org/>.

that can support expansion of such firms and lead to future data injustices for the poor. In Kenya, fintech apps, often from firms based in the United States, not only provide apps for management of payments, insurance and so on – they are also part of a data collection infrastructure that allows the firms to build social risk models of participants, which may be as important a part of profits as the direct commissions they make from their financial products (Donovan and Park, 2019; Iazzolino and Mann, 2019).²¹

Specific policies around cross-border data flows might then need to consider the goals of reducing data injustices and risks, and leverage digital and data for more inclusive development (Foster and Azmeh, 2020; Singh, 2018a; Singh and Vipra, 2019). Moreover, Governments can focus on building and supporting digital public goods such as data for social value, as discussed above, and developing more open infrastructure and platforms to support development.

H. DEVELOPING COUNTRIES IN THE INTERNATIONAL DATA VALUE CHAIN

Power imbalances and inequalities discussed in the previous section result in emerging unbalanced geographies of data. While there appears to be growing potential for activities in the data value chains at the margins, very few digital leaders are emerging in developing countries, and only in limited locations, such as in China, India, Indonesia and South Africa (David-West and Evans, 2016a; Evans, 2016). Some developing countries – most notably China, but also others, such as India and Indonesia – have growing digital prowess. But this is not the case for many other developing countries, which lag far behind in terms of preparation for the data-driven digital economy.

In the context of the international data value chain, different stages of data collection, storing, analysis and other processing into digital intelligence mostly take place in different countries. There is a growing awareness that cross-border data flows are imbalanced. For developing countries, flows of extracted data are strongly defined by “South-to-North” flows (McKinsey, 2014), which are mainly raw data. Given the dominance of data firms in developed countries, processed data in the form of digital intelligence are characterized as being concentrated in a limited number of advanced countries (Mueller and Grindal, 2019; Weber, 2017), mostly in the United States, as well as in China. These countries tend to capture the competitive advantage from data generation and their use for productive purposes.

Developing countries could be at risk of becoming mere providers of raw data to global digital platforms, while having to pay for the digital intelligence obtained from their data.

As UNCTAD (2019a) warned, firms in many developing countries may find themselves in subordinate positions, with data and their associated value capture being concentrated in a few global digital platforms and other multinational enterprises that control the data. Thus, developing countries could be at risk of becoming mere providers of raw data to global digital platforms, while having to pay for the digital intelligence obtained from their data. This points to a new centre–periphery model of international relations in the data-driven digital economy, in which the United States and China are at the centre and the rest of the world is at the periphery. This configuration represents a departure from the traditional separation between developed and developing countries; one developing country is in the centre, while a number of developed countries are in the periphery. However, those developed countries in the periphery are far more prepared to tackle the challenges emerging from this situation than developing countries are.

Thus, the emergence of data as an economic resource has given rise to a new layer in the international division of labour (Rikap, 2021; Coyle and Li, 2021; Feijóo et al., 2020), as reflected in the typology of data flows presented in table III.1. It shows different types of countries according to several criteria:

²¹ See also the discussion on the expansion strategies of major areas of influence in the global data economy in chapter IV.

Table III.1. Classification of countries/country groups according to their data flows across borders, by level of development		
	Data inflows	Data outflows
Developed countries	<p>Large countries with dominant international online platforms (DIOPs) and leading high-tech industries, and talent (LHTIs):</p> <ul style="list-style-type: none"> - <i>United States</i> 	<p>Countries and regions without DIOPs but with LHTIs:</p> <ul style="list-style-type: none"> - <i>European Union</i> - <i>Japan</i> - <i>United Kingdom</i>
Developing countries	<p>Large countries with DIOPs and LHTIs:</p> <ul style="list-style-type: none"> - <i>China</i> 	<p>Large countries without DIOPs but with LHTIs:</p> <ul style="list-style-type: none"> - <i>India</i> <p>Large countries without DIOPs or LHTIs:</p> <ul style="list-style-type: none"> - <i>Indonesia</i> <p>Small countries without DIOPs or LHTIs:</p> <ul style="list-style-type: none"> - <i>Countries in sub-Saharan Africa</i>

Source: UNCTAD, based on Coyle and Li (2021).

(a) whether they are mostly the destination of data inflows or the source of data outflows; (b) whether they are developed or developing countries; (c) the size of the country; (d) whether they have dominant international online platforms; and (e) whether they have leading high-tech industries and talent. Some examples are provided for each type.

There has been debate about whether this imbalance of data flows is problematic, using adapted economic models of trade to consider cross-border data flows (Mueller and Grindal, 2019). Economic approaches that associate development with free-market trade are based on the assumption that open trade across borders reduces the costs of goods for consumers in developing countries. Open markets also push competition and innovation, and support specialization, as domestic firms look for comparative advantage (Hunt and Morgan, 1995). It has been argued that, in the digital economy, free flows of data follow this broader paradigm, and an open Internet would be an important driver of development and trade (Bauer et al., 2014; Meltzer, 2015). From this perspective, a data flow imbalance would not necessarily be problematic, but part of an ongoing economic process where differences in flows relate to cost differentials. Imbalances would be resolved by the market. Indeed, given that the digital economy thrives on rapid cross-border data flows, attempts to restrict them are likely to reduce their benefits (Aaronson, 2019a).

Cross-border data flows cannot work for the benefit of people and the planet if only a few global digital corporations from a few countries privately capture most of the gains from the data.

In the trade arena, there has been pushback against these ideas of unfettered open trade by some observers. Such open trade tends to benefit powerful developed countries and presents challenges for developing countries, as imports grow and domestic firms are crowded out (Stiglitz, 2012). Reflections on uneven cross-border data flows suggest that they may also be problematic in terms of the location of value-added production in the digital economy (Weber, 2017). In this view, imbalances resulting from cross-border data flows may justify strategic intervention and policy measures by developing countries, to ensure that a larger part of the value added resulting from data remains within their boundaries.

Cross-border data flows cannot work for the benefit of people and the planet if only a few global digital corporations from a few countries privately capture most of the gains from the data. For development purposes, a properly functioning international system regulating those flows could go a long way in helping developing countries to appropriate a more equitable share of the value of data.

I. SOVEREIGNTY AND DIFFERENT LEVELS OF DATA GOVERNANCE

Cross-border data flows raise issues in relation to sovereignty over data and their use. Sovereignty commonly refers to which actors or groups have the legitimacy, authority and power to control and have influence in a society. Different actors have sought to assert control on data flows – through various activities, rules and policies (Couture and Toupin, 2019). But, as in the case of ownership of data, in the data-driven digital economy, the notion of sovereignty is broadly altered, as new nuances and meanings emerge. Traditionally, sovereignty has been associated with national territories and physical borders. However, the data-driven digital economy challenges this concept, as data are transmitted through the Internet, which originally was conceived as an open space, and national borders become blurred.

An additional factor that affects sovereignty is that, with increasing market power and size, powerful global digital platforms can behave in a nation-State-like manner, self-regulating their huge digital ecosystems, which include more and more aspects of life and society, and affect the sovereignty of true nation States. This section examines the different levels and scales of control, applying the concept of sovereignty to digital technologies and data. In what follows, sovereignty in the data-driven digital economy is explored at national and individual levels (as well as for communities and groups), and in terms of geography.

1. National sovereignty

Conventionally, sovereignty has been advanced at the level of the nation State, as it has the legitimacy, power and capacity to establish rules and govern (normally attributed by the sovereign will of its population through democratic elections). As data become increasingly economically important and States perceive a loss of control, against other countries or global digital platforms, as a result of cross-border data flows, there have been growing concerns in relation to data sovereignty at a national level.

The terms digital and data sovereignty have been widely debated recently;²² the notion of “data sovereignty” practically did not exist before 2011 in academic and public debates (Couture, 2020). It has taken various meanings that reflect different cultural values and political preferences in different regions (Couture and Toupin, 2019); the meaning may also be evolving over time as national priorities change (see chapter IV). For example, there is a growing discussion in the European Union on digital sovereignty, based on its values focused on the protection of fundamental rights; it also connects to the idea that the European Union needs to build capacity and “catch up” in the data-driven digital economy, in the face of dominant global digital platforms from the United States and China (European Parliament, 2020).

But the focus seems to be moving more recently towards the concept of “strategic autonomy”.²³ The approach of China to digital sovereignty positions digital technologies and the Internet as a broader geopolitical asset. Therefore, it emphasizes nationally-driven plans that push global technology leadership, and protection of data as a core and strategic asset for the Government (Budnitsky and Jia, 2018), with a strong focus on security (Creemers, 2020). In the United States, sovereignty over data is mainly entrusted to the private sector. Chapter IV discusses in some detail the major global approaches with regard to data governance, which strongly relate to different visions about data sovereignty.

Where other developing countries have referred to ideas of national sovereignty, it has often been a mix of these different ideas. In Brazil and Indonesia, for example, discussions have stressed the building of capacity, as well as alluding to critical infrastructures that nations need to control within the idea of sovereignty (Azmeah and Foster, 2018). Developing country discussions have also more strongly embedded social and cultural ideas of digital sovereignty that were previously more common among

²² There is a wide debate about digital and data sovereignty, which shows the significant differences and complications emerging in relation to these concepts. For detailed reviews, see Hummel et al. (2021), Pohle and Thiel (2020), Aydın and Bengshir (2019), Couture (2020) and Coyer and Higgott (2020).

²³ See, for instance, “Digital sovereignty is central to European strategic autonomy”, a speech by European Council President Charles Michel at the Masters of Digital 2021 online event, available at www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/; and Aktoudianakis (2020).

social movements and open-source communities. These link to longer histories of dominance and post-colonial inequalities, with the desire for groups to collectively take control of their own assets and destinies (Avila, 2018; Couture and Toupin, 2019; Kwet, 2019). In the context of the data-driven economies, digital/data colonialism is understood to take a broader reach than the historical colonialism of countries over countries; colonialism in the digital context is related to the exploitation of human beings over data by companies or by Governments, and it can happen in all countries (Couldry and Mejias, 2018, 2021).

The emergence of national sovereignty in all these cases, however, can sit uneasily with the global nature of the Internet and the difficulty in assigning territoriality to cross-border data flows. The approach of more strategically controlling key digital assets is also potentially only viable in large nations with centralized leadership that are willing to undertake highly interventionist regulations. Even there, the question remains open as to whether such approaches provide value for money in the face of fragmented global production networks and innovation.

National digital sovereignty is often associated with the need to store data within national borders. However, as discussed before, the link between domestic data storage and development is not so evident. A well-defined and properly functioning international framework for data governance, including for cross-border data flows, could allow for some common understanding and clarity over sovereign rights over data.

2. Individuals, communities and groups

Issues related to cross-border data flows go beyond companies and Governments, and affect individuals (in connection with their personal rights); thus, the issue of individual data sovereignty is also key in the context of the data-driven digital economy. Individual data rights are of relevance to control how individuals' data are used, and to prevent abuse or misuse; companies and Governments alike should respect these rights, at both the national and international levels.

Given private sector capacity to control digital technologies and data, as well as the control that Governments can exercise, debates on individual digital sovereignty frequently revolve around data rights, as discussed earlier, and how individuals can make claims to access, control, own or use their private data (Floridi, 2020), as well as protect them from abuse and misuse. Indeed, the notion of digital sovereignty in the European Union gives emphasis to the role of individuals regarding control of their data (European Parliament, 2020).

Digital sovereignty for the people can imply “that digital technologies can facilitate the transition from today’s digital economy of surveillance capitalism – whereby a handful of US and China based corporations battle for global digital supremacy – to a people-centric digital future based on better workers, environmental, and citizens’ rights, to bring long-term social innovation... break the binary logic that always and only presents us with two scenarios for the future of digital:... Big State strips people of their individual liberties, Big Tech creates data monopolies that will eventually run critical infrastructures such as healthcare or education; neither is an option for a democratic world”. A possible option is “a third way: Big Democracy. A democratization of data, citizen participation and technology at the service of society and the ecological transition” (Bria, 2020).

There are signs that individuals may choose to take control of their data. There is evidence that some users are thinking about “personal data sovereignty”, where consumer decisions are made on how they use digital technologies based upon how their data are used, particularly where they perceive problematic data handling (Kesan et al., 2016). In recent times, activists have also begun to build tools that seek to more easily allow personal data sovereignty, using specific devices or software for maintaining control of their data (Couture and Toupin, 2019). Privacy-oriented open-source software, such as ownCloud and nextCloud, allows users to host their own cloud services, without personal data extraction. Another example is Signal, a competitor to WhatsApp, which uses end-to-end encryption to keep conversations secure. A number of start-ups have also emerged under the label of the personal data economy, such as Digi.me and Meeco, that allow users to share or profit from their data. To date, such activities have been limited in scale, but they could influence data flows in the future.

Communities have often engaged with activities in connection to data sovereignty, looking to assert their group rights to data. For example, some indigenous communities have looked to claim rights over their data (Kukutai and Taylor, 2016). In developing countries, there have also been calls for other groups and communities at different scales to gain rights to data, such as traders or broader sets of workers (Singh and Vipra, 2019). More broadly, growing arguments around discrimination and racial biases embedded within data (Arora, 2016; Noble, 2018), might lead to future demands for larger communities, marginal or discriminated groups to seek community rights to data as an aspect of data justice (Heeks and Renken, 2018). Unlike personal data, claims for group sovereignty are emergent and often less well supported by underlying rights (compared with personal data rights). They should not be underplayed, however, where communities, groups or workers perceive that ownership of their own spaces and practices, and their ability to independently control their condition, are declining due to data extraction (Singh and Vipra, 2019).

3. Geography

Claims for digital sovereignty have been made at different geographic levels. At a subnational level, these typically focus on gaining access to privately collected data in spaces within the public interest. This might include local traffic, citizen or pollution data held by private firms that can support better spatial analysis, management and planning. Through negotiation or in specific moments, technology firms such as Uber, Siemens, Airbnb and Orange have shared data to support urban projects (see, for example, OECD, 2020a; Villani, 2018). In some developing country projects, sovereignty has also emerged through strategic joint projects between data providers and the public sector in building data infrastructure, and capturing and analysing data, as seen – for example, in smart city projects in India (Heeks et al., 2021). There are also proposals that seek to support expanded sovereignty over data, such as open data, data trusts, data cooperatives and data stewardship (Gonzalez-Zapata and Heeks, 2015; Open Data Institute, 2019a; O’Hara, 2019). Such claims to sovereignty are often less strongly made and their practical implementation is still limited. In the examples mentioned above, cities have rarely sought to control data or prevent cross-border data flows. Rather, they simply demand the ability to access and use data for their own ends.

There are significant difficulties in reconciling the notion of national sovereignty traditionally associated with country territories with the borderless nature, globality and openness of the digital space in which data flow.

In sum, there are different notions of sovereignty for claiming rights over data, and at different layers and geographical levels; the meaning of digital/data sovereignty (and therefore the associated sovereign rights) remains confusing (Christakis, 2020; De La Chapelle and Porciuncula, 2021). There are significant difficulties in reconciling the notion of national sovereignty traditionally associated with country territories with the borderless nature, globality and openness of the digital space in which data flow. Moreover, it is not only national sovereignty that matters in the data-driven digital economy; individual (or community) data sovereignty also becomes key in view of the nature of data. This implies that individual data sovereignty of people or communities may need to be protected from both private companies and Governments, to guarantee that individuals (and communities) have control of their data, and to prevent abuse and misuse of data. Hence the need for data to be properly regulated in a broad international data governance framework. It is important that countries are able to claim their sovereignty rights over data generated domestically, in order to be able to take autonomous decisions based on those data, and benefit from them, as well as maintain their independence from global digital platforms and foreign Governments. However, this should not be reflected in self-sufficiency or isolationist strategies, which are not likely to pay, given the network character of the Internet and the high level of interdependence in the data-driven digital economy.

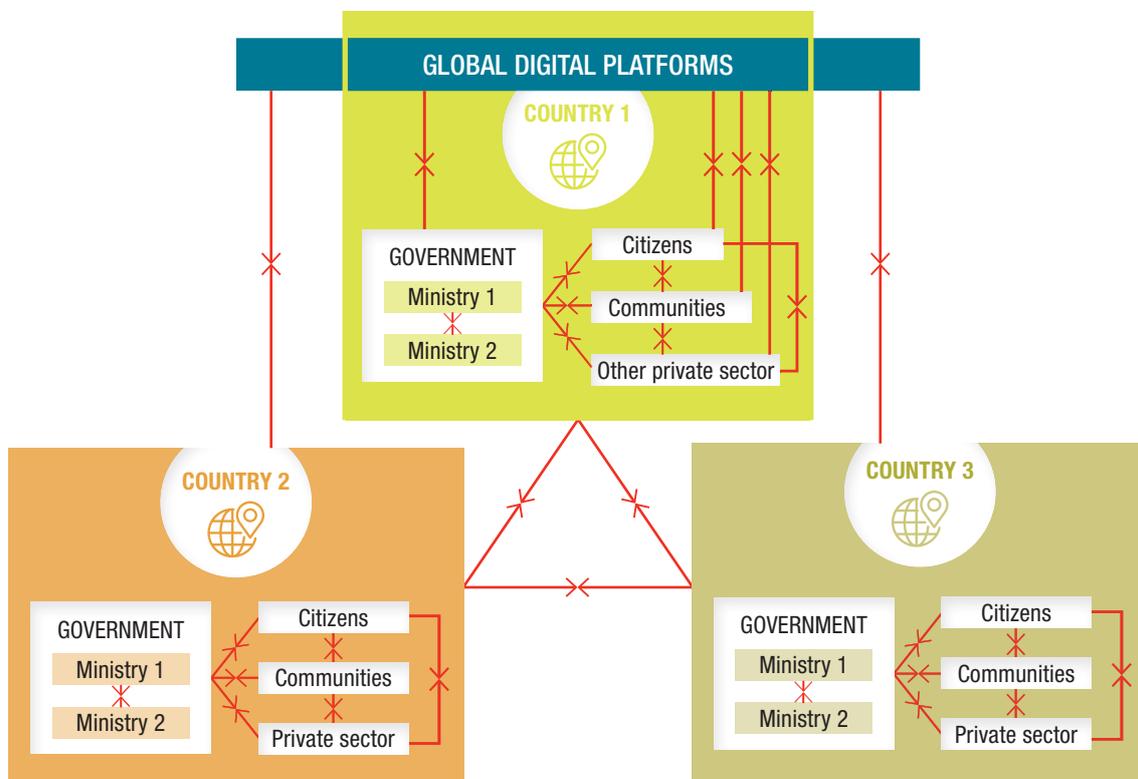
J. CONFLICTING INTERESTS IN CROSS-BORDER DATA FLOWS AND POLICY TRADE-OFFS

Economic, political and cultural differences among countries may result in diverging views about data, privacy, the Internet, the digital economy, surveillance and so on. Conflicting interests of different countries can lead to tensions among them. There can also be tensions within countries between various actors in the digital economy – such as individuals, communities, large and small private companies in the digital or other sectors, as well as civil society and Governments – as their interests also differ.

Against this background, major dilemmas emerge between different policy objectives at the national level, and between countries, as well as different interests among various actors in relation to cross-border data flows. Examples of these dilemmas include national security versus privacy, innovation versus data protection, surveillance versus privacy, and in relation to the distribution of the gains by country or by economic agent. Even inside these, there may be additional dilemmas to address; for example, in terms of innovation, what is the purpose of innovation? Is innovation going to serve only the interest of global digital platforms that benefit from the control of data and further enhance their power through the control of AI? Or is it going to serve the public interest? Among countries, different cultures and values with regard to issues related to data, privacy and sovereignty, among others, may lead to contrasting views on the ways to approach them and the policies needed to regulate cross-border data flows.

A simple illustration of how these tensions could work in a context of three countries (which could be projected to multiple countries) is presented in figure III.1. It shows the complexity of relations among different actors in the digital economy at national and international levels. The lines between countries and actors represent the different tensions that may emerge.

Figure III.1. Different actors and complexity of relations in the context of cross-border data flows



Source: UNCTAD.

Discussions on cross-border data flows highlight that rulemaking emerges in context-dependent ways in terms of different data categories and data flows, based upon different perspectives. Therefore, developing countries likely need to consider how decisions around data policy will shape such flows, firm costs, data privacy, national security, innovation and competition, among others. Countries will need to make trade-offs between these benefits, depending on their development goals.

Thus, policymaking in this area requires recognizing the complexity of the conflicting interests, dilemmas and trade-offs that arise, and properly assessing them. This implies policy choices, as interests may go in different directions. Policymakers will therefore need to assign weights to the different interests and objectives, and find the necessary balance that meets their specific needs and supports their development objectives. Ultimately, the outcome will be the result of political and societal choices.

This discussion also highlights that data governance requires a holistic, whole-of-government approach, which balances different policy objectives against each other. It is also important to consider the interests of all stakeholders. Finally, to address conflicting interests among countries in relation to cross-border data flows, policymaking at the international/multilateral level is key for developing countries' voices and views to be properly reflected in global data governance.

K. CAPACITY TO BENEFIT FROM DATA

The discussion in previous sections has highlighted the importance of data access and use for productive and developmental purposes. However, data can also be abused and misused, which raises significant challenges. While access to data is a necessary condition to benefit from data, it is not sufficient. The value of data comes from their aggregation, analysis and processing into digital intelligence. Thus, in addition to access, having the capacity to convert the data into digital intelligence that can be monetized, or used for purposes of public good is critical. Therefore, it is important to look at what are the capacities needed to be able to harness data for productive uses, and for development. Value creation and capture from data require the availability and affordability of data-related infrastructure for data to flow, as well as skills, resources and linkages with the rest of the economy, and support through appropriate regulation and policies (UNCTAD, 2019a).

While access to data is a necessary condition to benefit from data, it is not sufficient; having the capacity to convert the data into digital intelligence that can be monetized, or used for purposes of public good is critical.

Countries have different levels of readiness to engage in and benefit from the data-driven digital economy in terms of connectivity and data infrastructure, digital entrepreneurship and skills; financial resources; and regarding institutional capacities. Most developing countries lack significant digital prowess. Moreover, the limited size of their markets limits the possibility of economies of scale and scope in the data economy. And, in most cases, these countries do not have large numbers of constituents demanding that policymakers develop rules to govern data (Weber, 2017).

Thus, many developing countries fear that they will be unable to catch up in this new context, and obtain a comparative advantage in other goods or services resulting from data use UNCTAD (2017) reported that, without data-driven expertise, the position of developing countries in trade in goods such as commodities would be negatively affected. These countries will need to use data analytics to improve their production processes and their products, and to remain competitive.

From a labour perspective, with regard to the work done in the production and processing of data, a common assumption is that data production is highly automated and involves skilled systems and data experts. However, unpacking data production reveals other types of labour involved in the process. Certain types of rich data – such as online data, video and audio – often require human intervention in collecting, categorizing, filtering and cleaning to ensure data processing is effective (Gray and

Suri, 2019). Thus, a labour view would pay more attention to the fact that, behind complex data-driven systems and algorithms, there are often armies of lower-paid “digital labourers”, many of them located in the developing world.

Skills required for dealing with stored data revolve around administering, managing and analysing databases, which often need skilled systems administrators and database professionals. However, the majority of these activities can take place remotely in the world through online tools. Therefore, the location of database analysts and professionals can be typically delinked from data centre locations (Azmeah et al., 2021).

Data analytics and transformation are primarily associated with data science and information technology professionals. Analytics professionals are characterized as highly skilled, often university educated. With strong demand for these skills in the global market, developing countries often struggle to retain workers with such data skills (Huang and Arnold, 2020). In addition, analytics increasingly requires medium- and lower-skilled data work. Such work may require lower data processing skills, with some roles offering opportunities for those with basic computer literacy. Lower-skilled work revolves around workers involved in data extraction, selection, correction, filtering and labelling, which are essential to the effectiveness of large, data-driven organizations. Key centres of online outsourcing and business processing, such as India and the Philippines, have become centres of low-skilled digital analytics (Graham et al., 2017; Gray and Suri, 2019). There has also been growth in other developing countries – for example, in more connected rural regions (Malik et al., 2016) and urban centres of Africa – as connectivity enables low-paid workers to become “digital labourers” (Anwar and Graham, 2020).

More broadly, as an emerging area in developing countries, the capacity to benefit from data will also require capacity within governmental bodies and regulators. This includes the ability to technically analyse data flows and build capacity, as well as an understanding of how data relate to wider sectors and industries. Moreover, there is a need for policymakers to pay more attention to the need for data science and AI-related talent, not only for entrepreneurship development, but most notably for institutional building of policymaking; Governments may often lack the necessary human resources to design, implement and monitor relevant policies, because most of the talent is attracted by the private sector.

There are therefore significant capacity challenges at an individual, firm and policy level to ensure that developing countries are not just sites of data collection, but that they can capture value from data.

A focus on development is also crucial in thinking about how data can be leveraged more broadly. As this chapter illustrates, given the multidimensional character of data and the prevalence of cross-border data flows, it requires regulators to balance the regulation of competing data flows with a clear understanding of benefits and challenges.

In sum, the growth of the data value chain offers opportunities for developing countries to build capacities, but it is important to emphasize that most data and data collection infrastructure are privately driven and controlled by large firms that are predominantly not located in the developing countries, with the notable exception of China. There are therefore significant capacity challenges at an individual, firm and policy level to ensure that developing countries are not just sites of data collection, but that they can capture value from data.

L. CONCLUSION

This chapter has explored in some depth the complexities in the relationship between cross-border data flows and development, which are strongly linked to the particular nature of data. In the context of data, and their flows across borders, there is a diversity of views about what they imply and on who can

claim rights to data, the categories of cross-border flows according to the type of data, and approaches to digital sovereignty. These different approaches result from the varying political, social and economic situations and visions in different countries, and have a bearing on the direction of policy.

The particular characteristics of data, notably their public good nature, imply that they can lead not only to significant private gains, but also to social value and developmental benefits. The value of data depends ultimately on their use. Individual data are of limited use, but they have potential value because they are the ingredient for the obtention of digital intelligence that can be monetized, or used for private and social value. For the benefits of the digital economy to be materialized, data need to be shared and used, which most often involves data flowing across borders. Access to data is key in this context. But the implications of how data are used have both economic and other dimensions.

There is a role for public policymaking, at national and international level, to maximize the gains from data and cross-border data flows, minimizing the risks involved, while ensuring an equitable distribution of the gains from cross-border data flows.

Moreover, from the economic perspective, the need to enable data flows should not imply that data can flow across borders for free. Under the current absence of an international system that regulates cross-border data flows, global digital platforms can extract the raw data from developing countries and appropriate most of the value created, which results in increasing power imbalances and inequalities. Cross-border data flows cannot work for people and the planet if a few global digital corporations from a few countries are able to capture most of the gains.

Market mechanisms alone cannot lead to efficient or equitable outcomes. Thus, there is a role for public policymaking to maximize the gains from data and cross-border data flows, minimizing the risks involved, while ensuring an equitable distribution of the gains from cross-border data flows. Given the global reach of cross-border data flows, this will involve both national measures and policymaking at the international level.

Main issues highlighted in this chapter include:

- The particular characteristics of data make them of a very different nature from goods and services. Data are intangible, non-rival, partially excludable, and of a relational and multidimensional nature.
- Given their particular nature, cross-border data flows should be treated differently from international trade in goods and services.
- There is no evident link between locating data inside national borders and economic development; different factors operate in different directions when the decision to locate data is to be taken, and they are highly dependent on the specific situation of a country.
- Different kinds of data can have different implications in terms of cross-border data flows and related policies to address them.
- Data access and use (including their potential negative use) are key for development, together with the capacity to create and capture value from data – that is, to process data into digital intelligence (data products).
- There is a complex mix of conflicting interests among actors in the global data-driven digital economy and policy trade-offs that need to be factored in for policymaking on cross-border data flows for development.
- Policymaking for global data governance needs to take a holistic, multidimensional, whole-of-government, multi-stakeholder approach, at the national and international levels.

In exploring the potential opportunities and challenges of cross-border data flows, this chapter provides relevant knowledge that can help policymaking. The emergence of key domains of data policymaking in areas such as data protection, building capabilities and rules driving economic growth highlights opportunities for developing countries to capture value in the data value chain.

Setting appropriate rules on cross-border data flows at the right point can help to guarantee data rights, reduce structural challenges and support economic development. Additional trade-offs linked to the ethics of data are important to consider, including the relationship between creating value from data and data surveillance of populations, and the links between data filtering and censorship.

Countries may have reasons to control access to data based on technical, economic, privacy and other human rights grounds. As long as there is not a properly functioning international system of regulations for cross-border data flows to ensure maximization of the value of data, private and public, while protecting them from harm, and equitably distributing those gains within and between countries, there will be no alternative for countries to ensure that the domestic economy benefits from the development gains from the data, other than trying to keep their data inside national borders. However, it is important to consider that, while on the one hand there cannot be value without the raw data, on the other hand, having access to the data without the capacity to process and monetize them, or to create social value, is of no use. In this context, imposing restrictions for cross-border data flows may lead to no benefits, while creating barriers and uncertainty for firms and individuals seeking to exchange data across borders.

The diversity of views and dimensions on the key characteristics of data and cross-border data flows, and the associated complexities, points to the need for careful assessment of all elements involved when designing policies. Since different factors can play in different directions, different interconnections and interests involved need to be accounted for. The combination of the different issues addressed in this chapter may lead to multiple combinations of policies that will require policy choices to be made, according to political and societal decisions, and on the basis of development objectives. Overall, there is no simple solution. Oversimplifications in the policy debate in the form of calls for free data flows across the board (or bans on data localization) on one extreme, and outright data localization as a general rule on the other extreme, are unlikely to be of much use. It is necessary to assess deeply what the implications of cross-border data flows are, taking into account differences among countries, types of data, interests and policy objectives. As is commonly said, “The devil is in the details”.

• Oversimplifications in the policy debate in the form of calls for free data flows across the board (or bans on data localization) on one extreme, and outright data localization as a general rule on the other extreme, are unlikely to be of much use.

Overall, data have become a key strategic resource that underpins geopolitical tensions among different countries around the world, as will be discussed in the next chapter. In essence, it is an issue about who wins in the race for the control of digital technologies and data, which give the power to influence and control society. Cross-border data flows are key in this context.

The discussion in this chapter also points to the potential for fragmented national approaches to regulation, with significant differences across countries that might not lead to overall development. It is therefore necessary to examine in more detail appropriate governance frameworks and emerging international cooperation around cross-border data flows that can support broader development trajectories. The rest of the Report discusses in detail existing policies on cross-border data flows at different levels, first at the national level – in chapter IV, which focuses on global data governance trends which have a bearing on cross-border data flows; and chapter V, which maps national regulations on cross-border data flows. Policies at the regional and international levels are discussed in chapter VI. Chapter VII then explores possibilities on the way forward with regard to policies on cross-border data flows.

ANNEX TO CHAPTER III: THE WAY DATA FLOW ACROSS BORDERS

1. The flow of data

a. The “client–server model”

Most of the current data flow on the Internet is based on the “client–server model”. This model refers to the distributed application structure that divides tasks or workloads between servers (service providers) and clients (service consumers). A server host runs one or more server applications, which share content or resources with clients. A client does not share any of its resources, but it requests content or a service from a server.

Clients and servers exchange messages (data packets) in a request–response messaging pattern. To communicate, the client device and host servers use common languages and rules for data transmission. Today, most communications follow the TCP/IP model. The Transmission Control Protocol (TCP) provides reliable, ordered and error-checked delivery data packets between server and client applications (the three-way handshake). The Internet Protocol (IP) is the principal communications protocol for relaying (routing) data packets across networks.

b. The ISP 3-tier model

The Internet itself is a collection of separate but interconnected networks, each of which is an autonomous system (AS). The AS networks are controlled by Internet service providers (ISPs), each with its own business policies, internal network topologies, services and customer profiles. Apart from the IP addressing scheme, the autonomous systems also share a global Border Gateway Protocol routing framework to connect the different networks.

All these networks are connected through Internet exchange points (IXPs), which are physical locations through which Internet infrastructure companies – such as ISPs, content delivery networks (CDNs), web enterprises, communication service providers, and cloud and software-as-a-service providers – connect to exchange Internet traffic. These Internet exchange locations co-locate different networks and allow network providers to share transit interconnections outside their networks.

ISPs provide transport of Internet traffic on behalf of other ISPs, companies or other non-ISP organizations and individuals. They are classified into a three-tier model that categorizes them based on the type of Internet services they provide:

- Tier-1 Internet providers are the networks that are the backbone of the Internet. These Tier-1 ISPs, also known as network service providers (NSPs), build infrastructure such as the Atlantic Internet sea cables. They provide traffic to all other ISPs, not end users. Tier-1 ISPs own and manage their operating infrastructure, including the routers and other intermediate devices (such as switches) that make up the Internet backbone. They only exchange Internet traffic with other Tier-1 providers on a non-commercial basis via private settlement-free peering interconnections. Tier-1 networks support very high traffic volumes and large customer bases with a large number of routers, and are typically comprised of many autonomous systems.
- A Tier-2 ISP is a service provider that utilizes a combination of paid transit via Tier-1 ISPs and peering with other Tier-2 ISPs to deliver Internet traffic to end customers through Tier-3 ISPs. Tier-2 ISPs are typically regional or national providers. Only a few Tier-2 ISPs can provide service to customers on more than two continents. Often, they will have slower access speeds than Tier-1 ISPs, and are at least one “router hop” away from the backbone of the Internet.
- A Tier-3 ISP is a provider that strictly purchases Internet transit. A Tier-3 provider is by definition primarily engaged in delivering Internet access to end customers. Tier-3 ISPs focus on local business and consumer market conditions. They provide the “on-ramp” or local access to the Internet for end customers, through cable, digital subscriber line, fibre or wireless access networks. Their coverage is limited to specific countries or subregions, such as a metro area. Tier-3 ISPs utilize and pay higher-tier ISPs for access to the rest of the Internet.

c. Steps in the data flow

Combining the client–server model with the ISP 3-tier model, the Internet data flow might look as follows:

1. A message from the client application (for example, a web browser) is broken into different data packets that include instructions for reassembly (TCP) and the destination (IP).
2. The data packets are transmitted from the device (for example, a PC, tablet or smartphone) through the router and modem to the client's ISP (local/Tier-3 ISP), which provides access to other networks on the Internet.
3. The data packets are received by the local ISP (Tier-3).
4. Connected through the IXPs, the data packets are then routed by the Tier-3 ISP to Tier-2 ISPs, which in turn may route the packets to Tier-1 ISPs (the Internet backbone).
5. Using the BGP, each individual data packet may be directed through different routes to their destination, passing through different IXPs, located in different countries and operated by different ISPs (see next section).
6. Ultimately, all data packets are received by the destination's ISP (local/Tier-3 ISP), which forwards the packets to the destination server (identified by the destination IP address).
7. At the destination, the data packets are reassembled and the request runs in its application.
8. The server response follows a similar process back to the client.

2. How data cross national borders

a. Identifying cross-border data flows

As explained in the three-tier model, data packets are routed through different local, regional or international networks. Cross-border data transfers will mostly flow between or within Tier-1 networks, and are typically transmitted over very high-speed fibre-optic cables. Given that the data travel with the speed of light, and the fact that the exact route of almost all data is only determined when it is in transit, it is practically impossible to determine where and when a specific data packet crosses a national border. However, whenever a data packet flows through a country, it will be routed through a data centre, where it will be forwarded in the ISP's own network infrastructure, or exchanged with the network of another ISP at an IXP. These are the physical entry and exit points where cross-border data flows can be determined.

Another way of looking at cross-border data flows is by focusing on the information (data), instead of the individual data packets. The individual data packets have only limited value, as they carry only a part of the information that is transmitted. Only when all data packets are reassembled can the data be processed. In this case, there are two physical locations through which all data packets are guaranteed to flow after being sent by the originator and before being received by the destination, which are the client's ISP and the server's ISP. It is at these ISPs that the cross-border nature of a data transmission can be determined.

b. Routing international Internet traffic

Internet traffic is routed through different networks controlled by ISPs and connected at IXPs. The route a data packet will travel between networks is determined by the Border Gateway Protocol (BGP). BGP is classified as a path–vector routing protocol, and it makes routing decisions based on path, network policies, or sets of rule configured by a network administrator. Each BGP router maintains a standard routing table used to direct packets in transit and best-path decisions based on current reachability, hop counts and other path characteristics. In situations where multiple paths are available (such as within a major hosting facility), BGP policies communicate an organization's preferences for what path traffic should follow in and out. As discussed above, routing can also take place within an autonomous

system (ISP network), in which case interior gateway protocols are used to determine the route of a data packet. Although data flows are highly “globalized”, experts have calculated that over 66 per cent of international web traffic is routed through the United States (Mueller and Grindal, 2019:77). This is linked to the high share of global data centres that are located in that country.

c. Registering cross-border data flows

Cross-border data flows are not registered at the national or international level. This does not mean that data cannot be traced across the Internet. For instance, the Internet Control Message Protocol (ICMP) is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address. Using the ICMP, traceroute and tracert are computer network diagnostic commands for displaying possible routes (paths) and measuring transit delays of packets across an IP network.

The IP addresses that network devices’ data packets flow through can be used to determine the country, city or post code, determining an object’s geographical location. There are several Internet geolocation databases that can be queried. The primary source for IP address data is the regional Internet registries, which allocate and distribute IP addresses among organizations located in their respective service regions. These can be complemented with secondary sources, such as data mining or user-submitted geographic location data, and further refined. Internet geolocations are used for criminal investigations, fraud detection, marketing and licensing.



The particular nature of data, and existing global imbalances in the way in which cross-border data flows can be harnessed for various development objectives, imply a key role for policies to achieve those objectives. However, as shown in this chapter and in chapter V, the approaches taken to govern data and data flows across borders vary considerably among countries. This chapter focuses on the major policy approaches towards the digital economy and data governance in some major economies, which may have a global influence on the digital economy, including on regulations of cross-border data flows. Diverging approaches in this context are reflected in tensions in the global economy – especially between the United States and China – and risk fragmentation of the digital space and the Internet, with potential significant implications for developing countries.

This chapter stresses the importance of avoiding silo-oriented approaches in order to foster more inclusive and equitable outcomes from the data-driven digital economy. A world of divergent “data nationalism” is not likely to work for the interests of developing countries and the world economy. It would result in suboptimal domestic regulations, reduced market opportunities for small businesses and fewer opportunities for digital innovation, leading to a small number of winners and many losers.

MAIN GOVERNANCE APPROACHES TO THE DATA-DRIVEN DIGITAL ECONOMY WORLDWIDE: RISK OF **FRAGMENTATION** IN THE DIGITAL SPACE?

IV



CHAPTER IV DIVERGING DIGITAL AND DATA GOVERNANCE APPROACHES RISK FRAGMENTING THE DIGITAL SPACE

The approach to governing data and data flows

varies considerably among the major players in the digital economy, and there is little consensus at the international and regional levels.

Data governance approach



Current global context

Risk of fragmentation in the digital space and of the Internet

Global digital platforms continue to expand their own data ecosystems



Tensions among the major players

Race for leadership in technological developments to gain economic and strategic advantages

A silo-oriented, data-driven digital economy would go against the original spirit of the Internet and is not likely to work for the interest of developing countries

In economic terms, **interoperability** should generate better outcomes

Fragmentation would hamper technological progress, reduce competition, enable oligopolistic market structures in different areas and allow for more Government influence

Fragmentation would also mean more obstacles to **collaboration across jurisdictions**

In the absence of an **international system for regulating data flows**, some countries may see no other option than to restrict them with a view to meeting certain policy objectives

A. INTRODUCTION

For cross-border data flows to work for development, there is a need for policymaking, as shown in chapter III. Most countries are implementing some kind of measure to govern their data and cross-border data flows. These can take various forms according to differences in political, economic, social and cultural conditions and values. They also reflect different priorities in their policy objectives. This chapter, together with chapter V, presents the state of play with regard to the country-level governance of cross-border data flows around the world. It starts by looking at the major approaches towards and trends in governance of the data-driven digital economy in economies that can have a global influence on cross-border data flows. Chapter V then zooms into providing more details on the specific measures taken with regard to cross-border data flow regulations, with a view to mapping the global situation of these regulations at the country level.

The Internet was once defined primarily by an absence of centralization (Medhora and Owen, 2020), in a free and open space. Much has also been said about the need for a global, interoperable Internet (ECLAC and I&JPN, 2020; Internet Society, 2020a), since its benefits potentially allow it to reach global audiences, integrate digital global value chains and access larger markets beyond domestic ones.¹ But now the platform economy, artificial intelligence (AI), the surveillance State and quantum computing all demand large-scale data sets, entrenching centralized nodes of influence. Global digital corporations that extract the data and have control over them are creating their own data ecosystems. At the same time, data-driven digital economy issues are increasingly considered to be national matters, following claims for sovereignty over the data generated domestically. Both of these trends point to a silo situation, which does not match well with the open nature of the Internet. Within these centralized nodes, however, it is possible to find very different notions of digital and data governance.

This chapter discusses in section B the major approaches towards the digital economy and data governance in five major economies that may have a global influence on regulations of cross-border data flows: the United States, China, the European Union, the Russian Federation and India. The expansion strategies of the approaches of the United States, China and the European Union are discussed in section C. Section D then looks at the possibility of fragmentation in the digital space, and explores the impact of the clash between different data regulation models, especially between the United States and China, and the possible risks resulting from a potential fragmentation of the Internet and the data-driven digital economy. It also points to possible consequences for developing countries of such a fragmentation. This chapter therefore provides an overview of the context on data governance worldwide, focusing on the major areas of influence. The following chapter then presents the mapping of specific policies on cross-border data flows applied at the national level in different countries.

B. MAJOR APPROACHES TO THE DIGITAL ECONOMY AND CROSS-BORDER DATA FLOWS

This section discusses the major prevailing approaches to governing the digital economy, as well as corresponding regulatory models on cross-border data flows. The five cases can be described, in a somewhat simplified manner, as a market-oriented approach (United States); a complex mixture of security-oriented and digital development-oriented approaches (China); a rights-oriented approach (European Union); a security-oriented approach (Russian Federation); and a domestic development-oriented approach (India). Several other countries choose to emulate these regulatory models in different ways, as will be discussed in the following chapter. However, these major approaches are in no way presented as models to follow, because each one reflects the particular situation and

¹ The Internet Society has identified the critical properties that define the Internet Way of Networking, to enable it as a “network of networks” to bring technological and economic benefits, which comprise: an accessible infrastructure with a common protocol; an open architecture of interoperable and reusable building blocks; decentralized management; a single distributed routing system; common global identifiers; and a technology-neutral, general-purpose network. See Internet Society, Internet Way of Networking, available at www.internetsociety.org/issues/internet-way-of-networking/.

priorities of the corresponding economy. Indeed, the discussions in this and the next chapter show that, when it comes to the governance of cross-border data flows, there is no one-size-fits-all approach.

The aim in this section is to describe the overall framework of major approaches to highlight differences that may lead to problems of compatibility or interoperability among them, or raise concerns of fragmentation of the digital space at the global level that may have an influence on developing countries, as discussed in the next section. Moreover, given the fast speed of changes in digital technologies and the increasing awareness about the need to regulate their implications in the data-driven digital economy, these approaches are not to be taken as static; regulatory approaches to data and cross-border data flows are constantly evolving. What is presented here is a broad characterization of the configuration as of early 2021.

1. Promoting markets and innovation: the approach of the United States

The United States has generally adopted a free-market approach towards the digital economy,² which includes a similarly liberal regulatory framework for cross-border data flows. Thus, the United States has favoured a private market-driven approach aimed at stimulating innovation as well as supporting first-mover advantages and subsequent dominant positions by its digital firms, through network effects and acquisitions. In this context, the country has used trade agreements to ensure its firms unfettered access to foreign markets by, for example, favouring free data flows and banning practices such as data and server localization requirements (see chapter VI). As stated in Congressional Research Service reports, “In general, the United States adopts a market-driven approach that supports an open, interoperable, secure, and reliable internet that facilitates the free flow of online information” (CRS, 2020a, 2020b). This approach enables data to flow back to the United States when users around the world engage with firms headquartered in the country.

A key motivation behind the regulatory approach of the United States on cross-border data flows is maintaining its leadership in the global digital market and further expanding into new markets (see below). Its technology sector to date has been extremely successful in developing data-driven products and services that have penetrated most markets of the world. This has created a “positive feedback loop”, which means that the more data that can be collected by United States companies, the better for their data products and, therefore, the greater their ability to succeed in global markets (Weber, 2017). Accordingly, the United States has advocated against digital and data protectionism – for example, by endorsing the Asia–Pacific Economic Cooperation (APEC) Privacy Framework and the Cross-Border Privacy Rules System, through which government-approved trusted agents can certify companies conducting international data transfers (see chapter VI).

An undivided Internet and the free flow of information across borders are integral parts of the political and economic philosophy of the United States (Clinton, 2010). Unlike most developed economies, the United States does not have an omnibus data privacy framework, nor does it impose any specific compliance requirements for cross-border transfers of personal data. The United States has, however, adopted strict localization policies for defence-related data, requiring that any company supplying cloud services to its Department of Defense must store its data only domestically.³ More recently, although not a general restriction on data flows, the United States has adopted the Clean Network Programme for protecting critical assets from foreign interference and guarding individual privacy by restricting untrusted telecommunications carriers, applications and cloud services, notably from

² The State has, however, played a fundamental role in the development of the Internet and in the emergence of global digital platforms.

³ United States Department of Defense, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, DFARS Case 2013-D018, available at www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for.

China.⁴ Therefore, despite the overall liberal framework on cross-border data flows, the United States takes a restrictive approach for specific defence and national security issues.

Due to the global, market-driven cloud computing model, the federal authorities in the United States have occasionally faced difficulties in obtaining data stored on overseas servers. After a complex dispute between the Federal Bureau of Investigation and Microsoft over obtaining user data stored on servers in Ireland in 2013,⁵ the United States adopted the Clarifying Overseas Use of Data (CLOUD) Act.⁶ This act has a two-fold purpose: (a) it allows federal law enforcement authorities to require United States-based companies to provide user data stored abroad based on a warrant or subpoena, provided that it does not breach the privacy rights of an individual in the foreign country where the data are stored; (b) it establishes a procedure by which the United States can enter into executive agreements with foreign countries⁷ to provide data for law enforcement purposes, provided such foreign countries are committed to the rule of law and privacy protections. Such executive agreements are intended to speed up access to data for law enforcement purposes, which has traditionally been slow under mutual legal assistance treaties (United States Department of Justice, 2019).

The United States has opted for a flexible and ad hoc sectoral approach in regulating data privacy, and has prescribed specific standards only in some areas, such as child privacy,⁸ health information⁹ and financial data privacy.¹⁰ None of these sectoral regulations, however, contains a restriction on cross-border data flows, although they impose relatively strong compliance requirements for all service providers. Recent years have seen increasing pressure to adopt a privacy law at the federal level, leading to the first bill to be proposed in March 2021.¹¹ Further, some states, such as California and Virginia,¹² have adopted comprehensive privacy laws providing strong privacy rights to individuals (Christakis, 2020).

These moves towards privacy regulation in some states in the United States, plus the proposed federal privacy regulation, may point to the tide turning towards a departure from the free market approach with giant digital companies. This is also the case in the area of antitrust regulations; Congress has performed a profound investigation on competition in digital markets, and different antitrust actions have been taken involving several states, the Department of Justice and the Federal Trade Commission.¹³

⁴ United States Department of State, *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, 5 August 2020, available at United States Department of State, *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, 5 August 2020, available at <https://2017-2021.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/index.html>. See also "The Clean Network", available at <https://2017-2021.state.gov/the-clean-network/index.html>.

⁵ *United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

⁶ Clarifying Lawful Overseas Use of Data Act or CLOUD Act (S.2383, H.R. 4943).

⁷ To date, the United States and the United Kingdom have entered into such an executive agreement. Department of Justice, "U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online", 3 October 2019, available at www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

⁸ The Children's Online Privacy Protection Act prescribes requirements for collection of personal information of children under the age of 13, including obtaining verifiable parental consent.

⁹ The Health Insurance Portability and Accountability Act of 1996 creates national standards for protecting sensitive patient health information, and provides for express consent for disclosure of data.

¹⁰ The Gramm-Leach-Bliley Act establishes standards for financial institutions to safeguard and store customer information.

¹¹ See, e.g., Remarks at the Future of Privacy Forum by Christine S Wilson, Commissioner, United States Federal Trade Commission "A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation", 6 February 2020, available at www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf; and IAPP, "The first but not last comprehensive US privacy bill of 2021", 17 March 2021.

¹² California Consumer Privacy Act of 2018 [1798.100 - 1798.199] and Virginia Consumer Data Protection Act of 2021.

¹³ See Subcommittee on Antitrust, Commercial and Administrative Law of the Committee of the Judiciary, *Investigation of Competition in Digital Markets*, available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519; and *The Guardian*, 19 December 2020, 'This is big': US lawmakers take aim at once-unreachable big tech.

It is also a sign that authorities are realizing that the excesses of these companies can have undesirable effects on society, and may need to be addressed through government regulation. Moreover, recent bans on activities of some foreign digital companies (e.g. Huawei, TikTok and Grindr) in the United States market also point towards more interventions of the State in the markets and increased restrictions related to data and cross-border data flows, for national security reasons. Indeed, this may suggest that the United States is advocating for a free data flow policy for its companies around the world, and thus free foreign data inflows into the country, but at the same time imposing a policy of preventing foreign data-driven companies to enter the United States market and banning related domestic data outflows.

2. Promoting national and public security, and championing digital development: the approach of China

Contrary to the free-market approach of the United States, the Chinese economic and political system implies strong State intervention in the economy and society, which naturally translates into an approach towards State intervention in the digital economy, and therefore strict regulation of cross-border data flows. In China, policymakers control data and information, not only across borders, but also within the country, so as to maintain social stability and nurture knowledge-based sectors.

China has been exceptionally successful in building its domestic digital sector. This has been explained by a number of factors, such as limited foreign competition (which has been supported by the “Great Firewall”), the presence of a huge domestic market, weak domestic enforcement of intellectual property laws, adequate technological capabilities and resources, strong regulatory capacity, and strategic governmental and private investments in the digital sector (Foster and Azmeh, 2020). Digital development is a key component of the Made in China 2025 initiative, including subsidization of emerging Chinese platforms; huge government investments in emerging and next-generation digital technologies, such as AI and Internet of Things (IoT); and facilitating growth of Chinese companies in regional markets. The expansion of its domestic technological prowess and self-sufficiency in critical technologies also constitutes an important component of the agenda of the Government of China. Nevertheless, the country has made recent moves on competition policy, responding to the strong market power of some companies – for example, with a record fine to Alibaba of \$2.8 billion after an antitrust investigation.¹⁴

The Chinese regulatory model on cross-border data flows is based on the central role of cybersecurity in national security (Lee, 2018; Liu, 2020) and is, therefore, highly restrictive. At the same time, China stands out as an exceptional example of success among developing countries, as its restrictive model, coupled with several strategic government interventions, has stimulated growth of the domestic digital market and further led to the global success of several Chinese technology companies, such as Baidu, Alibaba, Meituan Dianping and Tencent. Thus, even though the predominant rationale for cross-border data regulation in China is national security and social stability, the economic agenda has become more central and critical to its data regulation policies over time. This was translated into an initial focus on data inflows regulations for national security and surveillance reasons (Nussipov, 2020a), and also to increase interest in restricting outflows. However, the protection of privacy has not been a major priority, and China is a major player in terms of mass digital surveillance (see chapter I).

China has introduced various restrictions on cross-border data flows in its domestic laws. For instance, its domestic cybersecurity law requires “critical infrastructure” providers to store “important data” and “personal information” within China.¹⁵ The term “critical infrastructure” is defined broadly and ambiguously to include public communications services, energy, transport, water conservation, finance, public services, e-government affairs or anything else where data loss, destruction or leakage can “result in serious damage to state security, national economy and people’s livelihood and public interests”.¹⁶ Further, cross-border transfers of personal data by critical infrastructure providers are subject to

¹⁴ *The Verge*, 10 April 2021, China fines Alibaba \$2.8 billion after antitrust investigation.

¹⁵ Article 37, Cybersecurity Law (China).

¹⁶ Article 31, Cybersecurity Law (China).

extensive security assessment by the regulators.¹⁷ Additionally, in order to ensure public security and facilitate regulatory access to data, China imposes several sector-specific data localization regulations, including for health information,¹⁸ information collected by credit investigation organizations,¹⁹ personal information collected by commercial banks,²⁰ Internet map service organizations,²¹ personal information and business data collected by online taxi platform companies²² and Internet bicycle rental operators,²³ and a general restriction on the cross-border transfer of State secrets.²⁴

The Chinese approach to preserving cybersovereignty has evolved over the years to include hardware regulation (controlling how data flow across networks – for instance, data exchange in Internet exchange points (IXPs)), software regulation (such as access to virtual private networks) and data/content regulation (Gao, 2019). Further, China exercises strong control over Internet/data standards used in domestic technologies, which indirectly increases sovereign control over data flows (Hoffman et al., 2020). Indeed, China is working on standardization issues in the technology sector, with a view to influencing global standards, through the “China Standards 2035” initiative. For instance, it has proposed a new IP protocol system at the International Telecommunication Union, which could change the way data flow.²⁵ The Government has also proposed a regulation that would require traffic to be routed locally if a user in China accesses a local website (Bennett and Raab, 2020).

Currently, China is in the process of finalizing its data protection framework, which proposes that one of the following conditions must be satisfied for cross-border transfer of personal data: (a) the data transfer must pass a security assessment by the Government; (b) the Government has provided a personal information protection certification for the data transfer; (c) the data transfer is in accordance with an international agreement; and (d) the data transfer meets any other conditions specified in the regulations.²⁶ Further, this law includes a clear data localization mandate – all critical information infrastructure operators and notified personal information handlers must store personal information collected by them domestically.²⁷ Moreover, the Government will seek international agreements for the transfer of personal data, and mutual recognition for standards of personal information protection.²⁸

The economic interest of China in the digital market may explain the subtle shift in the country's previously non-negotiable stance on cross-border data flows in recent months. For instance, in 2020, it indicated its willingness to permit cross-border data flows in the Hainan free trade zone.²⁹ Similarly, in another statement, the Government indicated the importance of international coordination on data security, and rejected a “one-size-fits-all” stipulation for local data storage, to ensure national security in a digitally-driven global economic environment (Liu, 2020:94).³⁰ A driver for the policy shift of China on commercial data flows could be to facilitate the digital component of the Belt and Road Initiative (BRI)

¹⁷ Draft Measures on Security Assessment of Cross-Border Transfer of Personal Information (China).

¹⁸ Article 10, Population and Healthcare Management Measures (China).

¹⁹ Article 24, Regulation on the Administration of the Credit Investigation Industry (China).

²⁰ Article 6, Notice to Urge Banking Financial Institutions to Protect Personal Financial Information (China).

²¹ Article 34, Regulation for the Administration of the Map (China).

²² Article 27, Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (China).

²³ Article 4(13), Guiding Opinions of Encouraging and Regulating the Development of Internet Bicycle Rental (China).

²⁴ Article 48, Law of the People's Republic of China on Guarding State Secrets (2010 Revision) (China).

²⁵ For a discussion on the new IP proposal, see Internet Society (2020b); on the “China Standards 2035” initiative, see Datenna, “China Standards 2035: A Global Standard for Emerging Technologies”, 15 June 2020, available at <https://www.datenna.com/2020/06/15/china-standards-2035-a-global-standard-for-emerging-technologies/> and Rühlig (2020).

²⁶ Article 38, Personal Information Protection Law (China).

²⁷ Article 40, Personal Information Protection law (China).

²⁸ Article 12, Personal Information Protection law (China).

²⁹ *The Diplomat*, 4 June 2020, Is China Changing Its Thinking on Data Localization?

³⁰ In fact, as Liu indicates, the Standing Committee also proposed a provision in the Chinese cybersecurity law that allows for data flows consistent with an international treaty.

known as the Digital Silk Road, which was launched in 2015 (Liu, 2020). This is a major strategy for China to expand its influence globally in the data-driven digital economy, as discussed below.

3. Guarding individual rights and fundamental values: the approach of the European Union

Contrary to the approach of the United States, which focuses on control of data by the private sector, and that of China, for the control of data mainly by the Government, the European Union emphasizes the control of data by individuals. Accordingly, it takes a strong regulatory approach towards the data-driven digital economy, which is based on the protection of fundamental rights and values of the European Union. In this sense, it is regarded as a human-centric approach.³¹ Thus, regulations on cross-border data flows are relatively strict and focus heavily on protecting the privacy of individuals. The European Union aims to build a single digital market within its borders, where digital products as well as data are free to flow under a set of rules to protect individuals, businesses and Governments from abuses arising from data collection, processing and commercialization.

Regulation of the digital economy and data in the European Union has taken place mostly in a defensive or reactive manner, as it aims to address the concerns stemming from the activities of global digital platforms – for example, on issues related to abuses of market power, competition or taxation, in addition to the protection of data. As highlighted in UNCTAD (2019a) and in chapter I of this Report, most global digital platforms are based in the United States and China, while digital platforms based in the European Union are relatively marginal. In recent years, the European Union has been taking a more proactive stance to develop the data-driven digital economy, with multiple policy initiatives in this context. The European Union is also characterized by looking at the different policies in the digital economy in a more integrated approach than in the rest of the world.³²

The General Data Protection Regulation (GDPR) of the European Union, which entered into force in 2018, is one of the most comprehensive frameworks for data protection in the world, containing extensive requirements for transferring personal data outside the region. However, no explicit restriction exists for cross-border transfers of non-personal data in the European Union. GDPR is applicable to the processing³³ of any “personal data”, which is defined as “any information relating to an identified or identifiable natural person”.³⁴ The fundamental approach of GDPR is that personal data can be transferred and processed outside the European Union only if there is full compliance with the privacy rights provided to its citizens.³⁵ To that effect, personal data transfers are automatically allowed only to a specific group of countries and territories that the European Commission has endorsed as having data protection frameworks that are essentially equivalent to GDPR (“adequacy finding”).³⁶ The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.³⁷ These adequacy findings have resulted from long bilateral negotiations, with the European Commission taking into account several factors in the foreign economies, including

³¹ See the European Union, “Principles for a human-centric, thriving and balanced data economy”, available at https://dataprinciples2019.fi/wp-content/uploads/2019/09/Dataprinciples_web_1.0.pdf.

³² See “Europe’s Digital Decade: digital targets for 2030”, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#documents.

³³ Processing is defined broadly in GDPR (article 4(2)), as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

³⁴ Article 4(1), GDPR.

³⁵ Recital 101, GDPR.

³⁶ Article 45(1), GDPR.

³⁷ The evolution of the situation with regard to adequacy findings can be consulted at “Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection”, available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

their data privacy/protection frameworks, respect for the rule of law, international commitments to data protection, and the strength of their economic and political relationship with the European Union.³⁸

Transfer of personal data to non-European Union countries that have not obtained positive adequacy findings is possible in only two ways: (a) if the data processor can offer “appropriate safeguards”, including binding corporate rules (BCRs) that allow intracompany transfers, standard contractual clauses (SCCs) approved by the European Commission for intercompany transfers, and certification mechanisms approved by the European Union;³⁹ or (b) if one of the following derogations apply: the data processor obtains explicit consent from the data subject for the transfer after informing him/her about the risks, where the data transfer is necessary for performance of a contract, to protect important public interests, to protect vital interests of the data subject, or if the transfer is made from a public register.⁴⁰ However, these derogations can be used only in specific situations, and not for regular day-to-day cross-border data transfers.

Although GDPR is a regulation applicable to personal data within the European Union, it has an extraterritorial effect, as it applies to all activities of controllers or processors in the Union, “regardless of whether the processing takes place in the Union or not”.⁴¹ The term “controller” refers to a body that determines “the purposes and means of the processing of personal data”,⁴² while the term “processor” refers to a body “that processes personal data on behalf of the controller”.⁴³ Due to this provision, even if a company does not have a physical presence in the European Union, it is required to comply with GDPR if its business activities include offering digital products/services within the Union or monitoring the behaviour of its residents.⁴⁴ However, there may be some challenges to this extraterritoriality in terms of enforcement (Greze, 2019).

In recent years, the European Union has put some emphasis on the objective of “digital sovereignty”. This is due to several factors, such as the predominance of United States and Chinese companies in the digital technology sector, and the need to reduce dependence on external technologies in the absence of successful European technology companies. It also reflects concerns regarding the ability of the European Union to ensure privacy of its citizens, and the security risks associated with foreign technologies (Hesselman et al., 2020). For instance, the inability of European Union Governments to develop indigenous contact tracing apps during the COVID-19 pandemic, and their dependence on technologies designed by Google and Apple, were considered to be major constraints on their digital sovereignty. While no clear definition of “digital sovereignty” exists in European Union policy, it can be considered to refer broadly to securing and protecting digital infrastructure in Europe, and addressing privacy rights of Europeans, including giving European Union citizens the right to decide where, how and by whom their personal data are used (Christakis, 2020).⁴⁵ The objective of digital sovereignty is reflected in a recent European initiative, first proposed by the Governments of France and Germany, called GAIA-X⁴⁶ (box IV.1).

Digital integration has been one of the focus areas of European policymakers in recent years, with initiatives such as the Digital Single Market. The European Data Strategy is a key pillar of these efforts; in this context, the Data Governance Act has been proposed to improve the availability of data and to strengthen data-sharing mechanisms across the European Union. It contains specific provisions for

³⁸ Article 45(2), GDPR.

³⁹ Article 46(2), GDPR.

⁴⁰ Article 49, GDPR.

⁴¹ Article 3(1), GDPR.

⁴² Article 4(7), GDPR.

⁴³ Article 4(8), GDPR.

⁴⁴ Article 3(2), GDPR.

⁴⁵ See also Statement by European Commission President von der Leyen at the round table event “Internet, a new human right”, after the intervention by Sir Berners-Lee, 28 October 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_1999.

⁴⁶ See “GAIA-X. A federated data infrastructure for Europe”, available at www.data-infrastructure.eu/GAIA-X/Navigation/EN/Home/home.html.

Box IV.1. GAIA-X

GAIA-X is an international non-profit organization based in Belgium. It was proposed by the Governments of Germany and France in 2019 to enable a federated cloud infrastructure for the European market to facilitate interoperable data exchange in the European Union under the protection of its laws, and has become a European initiative. It aims to set up a “high-performance, competitive, secure and trustworthy data infrastructure for Europe” that achieves the “highest aspirations in terms of digital sovereignty while promoting innovations”. It therefore aims to build a federated data infrastructure for Europe based on open and interoperable standards facilitating a single data market in the European Union, which in turn can boost the ability of European cloud providers to monetize data and, in the long run, entrench the position of European digital companies in the market.

The initiative promotes the European idea of digital sovereignty based on transparency, openness, data protection and security. It is aimed at creating a secure and robust infrastructure and ecosystem in the European Union to facilitate data exchange across European industries and thereby support the growth of data-driven sectors within Europe by enabling AI, IoT and Big Data analytics.

The GAIA-X initiative is open to foreign companies, but they must abide by the principles and policies followed by their European Union counterparts under the initiative. Some of the expected outcomes of this initiative are facilitating data-driven infrastructure in Europe, promoting domestic companies, increasing compliance with European values, and reducing excessive dependence on American and Chinese technology companies. It is expected that the project will become a tool to boost the digital sector in the European Union, while enhancing the ability of its Governments to ensure adoption of European Union privacy standards. The initiative is coming into form in 2021.

Source: UNCTAD, based on Project GAIA-X, available at www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6; BMWI, GAIA-X A Federated Data Infrastructure for Europe, available at www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html; The Financial Times, 21 December 2020, Regulation alone will not strengthen Europe’s digital sector; and Special Meeting of the European Council (1 and 2 October 2020) – Conclusions (point 9), available at <https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf>.

transfer of non-personal data to non-European Union countries, following a similar approach to the adequacy framework under GDPR. While the requirements are not equivalent to data localization per se, they impose a strict framework for the cross-border transfer of public data outside the European Union.⁴⁷

Given the importance of data flows among the European Union and the United States, in 2016 they entered into a transatlantic agreement for cross-border transfer of personal data, the European Union–United States Privacy Shield, to enable those transfers. This agreement replaced the European Union–United States Safe Harbour Scheme, which had been invalidated by the European Court of Justice in the *Schrems I* case in 2015. Under the Privacy Shield, companies could self-certify to be GDPR-compliant, and thereafter transfer data from the European Union to the United States. However, a decision of the European Court of Justice in *Schrems II* invalidated it in July 2020.⁴⁸ In this dispute, the court found that data surveillance laws in the United States were inconsistent with GDPR (box IV.2).

⁴⁷ See European Data Strategy, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en; and Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN>. There are two other related proposals, the Digital Services Act and the Digital Markets Act (see the Digital Services Act package, available at <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>).

⁴⁸ *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems (Case C-311/18, “Schrems II”)*.

Box IV.2. Privacy Shield and the Schrems II decision

In July 2020, the European Court of Justice in *Schrems II* invalidated the Privacy Shield for being inconsistent with European Union data protection laws. In particular, it found that the data surveillance laws in the United States did not provide equivalent protections to those in the European Union, and were inconsistent with the rights guaranteed in the European Union, such as Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333. Additionally, the Court of Justice held that, although the standard contractual clauses (SCCs) were a valid mechanism for personal data transfers to non-adequate countries, supplementary measures may be necessary to ensure that personal data of Europeans were protected. Subsequently, in November 2020, the European Data Protection Board provided some clarifications on supplementary measures.

In the aftermath of the decision, data transfers are no longer allowed under the Privacy Shield Agreement. Several industry associations and experts have criticized the *Schrems II* decision, as it creates new uncertainties for all companies using the SCCs. Further, although the European Court of Justice adopted an invasive approach in examining surveillance laws in the United States, similar standards do not apply to individual members of the European Union. The United States responded that the court failed to take into account several oversight mechanisms in the surveillance laws of the United States and the availability of redressal mechanisms to affected individuals under the Foreign Intelligence Surveillance Act.

Some experts argue that, as a result of *Schrems II*, foreign companies will find it harder to operate in the European Union without local processing, and thus the decision facilitates a form of “soft data localization” (Chander, 2020). Recent industry surveys have also indicated some adverse economic impacts of the decision, especially for small-sized companies, both within the European Union and elsewhere (DigitalEurope et al., 2020). Further, businesses have expressed concerns regarding the requirement for implementing “supplementary measures” for SCCs. Although the European Data Protection Board subsequently issued guidelines for SCCs (European Data Protection Board, 2020), they do not provide sufficient clarity, and introduce additional constraints on cross-border transfer of personal data to non-adequate countries, such as enhanced encryption requirements (Christakis, 2020).

Source: UNCTAD.

The European Union does not favour data localization per se in its laws.⁴⁹ For instance, GDPR recognizes the importance of cross-border flows of personal data for promoting international trade and international cooperation.⁵⁰ But given the strict requirements in GDPR, there is no easy way for cross-border data flows, as few countries have been granted adequacy. Moreover, certain recent developments – such as the Data Governance Act, the decision of the European Court of Justice in *Schrems II*, as well as the GAIA-X initiative – may suggest that the European Union is shifting in its position on data localization. Indeed, these initiatives may have an impact on the trade policy of the European Union; as stated by the European Commission (2021:15): “The question of data will be essential for the EU’s future. With regard to cross-border data transfers and the prohibition of data localisation requirements, the Commission will follow an open but assertive approach, based on European values and interests. The Commission will work towards ensuring that its businesses can benefit from the international free flow of data in full compliance with EU data protection rules and other public policy objectives, including public security and public order. In particular, the EU will continue to address unjustified obstacles to data flows while preserving its regulatory autonomy in the area of data protection and privacy.” Furthermore, in the context of the WTO negotiations, the European Union stated that “Members are committed to

⁴⁹ For example, in the Regulation for the Free Flow of Personal Data, members agree that “Member States should only be able to invoke public security as a justification for data localisation requirements”. See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, para. 18. Similarly, in several recent trade negotiations, such as with New Zealand and Australia, the European Union has proposed provisions prohibiting data localization measures.

⁵⁰ Recital 101, GDPR.

ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted by: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localization of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory".⁵¹

A summary of the main features of the data-related policies of the United States, China and the European Union is presented in table IV.1.

As will be discussed in section C, these are the three main approaches that have an impact at a global level. While the approaches of the Russian Federation and India are also presented in this section, their global influence is relatively limited. The Russian Federation has influence mainly at a regional level, as a leading economy and driver of digital development in the Eurasian Economic Union (Abramova and Thorne, 2021). And the approach of India is mostly focused on the domestic market, with no expansion ambitions so far, although the country is a strong voice among developing countries in international debates on issues related to the digital economy.⁵²

	United States	China	European Union
Economic growth and development in the data-based digital economy	Mainly market-based	Strong government intervention	Regulation; part of recovery plan after COVID 19 to support development of the digital economy
Data protection and privacy	Not historically prioritized; no comprehensive federal law (but discussions and proposals); state laws in California and Virginia	Rules focusing on business	GDPR, based on fundamental rights
National security	Data for national security are a clear priority	Wide government access and control	Each member responsible; European Union can overrule in certain circumstances
Competition policy	Data not typically seen as a competition issue; but tide turning with important antitrust investigations and court cases	Unclear if data are considered a competition issue; may support domestic and State-owned companies; recent antitrust fine to Alibaba	Data can be considered a competition issue
Cross-border data flows	Promote free data flow	Extensive restrictions to data flows	Free data flow within the European Union and adequate States; trade policy promoting free data flows, but some recent initiatives pointing to restrictions

Source: UNCTAD, partly based on Government Office for Science, United Kingdom (2020).

⁵¹ See Communication from the European Union, Joint statement on electronic commerce, EU proposal for WTO disciplines and commitments relating to electronic commerce (INF/ECOM/22), 26 April 2019, available at https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf (page 4).

⁵² Some countries – such as Kenya, Nigeria, South Africa and Rwanda – appear to be influenced by similar ideas to those on data localization in India (Elmi, 2020).

4. Promoting national and public security: the approach of the Russian Federation

Similar to the Chinese model, the Russian regulatory model on cross-border data flows is premised on the centrality of network and data security as a political and national security issue. The Russian Federation considers cybersecurity to be a purely sovereign prerogative (Nocetti, 2015). However, unlike China, the Russian Federation has not put such a strong focus on the economic agenda for digital development, and has been relatively less successful in boosting the domestic digital sector, with some notable exceptions, such as Yandex (a search engine platform) and Kaspersky (a cybersecurity services and antivirus software provider).

The Russian Federation has imposed a series of restrictions on cross-border data flows. The most significant is a blanket data localization requirement for personal data, requiring all companies operating in the country to “record, systematize, accumulate, store, amend, update and retrieve personal data of all Russian nationals, using Russian servers”.⁵³ The Federal Service for Supervision of Communications, Information Technology and Mass Media clarified that, to comply with this provision, any company whose business activities are focused on the country (including having a Russian language website or offering pricing in roubles) should initially record and store personal data in local servers as master copies and, thereafter, may mirror these data in foreign servers (Savelyev, 2016).⁵⁴ Further, several domestic laws include strong information controls, including providing access to encrypted data, as and when required by law enforcement officials (Maréchal, 2017). The Russian Federation recently adopted a suite of amendments to its federal laws “On Communication” and “On Information, Information Technologies, and Information Protection” (often referred as the “Sovereign Internet Law” in the international media), requiring all Russian Internet providers to install equipment to route all domestic Internet traffic through servers located within the country.⁵⁵ Additionally, these amendments allow for the implementation of a Russian domain name system that would enable the domestic Internet to function, even when disconnected from the global network (Epifanova, 2020).

Unlike China, the Russian Federation has not had an economic strategy to develop its domestic digital sector until very recently; its Digital Economy Programme was established in 2017 (Lowry, 2020). Some experts argue that the Government considers technological self-sufficiency necessary to the extent that it is required to establish a sovereign domestic industry free from foreign influence; however, there is no sustained ambition for Russian digital companies to compete in the global market (Budnitsky and Jia, 2018). The most successful digital platform in the Russian Federation is Yandex, which represents approximately 55 per cent of the domestic search engine market; Yandex is considered superior to the Google search engine because of its exceptional Russian language capabilities.⁵⁶ Other companies, such as Mail.ru and Avito, have seen moderate success in the domestic market (Eferin et al., 2019). Russian platforms do not have a large market outside the country, and are popular only in some Russian-speaking countries.

⁵³ Article 18(5), Federal Law No. 152-FZ on Personal Data as Amended in July 2014 by Federal Law No. 242-FZ on Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks (Russian Federation).

⁵⁴ As per Federal Law No. 152-FZ On Personal Data (Russian Federation), cross-border transfers are only allowed to countries that have signed the Council of Europe Convention 1981, or countries that have been expressly approved by the regulator (Angola, Argentina, Australia, Benin, Canada, Chile, Costa Rica, Gabon, Israel, Japan, Kazakhstan, Malaysia, Mali, Mongolia, Morocco, New Zealand, Peru, Qatar, the Republic of Korea, Singapore, South Africa and Tunisia).

⁵⁵ *The BBC News*, 1 November 2019, Russia Internet: Law introducing new controls comes into force, available at www.bbc.com/news/world-europe-50259597.

⁵⁶ *CNBC*, 21 January 2019, Google is the most popular search engine in most of the world except Russia – here's why, available at <https://www.cnbc.com/2019/01/18/yandex-is-beating-google-in-russia.html>.

5. Championing domestic digital development: the approach of India

In contrast to the above-mentioned models on cross-border data flows, India is increasingly shifting towards a regulatory model primarily focused on maximizing the economic and social benefits of data and data-driven sectors for its citizens and the domestic economy, and minimizing revenue flows to companies based in digitally advanced economies. The underlying idea behind this approach is shielding India from “data colonialism”, i.e. preventing rich countries from deriving benefits from cross-border data flows at the cost of hurting the interests of India (Weber, 2017).

The Personal Data Protection Bill 2019⁵⁷ and the Draft National E-Commerce Policy (entitled “India’s Data for India’s Development”),⁵⁸ both clearly outline the ambition of India to build its digital sector by capitalizing on the data of Indian people through data localization measures. The Personal Data Protection Bill contains data localization requirements, as it requires a copy of sensitive personal data to be stored in India,⁵⁹ and further prohibits cross-border transfers of critical personal data.⁶⁰ Sensitive personal data are defined as (a) financial data, (b) health data, (c) official identifier, (d) sex life, (e) sexual orientation, (f) biometric data, (g) genetic data, (h) transgender status, (i) intersex status, (j) caste or tribe, (k) religious or political belief or affiliation, or (l) any other data categorized as sensitive personal data by the Government.⁶¹ Given the broad definition of sensitive personal data, the proposed legislation creates a greater compliance burden for companies compared with the current legal regime (under which data can be transferred to any country providing the same level of protection as India, provided the transfer is necessary for the performance of an existing contract, and the user has consented to such transfer).⁶² The Government can consider any data as falling within the scope of “critical personal data”, because this term is not defined.⁶³ Further, this bill emulates the approach of GDPR in permitting cross-border transfers of personal data only in limited circumstances: to countries for which the Government expressly allows transfers (adequacy approach); subject to approval of intra-group data transfer schemes; consent of the data subject; or based on specific necessity, as approved by the regulator.⁶⁴

The Draft National E-Commerce Policy⁶⁵ envisages broad data localization measures, although it does not include any explicit restrictions on cross-border flows of non-personal data. However, more recently, a report by the Committee of Experts on Non-Personal Data, established by the Ministry of Electronics and Information Technology, has recommended data localization requirements for some categories of non-personal data (in a manner similar to the Draft Data Protection Bill): general non-personal data can be stored and processed anywhere in the world; sensitive non-personal data can be transferred outside the country, but must be stored in India; and critical non-personal data can be stored and processed only in India.⁶⁶ Data localization requirements also apply to data collected using public

⁵⁷ Personal Data Protection Bill (India), available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

⁵⁸ Draft National E-Commerce Policy: India’s Data for India’s Development, 2019, available at https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

⁵⁹ Section 33(1), Personal Data Protection Bill (India).

⁶⁰ Section 33(2), Personal Data Protection Bill (India).

⁶¹ Section 3(36), Personal Data Protection Bill (India).

⁶² Rule 7, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (India).

⁶³ Section 33(2), Explanation, Personal Data Protection Bill (India).

⁶⁴ Section 34, Personal Data Protection Bill (India).

⁶⁵ Still being revised at the time this Report was prepared.

⁶⁶ Ministry of Electronics and Information Technology, Report by the Committee of Experts on Non-Personal Data Governance Framework (August 2020), para. 7.6 and recommendation 6(ix), available at <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

funds,⁶⁷ subscriber information collected by broadcasting companies,⁶⁸ electronic books of accounts,⁶⁹ and policyholder information collected by insurance companies.⁷⁰

A key motivation behind the various proposed data regulations in India appears to be protecting the country's economic interests by ensuring that local digital data are primarily used to develop domestic digital start-ups (or “data champions”), and thereby push back against the “data colonialism” of big technology companies.⁷¹

In addition to protecting economic interests, the regulatory approach of India on cross-border data flows is informed by the various advantages of data localization for ensuring effective regulatory oversight and enforcement of domestic laws. For instance, India requires all payment system providers to store data relating to payment systems in India (even if such data are processed abroad) so that the Reserve Bank of India can “have unfettered supervisory access to data stored with these system providers as also with their service providers/intermediaries/third party vendors and other entities in the payment ecosystem”.⁷² In the context of personal data protection, the Srikrishna Committee report stated that “effective enforcement” of Indian privacy law would “invariably require data to be locally stored within the territory of India, and this would mean that such a requirement, where applicable, would limit the permissibility of cross-border transfers” (Srikrishna Committee Report, 2018:87). However, requiring data localization for legal purposes also complements the domestic economic development logic behind the regulatory approach of India towards data governance, i.e. if more data can be stored within India, then it will lead to better domestic digital infrastructure for emerging digital technologies such as AI and IoT (Srikrishna Committee Report, 2018).

Certain civil society bodies have expressed concerns that the Draft Data Protection Bill does not contain adequate checks and balances, especially because any governmental agency can be exempted from the law.⁷³ Therefore, while the data protection bill enshrines tough compliance requirements for private companies, including for cross-border transfers of personal data, it remains unclear if the proposed law will be equally effective in protecting individuals from government surveillance (Burman, 2020).

C. GLOBAL EXPANSION STRATEGIES BY THE UNITED STATES, CHINA AND THE EUROPEAN UNION

With the realization of the enormous potential economic and strategic value of data that can be created thanks to digital technological progress, the United States, China and the European Union are very active in globally expanding their approaches towards the data-driven digital economy; they seek to capture as much of the gains from data as possible. Their expansion approaches match the logic of their domestic regulations. In the United States, it is mainly driven by the expansion of its global digital corporations, supported by the free flow of data and bans on data localization requirements in trade agreements (see chapter VI). In China, the Government-driven Belt and Road Initiative (BRI) supports the expansion of its global digital and telecommunications giants to other countries. Powerful digital corporations in these countries seek new markets, where many potential customers are not yet connected to Internet markets. As most of the population in developed economies and China is well connected, and their data are already largely under their control, potential new users and related access to new data are mainly in developing

⁶⁷ National Data Sharing and Accessibility Policy (India), 9 February 2014, available at <https://dst.gov.in/national-data-sharing-and-accessibility-policy-0>.

⁶⁸ Consolidated FDI Policy 2017 (India).

⁶⁹ Rule 3(5), Companies (Accounts) Rules, 2014 (India).

⁷⁰ Rule 18, IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017 (India).

⁷¹ See, for example, Sinha and Basu (2019); *The Print*, 29 September 2019, ‘Digital colonialism’: Why countries like India want to take control of data from Big Tech; and *Mint*, 20 January 2019, India’s data must be controlled by Indians: Mukesh Ambani.

⁷² RBI Notification on Storage of Payment Systems Data (India), RBI/2017-18/153, DPSS.CO.OD No.2785/06.08.005/2017-2018, 6 April 2018, available at www.rbi.org.in/scripts/NotificationUser.aspx?ld=11244.

⁷³ Section 35, Personal Data Protection Bill (India).

economies; they are often referred to as the “next billion users” (Pisa and Polcari, 2019; Arora, 2019). By contrast, the European Union strategy focuses mainly on exporting regulatory frameworks.

These expansion strategies would basically aim to extend influence on the global data-driven digital economy, to increase power stemming from controlling data, which in turn allows controlling markets and the society. In the case of the United States and China, given their technological dominance, a major objective is to set global standards on data-related technologies. The European Union mainly seeks to influence global regulatory standards. While these expansion strategies towards developing countries may allegedly be grounded in international cooperation, humanitarian or development-oriented motivations, there seems to be motivation for extracting data from those countries to create value from their processing. Thus, there is an extractive logic in these expansion strategies, which is similar to the experiences of developing countries that have specialized in natural resources production; it would result in an unequal exchange, as countries that provide raw data become highly dependent on those that extract and control them, making them flow out to foreign countries. The latter have the technological capacity to capture the value of data by converting them into digital intelligence. However, developing countries would need to pay for the imports of those data products, which could support their development, created in part on the basis of raw data originally generated domestically.⁷⁴

Global digital corporations in the United States have applied different programmes to improve Internet access in developing countries, such as Facebook Free Basics or Google Project Loon. They are also heavily investing in digital infrastructure in developing countries. For example, Facebook is leading the project “2Africa”, which is building an undersea cable around Africa to connect 23 countries in Africa, West Asia and Europe by 2023.⁷⁵ While these initiatives and infrastructure investments may bring some benefits to developing countries in terms of connectivity, it is not evident that they outweigh the costs (see also chapter III). They are likely to lead to an outflow of domestically generated data to companies in the United States, affecting their capacities to innovate and capture value by processing them. Thus, there are rising concerns on this new form of “colonialism” through data (Elmi, 2020), which can create challenges related to data privacy, disinformation and reinforcing market concentration and inequalities (Pisa and Polcari, 2019). These corporations also expand worldwide by acquiring successful digital start-ups and potential competitors (UNCTAD, 2019a), affecting the ability of domestically grown companies to contribute to long-term development.

China seeks to contribute to South–South cooperation and expand its influence via BRI, which brings together traditional infrastructure with digital technologies that reflect the values and standards of China. The Digital Silk Road (DSR) aims, among other things, to expand the growth of Chinese tech companies – such as Alibaba, Tencent and Huawei⁷⁶ – to foreign markets, which often also expand through acquisitions of foreign companies, as in the case of the United States. It also aims to increase Chinese investments in digital and telecommunications infrastructure, such as digital trade zones and smart city projects, in foreign countries (Triolo et al., 2020).⁷⁷

The success of the projects under DSR depends on the widespread adoption of Chinese data-driven technologies and services in BRI countries, and interconnectivity across China and BRI countries, all

⁷⁴ For discussions on the extractive logic of the data-driven digital economy, see Morozov (2017), and Gurumurthy and Chami (2020).

⁷⁵ See Facebook, “Building a transformative subsea cable to better connect Africa”, available at <https://engineering.fb.com/2020/05/13/connectivity/2africa/>.

⁷⁶ For example, it has been reported that Huawei has built more than 70 per cent of the 4G networks in Africa (see, The Africa Report, “Huawei’s African business could be hurt by US blacklisting”, 22 May 2019).

⁷⁷ See *Nikkei Asia*, 24 November 2020, China Rises as World’s Data Superpower as Internet Fractures, available at https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-Internet-fractures?utm_source=CSIS+All&utm_campaign%E2%80%A6; George Magnus, “Will digital diplomacy cement the Belt and Road Initiative’s ‘common destiny’?” 17 September 2020, available at <https://blogs.lse.ac.uk/cff/2020/09/17/will-digital-diplomacy-cement-the-belt-and-road-initiatives-common-destiny/>; Robert Greene and Paul Triolo, “Will China Control the Global Internet Via its Digital Silk Road?” 8 May 2020, available at <https://carnegieendowment.org/2020/05/08/will-china-control-global-Internet-via-its-digital-silk-road-pub-81857>. For more detailed recent discussions on the Digital Silk Road, see Ly (2020); CFR (2020); Dekker, Okano-Heijmans and Zhang (2020); and Eder, Arcesati and Mardell (2020).

of which require data to flow between China and BRI members. According to Erie and Streinz (2021), China shapes transnational data governance by supplying digital infrastructure to emerging markets through DSR, in what they call the “Beijing effect”. In economic terms, these investments also imply benefits, including in terms of development (Arcesati, 2020; Gong, Gu and Teng, 2019), as well as costs for developing countries from losing control of their data to a foreign country. Moreover, a political dimension is added in the Chinese approach, as there are fears that Chinese technologies may support government surveillance over the population in developing countries (Kurlantzick, 2020; CFR, 2020).

Contrary to the global expansion strategies of the United States and China, which are based on their technological leadership, the European Union mainly relies on its regulatory leadership. For example, GDPR may be becoming a global model for data protection (box IV.3).

Some experts argue that, through GDPR, the European Union intends to export its privacy norms abroad and emerge as a global “regulatory champion” (Ciuriak and Ptashkina, 2018). This has been termed the “Brussels effect”; for example, the recent European proposal for a legal framework on AI (which is closely linked to data), is seen with a view to “provide Europe with a leading role in setting the global gold standard”.⁷⁸

The European Union is also establishing partnerships with developing countries. One example is the Africa–Europe Digital Economy Partnership. Indeed, in the context of international partnerships for the digital decade, the digital targets for 2030 include “The EU will promote its human-centred digital

Box IV.3. GDPR as a global standard for data protection?

GDPR is extending its global reach through various routes. First, to comply with GDPR, several companies have made significant changes to their global data processing and business models, and consequently offer such privacy protections worldwide (Chakravorti, 2018). Second, as a comprehensive framework, GDPR has become a model for several developing countries that have recently adopted or are in the process of devising their data protection laws. As of 2018, 67 out of 120 countries outside the European Union have adopted GDPR-like laws (Srikrishna Committee Report, 2018). Third, in addition to achieving desired levels of data protection, several countries adopting GDPR-like laws nurture the hope of achieving a positive adequacy finding from the European Commission in the future, which can increase access of their home-grown companies to European markets (Christakis, 2020). However, the enforcement of GDPR-like rules requires significant regulatory resources, and may not be consistent with the realities on the ground in many developing countries (Chakravorti, 2018). Further, GDPR-like rules on data transfer are likely to entail high compliance costs and could be especially unaffordable for micro-, small and medium-sized enterprises (MSMEs) in developing countries. Indeed, it has been argued that GDPR is a poor fit for lower-income countries, because of its complexity (Pisa et al., 2020).

In the case of Latin America, for example, the 1995 European Data Protection Directive had already spurred some countries to gain adequate status in order to exchange data flows. But the momentum leading to the implementation of GDPR served to catalyse debates and reassess the current level of adequacy in protection, in light of the ubiquitous presence of digital communications technologies connecting more productive sectors, as well as due to the revisionism on how data are collected and processed, which emerged in 2013 after Edward Snowden’s declarations (ECLAC and I&JPN, 2020). The implementation of GDPR has prompted more adaptation, which is still being considered in many jurisdictions in the region. Current status of adequacy to GDPR from countries in the region includes three States (Argentina, Mexico and Uruguay); and in the case of Caribbean territories, Guadeloupe and Martinique are under the scope of GDPR (Bleeker, 2020). GDPR has inspired the legislations of Brazil, Panama and Barbados that have recently been approved and which will be seeking adequacy with that standard in the short term (Rodríguez and Alimonti, 2020).

Source: UNCTAD.

⁷⁸ See Bradford (2020) and The Brussels Effect, “How the European Union rules the world”, available at www.brusselseffect.com/; European Commission, “A European approach to Artificial intelligence”, available at <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>; and *The Economist*, 24 April 2021, The EU wants to become the world’s super-regulator in AI.

agenda on the global stage and promote alignment or convergence with EU norms and standards.”⁷⁹ This implies that, once regulations become similar to those of the European Union, data will freely flow among the European Union and the corresponding countries.

Whatever the global expansion strategy is, it is up to developing countries to evaluate the net developmental benefits that may eventually emerge. They should assess the positive effects in terms of improvements in infrastructure and connectivity, or data-related regulations, against the costs of relinquishing their data to entities based in foreign countries, losing their ability to derive value from the data.

D. RISKS AND IMPACTS OF A POTENTIAL FRAGMENTATION IN THE DIGITAL SPACE

1. Fragmentation or convergence?

The discussions in previous sections indicate that prevailing and most influential worldwide approaches towards the digital economy and regulations on data governance are quite different from each other, and also differ in their global influence. Policies on cross-border data flows vary according to economic, social, political, institutional and cultural views and values. Most prominently, the “cybersovereignty model” advocated by China and the Russian Federation is in sharp contrast to the “free flow of information” model advocated by the United States. Further, the digital sovereignty model of the European Union is not aligned with the United States model of data governance. Finally, emerging developing economies such as India are advocating for digital economic development and data regulation models premised on keeping data inside national borders, which contradict the free flow of information, and are distinct from the Chinese or European regulatory model.

These differences have raised fears about the possibility of fragmentation of the Internet and the data-driven digital economy. For example, one of the main global risks highlighted in 2020 (WEF, 2020c) was fragmentation in the digital economy. Fragmentation of the Internet has many interrelated approaches. A heuristic approach was developed by Drake, Cerf and Kleinwächter (2016), who described the forces leading to a fragmentation of the Internet in terms of political, commercial and technical perspectives. According to these authors, political fragmentation addresses issues such as cybersovereignty, national sovereignty and cyberspace, e-commerce and trade, content and censorship, national security, data localization and privacy, and data protection. Commercial fragmentation is produced by peering and standardization procedures, the non-protection of net neutrality, walled garden approaches, geolocation and geoblocking mechanisms, and by the enforcement of intellectual property rights. Technical fragmentation is produced by tinkering with the DNS and IP addresses, mostly the so-called critical Internet resources. De Nardis (2016), on the other hand, has classified approaches to Internet fragmentation considering the infrastructure, logical and content layers. While these different perspectives and layers could be fairly separated in earlier times of the Internet, with the increasing digitalization of more and more activities and areas of life, economy and society, and higher interconnections, the boundaries among them have become increasingly blurred. This is also due to major global digital platforms being able to play a prominent role over the whole Internet and digital space, including networking infrastructure (chapter I). Therefore, Internet fragmentation and digital economy fragmentation would be becoming joint processes.

The impact of the conflicting models on the Internet, digital technologies and data governance is well demonstrated by geopolitical tensions at the international level. The most notable are the ongoing technology and trade tensions between the United States and China. While China has historically followed a restrictive approach and banned several United States-based services, and instead promoted local digital platforms and services, the United States has in recent years started taking a more aggressive

⁷⁹ See European Commission, “Africa–Europe Alliance: European Commission and African Union Commission welcome the Digital Economy Task Force report”, available at <https://digital-strategy.ec.europa.eu/en/news/africa-europe-alliance-european-commission-and-african-union-commission-welcome-digital-economy>; and European Commission, “Europe’s Digital Decade: digital targets for 2030”, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

stance towards Chinese technology companies. The Clean Network Programme, discussed above, is one such example. Some have suggested that this programme, targeted at removing untrustworthy Chinese apps and services from the network in the United States, and reducing the Chinese presence in the United States telecommunications networks and undersea cables, will ultimately contribute to Internet fragmentation.⁸⁰

The recent suite of measures adopted by the Russian Federation to disconnect from the global network is also indicative of growing Internet fragmentation.⁸¹ Another example is the ban on Chinese applications in India. Finally, although the European Union has remained a supporter of a free and open Internet, the highly prescriptive application of GDPR rules on cross-border transfer of personal data (e.g. the *Schrems II* case) and the assertion of digital sovereignty to safeguard policy space for European Governments to regulate for protecting European values (e.g. Data Governance Act and the GAIA-X initiative) can also be seen as a potential threat to an integrated digital trade ecosystem.

These tensions, particularly between the United States and China, are based on the search for worldwide digital and technological leadership or supremacy, and the objective to set global standards. As control of data and AI technologies leads increasingly to control of the economy and the society, this is basically an issue of global economic and political power. However, while in terms of winners and losers, there could be a winner in such a “race”, it is highly unlikely that this would benefit the overall population of the planet. It is likely that a cooperative solution would give better results from a global perspective.

While the diversity in approaches at the national level would suggest that fragmentation could be a possibility, from the discussions above, some convergence can be found when taking a dynamic perspective of the different approaches. As will be discussed in more detail in chapter V, when looking at the specific regulations on cross-border data flows, all countries tend to have economic growth and development, privacy and data protection and national security as major objectives. What changes is the priority given to each of these three objectives and how the regulations are applied. In the case of the United States, in spite of its free market focus, it is moving towards more defensive interests, as shown above. China is hinting towards some opening of its data flows. And the initially defensive interests of the European Union are moving towards industrial policies resembling those of China. Thus, the respective approaches seem to be pointing towards a moderation of positions and turning slightly towards more balanced approaches, which might hint at hope in finding some basic common ground between the main players.

The final outcome of whether the Internet and the digital economy will fragment is uncertain, and depends largely on the will of policymakers worldwide to find a global solution that benefits all. A divided approach to data governance could eventually lead to a world of “divergent data nationalism”, where countries adopt inward-looking data policies with no international consensus, resulting in reduced opportunities for digital innovation and development across the world (Government Office for Science (United Kingdom), 2020). This fragmentation is likely to lead to a suboptimal outcome, where it would not be possible for the potential benefits of the data-driven economy, which are mostly based on the flow of data, to materialize.

2. Impact of fragmentation on developing countries

A potential fragmentation in the data-driven digital economy may create difficulties for technological progress, with reduced competition, oligopolistic market structures in the different areas, and stronger influence of the Government. It would reduce business opportunities, as the access of users and companies to supply chains would become more complicated, and data flows would be restricted across borders. Also, there would be more obstacles for collaboration across jurisdictions, which would become less reliable (Feijóo et al., 2020).

⁸⁰ See, e.g., *Forbes*, 17 September 2020, CFIUS and a Tale of Two Internets, available at www.forbes.com/sites/riskmap/2020/09/17/cfius-and-a-tale-of-two-internets/?sh=5c37db2439fb.

⁸¹ See Internet Governance Project, 16 May 2019, “A closer look at the ‘sovereign Runet’ law”, available at www.internetgovernance.org/2019/05/16/a-closer-look-at-the-sovereign-runet-law/; *Wired*, 6 June 2019, Russia and Iran Plan to Fundamentally Isolate the Internet.



The three data behemoths – the United States, China and the European Union – have each created distinct data realms, which creates problems of compatibility or interoperability among them, severely impeding the ability to devise global rules to govern cross-border data flows and, thereby, create a level playing field for all countries. For those countries outside these dominant “data realms” (except for a few exceptions, such as India and the Russian Federation), this means that, as rule-takers, they will likely have to choose which of the models of data governance to follow if divergence continues to grow (Aaronson and Leblond, 2018).

To enhance their access to data and their market dominance, the United States, China and the European Union seek to bring other countries under their realm through instruments such as trade agreements or capacity-building, or in exchange for market access. Officials in smaller or less advanced countries will likely feel compelled to choose one realm over the others, because they already have significant trade relations with that market, or because they favour that realm’s approach to data governance. For many countries, however, it will prove difficult, if not impossible, to choose, since they have significant economic relations with more than one realm. Consequently, those countries’ Governments will try to delay for as long as possible before aligning themselves with one particular realm. Thus, developing countries would be trapped in making choices that would affect other economic relations.

For instance, Latin American countries often have to choose between the GDPR model and the United States model with regard to regulation of cross-border data flows and data protection rules; given that their economic interests are aligned with both these blocs, most Latin American countries face a tough choice (Aguerre, 2019). Several countries in Africa now appear to be aligning with the Chinese model of cybersovereignty,⁸² but they also have ties with the European Union and the United States. China has stronger influence in many Asian developing countries. The traditional allies of the United States have been encouraged to take a tough stance against Chinese companies, such as excluding Huawei from their telecommunications networks and banning social media apps such as TikTok.⁸³

In terms of infrastructure, less points of interconnection to the global network resulting from Internet fragmentation would entail increased costs and overall lower efficiency; fragmentation would also lead to a reduced ability to participate in the network effects of the dynamics of a relatively global interconnection. Given the high degree of interconnection and interdependence with global content and service providers in many developing countries, there may be significant implications for local companies and users affected by the fragmentation of Internet services.

Divergent “data nationalism” will be especially inimical to the interests of developing countries, including LDCs. First, it will result in suboptimal domestic regulations, especially in developing countries with low regulatory capacity, resulting in adverse consequences for privacy and security, and prejudicing the interests of domestic Internet users, as will be discussed in the following chapter. Second, a fragmented Internet reduces market opportunities for domestic MSMEs to reach worldwide markets, which may instead be confined to some local or regional markets. Third, divergent data nationalism reduces opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation. Finally, a world of divergent data nationalism has only a few winners and many losers. Certain established digital economies may emerge as winners due to their advantageous market size and technological prowess, but most small, developing economies will lose opportunities for raising their digital competitiveness.

However, in the absence of a properly functioning international system of regulations of cross-border data flows that allows maximizing benefits from data, while addressing the risks, in a way that income gains are equitably distributed, the only option for developing countries is to regulate their data flows at the national level. The following chapter explores in some detail specific policies on cross-border data flows, with a view to mapping the different national measures that countries can adopt to regulate cross-border data flows.

⁸² *The Diplomat*, 23 February 2019, How China Exports Repression to Africa.

⁸³ See, for instance, Rodrik (2020); and *The Guardian*, 13 July 2020, Europe divided on Huawei as US pressure to drop company grows.

This chapter maps national policies that are in place around the world to govern cross-border data flows. National regulations in this area vary considerably and can be placed along a regulatory spectrum from strict data localization to virtually free flows of data. The approach taken tends to reflect differences in countries' technological, economic, social, political, institutional and cultural conditions.

Regulations on cross-border data flows are based on various public policy reasons, including those related to the protection of privacy and other human rights, law enforcement and national security, as well as economic development objectives. Countries use a range of legal and regulatory instruments. Finding the appropriate model for regulating data flows in each country thus remains a challenging policy choice. A holistic balancing exercise to reach different regulatory outcomes based on a complex interplay of domestic and international factors is particularly important for developing economies to maximize the potential benefits of the digital economy and ensure greater welfare of their citizens.

MAPPING NATIONAL POLICIES ON CROSS-BORDER DATA FLOWS

V

CHAPTER V THERE IS NO ONE-SIZE-FITS-ALL APPROACH TO REGULATE CROSS-BORDER DATA FLOWS

Conditions determining national approaches to governing data and data flows



Public policy reasons to regulate cross-border data flows



Legal instruments to regulate cross-border data flows may include references to:



Regulatory spectrum for cross-border data flows

Strict data localization	Partial data localization	Conditional transfer: Hard	Conditional transfer: Intermediate/soft	Free flow of data
Restrictive or guarded approach		Prescriptive approach		Light-touch approach

Developing countries need to find the **optimal balance** between promoting domestic economic development, protecting public policy interests and integrating into the global digital ecosystem

A. INTRODUCTION

The rapid digitalization of the economy and datafication of the society have prompted Governments across the world to adopt wide-ranging regulations on cross-border data flows. Zooming in from the worldwide landscape of major data governance trends presented in chapter IV, including on cross-border data flows, this chapter discusses specific measures to regulate cross-border data flows in countries around the world. The country sample considered is not exhaustive; for example, in some countries, particularly LDCs, such regulations may not have been developed. However, it is representative of the variety of measures and motivations of different countries – with a diversity of technological, economic, political, institutional and cultural conditions – to regulate these flows, as well as where they are positioned in the regulatory spectrum.

While some countries strictly restrict cross-border data flows, others have adopted more nuanced compliance frameworks for regulating the transfer of data across their borders. Such regulations may be sector-specific, data category-specific, or apply broadly to several sectors of the economy and across different data categories. This chapter explores the varying regulatory frameworks by categorizing cross-border data regulations of countries in various ways, and then evaluating their advantages and disadvantages. It also provides a mapping of national regulations in this area.

Depending on the political, economic, social, technological and cultural values, as well as ideological context, in different countries, the motivations for regulating cross-border data flows may differ or overlap. Some of the key policy objectives include promoting domestic economic growth; maximizing the socioeconomic benefits of data-driven technologies; engendering trust in the domestic digital economy; addressing serious public policy challenges, such as privacy violations and surveillance; minimizing cyberthreats (especially in critical infrastructure); and building resilient and secure cyberinfrastructure. Further, some Governments seek guaranteed and timely access to data for regulatory oversight and law enforcement purposes by imposing data localization measures. Finally, several countries believe that their cross-border data regulations are essential tools for establishing and maintaining their “data sovereignty” or “cybersovereignty” – i.e. sovereign control over the domestic Internet and data flows. Regulations intended to increase sovereign control over the domestic Internet, however, can also be used for increasing governmental surveillance of domestic Internet users. Different concepts of relevance in the context of these regulations are defined in box V.1.

Developing robust, balanced and relevant regulatory frameworks on cross-border data flows is one of the most critical policy challenges in the digital economy. Governments need to assess the domestic benefits and risks pertaining to cross-border data flows, both at societal and individual levels. For instance, cross-border data flows can benefit societies by strengthening the realization of certain human rights, providing individuals with greater choice of competitive online services, and enabling companies to make economically efficient choices (Kuner, 2013; WEF, 2020b; Freedom House, 2020). At the same time, Governments need to address critical threats to data, including privacy and cybersecurity risks. Further, the “built-in potential for market failure” in data-driven sectors – including “network externalities, economies of scale and scope, and pervasive information asymmetry” (Chen et al., 2019:6; Ciuriak, 2019, 2020) – raises very complex policy concerns in data regulation. Governments should also ensure equitable access to data, as they constitute an “essential capital stock” for emerging digital technologies such as artificial intelligence (AI) and Internet of Things (IoT) (Ciuriak and Ptashkina, 2018). This challenge is particularly enormous for LDCs with poor digital infrastructure, weak digital capabilities and limited regulatory capacity.

Section B of this chapter categorizes cross-border data flow regulations in various ways, including by the type of data, the sectors affected and the degree of restrictiveness. It then discusses examples in each category from numerous countries, specifically identifying the policy rationales behind the regulations and potential risks from the perspective of regulatory effectiveness, economic development and global data governance. Section C maps the domestic regulatory frameworks on cross-border data flows along a regulatory spectrum, based on their degree of restrictiveness – i.e. ranging from a “light-touch” approach, to a “prescriptive” approach, to a “restrictive” or “guarded” approach – and then explains existing regulatory trends. Section D provides some conclusions.

Box V.1. Concepts related to national policies on cross-border data flows

Certain concepts and terms are commonly found in regulatory models on data governance. A plain language explanation of these terms is included below:

- *Data localization* refers to the requirement to store data in and/or process data using local servers. Data localization is also often referred to as data residency.
- *Cybersovereignty* broadly refers to the control exercised by States over various aspects of Internet and Internet-related activities – including digital content, digital infrastructure and digital services – inside their borders. Unlike multistakeholder models of Internet governance, cybersovereignty places the State at the heart of Internet governance.
- *Data or information sovereignty* refers to States controlling all data flows through the Internet (i.e. within and to and from their territory) to ensure, inter alia, that all data generated and processed within the State are subject to national laws and can be appropriated in any manner that the State deems fit.
- *Data protectionism* refers to the regulation of data flows by Governments to create competitive benefits for the domestic sector, including by adversely affecting level playing competitive conditions for foreign players.
- *Data nationalism* refers to policies that aim to ensure that domestic data are used primarily to benefit national interests.

Source: UNCTAD.

B. DOMESTIC MEASURES ON CROSS-BORDER DATA FLOWS AND THEIR POLICY IMPLICATIONS

Based on a review of regulations on cross-border data flows,¹ this section first examines the varied rationales for regulating cross-border data flows from three different perspectives – citizens' protection policy, national security and economic development – covering a variety of regulatory objectives, such as data protection, cybersecurity, protecting State secrets, safeguarding public/government data from foreign surveillance, ensuring access to data for regulatory needs and law enforcement, and facilitating the growth of the domestic digital sector. Next, this section proposes different ways of categorizing such regulations, using various examples from across the world. Finally, it analyses the domestic policy implications of regulations on cross-border data flows from different perspectives, outlining the various complex policy choices involved in adopting a governance framework for cross-border data flows.

1. Policy rationales behind regulating cross-border data flows

This section outlines the different policy reasons for Governments to regulate cross-border data flows, so as to broadly understand the current geopolitical views and sociopolitical perspectives affecting how different countries govern data flows. For a more systematic understanding, the section examines underlying policy rationales from three different perspectives: (a) citizens' protection policy lens, (b) national security lens, and (c) economic development lens. In practice, a country's regulatory framework on cross-border data flows can be based on policy rationales falling under overlapping lenses.

¹ In selecting the sample of countries for the review, various factors were considered to ensure that the sample is representative in nature: geography/location of the country, level of development of the country, type of data regulations, regulatory motivations and information accessibility. A detailed literature review was also conducted, and then the references to the relevant laws and policies were cross-checked for accuracy. The list of regulations reviewed is presented in the online annex to chapter V, available at https://unctad.org/system/files/official-document/der2021_annex2_en.pdf. As mentioned in chapter IV, the Report reflects the situation as of early 2021.

a. Citizens' protection policy lens

Several regulations on cross-border data flows often relate to objectives of Governments to protect the interests of their citizens, such as privacy and data protection, cybersecurity, stronger regulatory oversight and law enforcement. Many countries restrict or regulate cross-border data flows to ensure compliance with their domestic data protection laws. In practice, very few countries impose explicit restrictions on the cross-border transfer of non-personal data, unless such data relate to highly sensitive sectors. While anonymized data sets transferred in digital transactions constitute non-personal data, several domestic laws define personal data to include any information relating to an “identifiable” person (such as General Data Protection Regulation (GDPR), article 4(1)). Data analytics tools have made it easier to deanonymize individuals in such data sets (Ohm, 2010); thus, the scope of personal data can be broad.

Typically, any restriction on the cross-border transfer of personal data is motivated by two objectives: (a) ensuring that companies (foreign or domestic) dealing with personal data of citizens are unable to circumvent any obligations contained in domestic data protection laws – for instance, by transferring the data to countries with more lenient laws (Bygrave, 2002; Kuner, 2013); and (b) protecting the right to privacy of individuals (including constitutional rights, if applicable), and providing consumers with adequate remedies for breach of their consumer rights, including financial losses and massive privacy breaches. The latter objective is especially critical for sensitive sectors such as health and finance; therefore, several countries impose localization or conditional transfer requirements in these sectors.

Some countries – such as China, Viet Nam, Indonesia, Saudi Arabia and Turkey – mandate localization of data in critical infrastructure sectors or, more broadly, for government data. Given the importance of security of government and critical infrastructure data, and their increasing reliance on computer networks, these Governments prefer local storage of data to ensure the highest degree of data security and resilience of their domestic infrastructure. In fact, as data-driven technologies grow further, especially in IoT and AI, several countries are also expected to introduce stringent data transfer restrictions in their cybersecurity laws and policies, in order to safeguard the security of data.²

To a certain extent, the fear regarding the security implications of IoT and AI-driven technologies is unsurprising, given that such technologies are still nascent; are highly susceptible to cyberthreats; and drastically affect several sectors – such as communications, transport and finance – which many countries rightly consider sensitive (Ciuriak, 2019). However, a distinction must be drawn between regulations aimed at technical security concerns related to digital technologies (for example, protecting networks from cyberthreats or ensuring integrity of networks, which may relate to day-to-day commercial threats or graver threats to critical cyberinfrastructure) and those aimed at broader political and national security concerns, including those related to national security and economic sovereignty, as explained below. While there is some overlap between technical security and national security concerns (for instance, cyberthreats to critical or defence infrastructure are also legitimate from a national security perspective), national security can be conceived more broadly to include ideas of social stability, economic security and self-sufficiency, and political control over domestic users (Mishra, 2020a; Roberts et al., 2019).

Further, several countries impose restrictions on cross-border data flows, including explicit localization requirements (strict or partial) in sensitive sectors, to ensure immediate and predictable access to data, if and when needed for regulatory oversight or law enforcement purposes. A common problem that many law enforcement agencies face across the world is gaining immediate access to data stored in foreign jurisdictions, given the cumbersome process for getting access to data stored abroad.³ The CLOUD Act in the United States (see chapter IV) illustrates the concerns arising from data being located in foreign jurisdictions. Scholars have also argued that data localization measures may be necessary to “increase the effectiveness of law enforcement” and “grant governments more jurisdictional control over data” (Sargsyan, 2016:2223). Further, Governments may be concerned if the personal data of their citizens are subject to laws in foreign jurisdictions that do not provide the

² See, for example, Essential Cybersecurity Controls (Saudi Arabia).

³ *The Economist*, 5 November 2016, Online governance: Lost in the splinternet.

same level of protection to their domestic users. For instance, in their digital transformation strategy, members of the African Union set out an objective of adopting national laws on data localization to protect the privacy of their citizens and residents (African Union, 2020). Countries in Latin America do not impose local presence requirements, but national law enforcement agencies, notably in the case of Brazil in recent years, are increasingly favourable to such approaches. Yet this tends to apply jurisdictional concerns on the location of conduct rather than on the location of data storage (ECLAC and I&JPN, 2020).

b. National security/sovereignty lens

Several regulations on cross-border data flows may be viewed through a national security and domestic sovereignty lens. As data technologies become widespread and integrated with various spheres of life, many Governments are increasing their interests in data as a strategic asset. Thus, control over data flows can be an important part of a country's defence against illegitimate foreign surveillance, whether commercial or governmental, as well as a useful tool for monitoring the digital activities of its residents. This may further include controlling the digital content on domestic networks (Sacks and Sherman, 2019). As discussed in chapter IV, the approaches of China and the Russian Federation towards the governance of data flows are premised on this idea, and extend well beyond the idea of technical security concerns to issues of social stability, technological/economic self-sufficiency and political control. Further, the Russian Federation has even amended its existing laws, allowing the Government to cut off the Russian Internet from the global network by rerouting all traffic through local servers.

Since the disclosure by Edward Snowden in 2013 of global surveillance programmes, several Governments have implemented restrictions on cross-border data flows to help ensure protection from foreign surveillance (Hill, 2014). Additionally, some Governments are motivated to maintain their sovereign control over data to protect their economic, political, social, cultural and religious values, although the human rights implications of such extreme localization measures can be severe (Taylor, 2020). For instance, data localization obligations imposed on social media/network service providers could provide Governments easier access to user data.⁴ If such data are misused, it may result in potential human rights violations, given the strengthened surveillance capability of Governments and the enhanced ability of domestic security and intelligence agencies to track citizens and, particularly, target political dissidents.⁵

c. Economic development lens

In addition to the political/security and citizens' protection policy lenses presented above, regulations on cross-border data flows can also be informed by an economic development rationale. As discussed in chapter IV, the approach of India to cross-border data flows regulation is increasingly shaped by economic development considerations. This policy rationale of promoting domestic economic development and building indigenous data champions is also implicit in laws and policies of several other developing countries, such as Kenya,⁶ South Africa (Barnes et al., 2019), Pakistan⁷ and Rwanda.⁸

⁴ See, for example, restrictions on social media enforced in Pakistan, the Russian Federation and Turkey.

⁵ See Report of the Office of the United Nations High Commissioner for Human Rights, *Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), paras 2, 3, 14, 42; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40 (17 April 2013), para. 33.

⁶ The Kenyan data protection act contains a provision that allows the Government to demand localization of personal data for the protection of revenue. See section 50, Data Protection Act, 2019 (Kenya).

⁷ The Pakistan Electronic Commerce Policy 2019 envisages various measures for data localization and cross-border data flow regulation in IoT-related sectors and commercial data. Available at www.commerce.gov.pk/wp-content/uploads/2019/08/Draft-E-Commerce-Policy-Framework-Final-23-8-19.pdf.

⁸ In its Data Revolution Policy, Rwanda views data as a "national sovereign asset". The document also sets out the ambition of Rwanda to build a robust data industry. See Data Revolution Policy (Rwanda), available at <http://statistics.gov.rw/file/5410/download?token=r0nXaTAv>.

Even digitally developed countries sometimes impose certain restrictions on cross-border data flows, arguably, *inter alia*, to shield their home-bred companies from foreign competition.⁹

Given that digital markets are often based on winner-take-all dynamics (Farrell and Newman, 2019; Ciuriak, 2018) coupled with the lack of inclusive digital economy growth in many developing countries (World Bank, 2016; UNCTAD, 2019a), several countries believe that targeted industrial policies in the digital economy are essential for catch-up (Azmeah and Foster, 2016) and to avoid an unhealthy dependence on American and Chinese technology companies (Elmi, 2020; Sherman and Morgus, 2018). Further, as digital investments tend to be asset-light, many companies based in developed countries do not make extensive investments in local infrastructure, even when they derive significant revenues from providing services in the domestic market (Casella and Formenti, 2018). As an example, Africa and Latin America taken together account for only 4 per cent of the world's co-location data centres (see chapter I). Further, with the exception of some Chinese platforms, no other technology company from developing countries has been able to establish a global market presence.

Given the importance of enormous amounts of data in developing AI and other data-driven technologies, some developing countries, such as India, are now focusing on the development of domestic data capabilities as a means to capture more of the revenue flowing to foreign digital companies, and thereby boosting the growth of their domestic digital sectors (Singh, 2018b; Jain and Gabor, 2020). In such countries, preventing the transfer of massive volumes of data on residents to foreign companies through strict data localization laws and policies is seen as a potential route to encourage the growth of domestic data facilities and massive data sets. This growth in data capabilities may in turn facilitate the development of domestic digital products and services for growing domestic consumer demand, thereby powering the growth of home-bred digital companies. However, as discussed below, data localization cannot per se facilitate development of successful digital platforms in developing countries.

A summary of the various reasons for countries to regulate cross-border data flows through the three lenses is presented in table V.1.

Table V.1. Reasons for countries to regulate cross-border data flows		
Protection of citizens	National security/sovereignty	Economic development
Data protection and privacy	Address foreign surveillance	Build domestic data champions
Cybersecurity	Protect critical infrastructure	Ensure equitable access to data
Regulatory oversight over sensitive sectors	Increase sovereign control over domestic Internet	Address local demand through local products and services
Access to data for law enforcement	Social/cultural stability	
Data ethics	Political stability	

Source: UNCTAD.

2. Categories of national regulatory measures on cross-border data flows

Regulations on cross-border data flows can be devised and implemented in various ways. Based on a broad evaluation of regulatory measures across the world, this section categorizes such regulations based on specific criteria: (a) scope of application: applicable generally or to cross-border data flows in

⁹ See, for example, Made in China 2025, available at www.csis.org/analysis/made-china-2025; Announcing the Expansion of the Clean Network to Safeguard America's Assets, 5 August 2020, available at <https://mr.usembassy.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/>.

specific sectors; (b) extent of restriction: strict localization; partial localization; conditional transfer – hard, intermediate and soft; free flow of data; and (c) with respect to specific restrictions on cross-border flows of personal data: accountability and adequacy approach.

a. *Scope of application*

Regulations on cross-border data flows can apply generally across all/most sectors, or may be limited to data collected and processed in specific sectors. Several countries have adopted data protection laws regulating cross-border transfers of personal data; as personal data flows are common to most sectors, such measures have a “general” scope of application. GDPR is a prime example (chapter IV). Similarly, as discussed before, several countries partially or completely replicate the approach of the European Union in regulating cross-border flows of personal data.¹⁰ For example, in Latin America, normative frameworks for data protection are the most relevant instruments that explicitly address the issue of cross-border data flows. In general terms, the region evinces a regime of conditional restrictions to cross-border data flows in those cases where there is national data protection legislation in place, which is the current trend in more than half of the countries involved.

Additionally, some countries impose regulatory approval requirements for cross-border transfers of personal data.¹¹ In certain rare scenarios, countries also impose a strict requirement to store and/or process personal data within the country. For instance, a provision in the Draft Data Protection Law in Rwanda requires data controllers/processors to host/store personal data in Rwanda;¹² if this law is adopted, then even if personal data are processed abroad, companies will be required to store them in Rwanda. Specific requirements for local storage and processing of personal data have also been proposed in the draft data protection law in China (chapter IV).¹³

In contrast, several countries use sectoral regulations of cross-border data flows. For instance, Australia, China, the United Arab Emirates and the United Kingdom expressly prohibit cross-border data flows in the health sector to safeguard patient confidentiality.¹⁴ Other sector-specific regulations related to both data confidentiality and security are restrictions on the cross-border transfer of web mapping data in China and the Republic of Korea.¹⁵ The United States similarly requires defence-related data to be stored in domestic cloud servers (chapter IV).¹⁶ Finally, several countries require local data storage in

¹⁰ Some examples include Argentina, Armenia, Bahrain, Barbados, Brazil, Colombia, Georgia, Israel, Malaysia, Peru, South Africa, Switzerland, Turkey and Ukraine.

¹¹ See, for example, article 44, Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data (Algeria); article 43, Law No. 09-08 of 18 February 2009 (Morocco); and article 54, Draft Data Protection Law (Rwanda).

¹² Article 55, Draft Data Protection Law (Rwanda).

¹³ Article 40, Personal Information Protection law (China) (applicable to critical infrastructure operators and notified personal information handlers).

¹⁴ See, for example, section 77, Personally Controlled Electronic Health Records Act (Australia); article 10, Population and Healthcare Management Measures (China); Health Data Law 2019 (United Arab Emirates); National Health Service and social care data: off-shoring and the use of public cloud services guidance 2018 (United Kingdom), available at <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services>.

¹⁵ See, for example, article 16, Act on the Establishment, Management, etc. of Spatial Data (Republic of Korea); article 34, Regulation for the Administration of the Map (China).

¹⁶ United States Department of Defense, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, DFARS Case 2013-D018, available at www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for.

sectors requiring stronger regulatory oversight, such as financial data,¹⁷ insurance data,¹⁸ electronic payments,¹⁹ telecommunications data²⁰ and gambling data.²¹

b. Level of restrictiveness

Regulations can also be categorized based on their degree of restrictiveness.

i. Strict localization

Strict localization refers to a legal requirement to store and/or process data in the country, and may potentially include a complete prohibition on cross-border data transfers (even for the purposes of processing). Some countries impose strict localization requirements that can affect the economy at large. For example, China has imposed strict data localization requirements for personal information and important data collected by operators of critical infrastructure,²² potentially implicating a large volume of cross-border data flows. The cybersecurity law in Viet Nam contains a broad and strict localization provision that requires all foreign and domestic suppliers of telecommunications, as well as Internet services (including over-the-top services) offered online to store data locally.²³

In some other countries, localization requirements can be applied very broadly, subject to the regulator's discretion. For example, in Kenya, the Government has the power to require personal data to be processed "exclusively through servers or data centres located in Kenya based on grounds of strategic interests of the state or protection of revenue"; if implemented very ambiguously or broadly, this provision can potentially become a broad localization requirement.²⁴ Similarly, India and Pakistan plan to explicitly prohibit cross-border transfers of "critical personal data" and require that such data be stored and processed locally, without providing a specific definition of this term;²⁵ therefore, if the term "critical personal data" is subsequently defined broadly by the Governments, this requirement would affect large volumes of data flows.

¹⁷ See, for example, section 12, Consolidated Act No. 648 of 15 June 2006 (Denmark); article 6, Notice to Urge Banking Financial Institutions to Protect Personal Financial Information (China).

¹⁸ See, for example, Rule 18, IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 (India) (applicable to policyholders of insurance companies).

¹⁹ See, for example, para. D6.1, Regulatory Framework for Stored Values and Electronic Payment Systems (United Arab Emirates); RBI Notification on Storage of Payment System Data (India); article 23, Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions, Law No. 6493 (Turkey).

²⁰ See, for example, German Bundestag Passes New Data Retention Law, 16 October 2015, available at www.gppi.net/2015/10/16/german-bundestag-passes-new-data-retention-law; Federal Law No. 374 on Amending the Federal Law "on Counterterrorism and Select Legislative Acts of the Russian Federation Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety" (2016) (Russian Federation); Guidelines for Nigerian Content Development in Information and Communication Technology (Nigeria), available at <https://nitda.gov.ng/regulations/>.

²¹ See, for example, article 15B(vi), Law No. 124 of May 2015, regarding the approval of the Government Emergency Ordinance no. 92/2014 regulating fiscal measures and modification of laws (Romania).

²² Article 37, Cybersecurity Law (China).

²³ Article 26.3, Cybersecurity Law (Viet Nam). A recent report, however, indicates that the Government intends to apply this provision only to those companies that fail to act after receiving notifications regarding violation of the law. See *The Business Times*, 15 October 2019, Data localisation requirements narrowed in Vietnam's cybersecurity law.

²⁴ Section 50, Data Protection Act, 2019 (Kenya).

²⁵ Section 33(2), Personal Data Protection Bill (India); section 14.1, Draft Data Protection Bill (Pakistan).

Some countries impose strict localization requirements for specific data categories, including health,²⁶ defence,²⁷ IoT,²⁸ and mapping data²⁹ and, more broadly, for critical government and public data.³⁰ Other examples of strict localization requirements relate to business records,³¹ tax records³² and accounting records.³³ The localization requirements related to business or accounting records are often legacy laws, i.e. implemented at a time when all records were stored physically on paper or in local computers rather than on cloud servers. Therefore, some experts argue that these laws may be less suited to the current digital age, where most records are stored in the cloud (WEF, 2020b:13).

ii. Partial localization

Partial localization refers to a legal requirement to store data locally, but does not include a prohibition on transferring or storing copies of the data abroad, although specific compliance requirements may be imposed for cross-border data transfer and storage. For example, the Russian Federation and Kazakhstan require companies to store a copy of personal data locally, even if they can otherwise be transferred abroad.³⁴ Turkey and Pakistan require social media companies to store all user data locally, although there is no express prohibition on cross-border transfers.³⁵ Certain provinces in Canada require personal information collected by public bodies to be stored locally, although these data may be transferred abroad in certain cases, such as upon obtaining consent of the data subject.³⁶

iii. Conditional transfer – hard, intermediate or soft

A conditional transfer requirement means that data can be transferred abroad subject to the data processor complying with specified regulatory requirements. Depending on the design of these compliance requirements, conditional transfers may be categorized as hard, intermediate or soft.

Compliance requirements for cross-border data transfer are extremely common in data protection laws. Hard conditional transfers entail a comprehensive compliance regime that includes country-specific

²⁶ See, for example, section 77, Personally Controlled Electronic Health Records Act (Australia); NHS, NHS and Social Care Data: Off-Shoring and the Use of Public Cloud Services Guidance 2018 (United Kingdom).

²⁷ United States Department of Defense, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, DFARS Case 2013-D018, available at www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for.

²⁸ See, for example, para. 7, Internet of Things Regulatory Framework (Saudi Arabia).

²⁹ Article 16, Act on the Establishment, Management, etc. of Spatial Data (Republic of Korea); article 34, Regulation for the Administration of the Map (China).

³⁰ See, for example, Presidential Circular on Information and Communication Security Measures (July 2019) (Turkey) (applicable to critical information and data, such as civil registration, health and communication information, as well as genetic and biometric data); article 17, Ministerial order No. 001/MINICT/2012 of 12 March 2012 (Rwanda); Essential Cybersecurity Controls (Saudi Arabia) 27; United States Department of State, *2020 Investment Climate Statements: Algeria*, available at www.state.gov/reports/2020-investment-climate-statements/algeria/.

³¹ See, for example, German Commercial Code – section 257, Nos. 1 and 4 (Handelsgesetzbuch § 257) (Germany).

³² See, for example, article 315, Income Tax Code (Belgium); article 60, VAT Code (Belgium).

³³ See, for example, section 388(2), Companies Act 2006 (United Kingdom); Accounting Act (1336/1997) (Finland).

³⁴ See, for example, article 18(5), Federal Law No. 152-FZ on Personal Data as Amended in July 2014 by Federal Law No. 242-FZ on Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks (Russian Federation); article 12(2), Personal Data Law (Kazakhstan).

³⁵ Amendments to Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts, Law No. 5651, October 2020 (Turkey), available at <https://iapp.org/news/a/turkish-data-localization-rules-in-effect-for-social-media-companies/>; section 5(d), Citizens Protection (Against Online Harm) Rules, 2020 (Pakistan).

³⁶ Section 30(1), Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996 (British Columbia, Canada); section 5(1), Personal Information International Disclosure Protection Act, S.N.S. 2006 (Nova Scotia, Canada).

approvals for transfers (e.g. an adequacy approach), regulatory approvals for transfers,³⁷ approved contracts for transfers (e.g. standard contractual clauses (SCCs) and binding corporate rules (BCRs) provided under GDPR), and are subject to strict regulatory audit.³⁸ Where contract-based transfers are allowed, the regulator may require the processor to demonstrate that the recipient has implemented the appropriate measures to ensure compliance with domestic data protection laws.³⁹ A requirement common to several African countries is maintaining a register of all persons and institutions collecting personal data, including for the purposes of data collection and cross-border data transfers.⁴⁰

Even when hard compliance requirements are in place, countries often allow cross-border transfers of personal data in limited circumstances, such as where necessity-based derogations exist in the domestic data protection law (e.g. necessity to perform a contract, to protect public interest, or to protect vital interests of the data subject), or where due consent is obtained from the data subjects.⁴¹ Some data protection laws also contain specific exemptions for cross-border data transfers for governmental or law enforcement purposes,⁴² medical research purposes,⁴³ bank or stock transfers,⁴⁴ or in accordance with an international treaty.⁴⁵

Intermediate or soft conditional transfer requirements refer to easier compliance requirements, such as obtaining implicit consent of users or limited user notice requirements, or if data processors can conduct cross-border data flows subject to a self-assessment of the data protection framework of the recipient country with necessary contracts (i.e. if prescribed by law). For example, for transferring personal data abroad, the data protection law of Mexico only requires consent from the users and entering into necessary contracts between data processors and the foreign parties handling the personal data, but no other requirements for prior regulatory approval.⁴⁶ Further, cross-border data transfers within corporate groups are expressly allowed.⁴⁷ Similarly, in the Republic of Korea,

³⁷ See, for example, article 9, Law on the Protection of Personal Data No. 6698 (Turkey) (applicable when transfer is to a country without a sufficient level of data protection); article 14, Personal Data Protection Law No. 151 (Egypt); article 44, Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data (Algeria); article 48, Law No. 2004-63 dated July 27, 2004, on the Protection of Personal Data (Tunisia); article 5, Law No. 2013-450 dated 19 June 2013 on the protection of personal data (Côte d'Ivoire).

³⁸ In that regard, some countries require the registration of all databases and/or cross-border data transfers. See, for example, section 21, Law No. 25326 (Personal Data Protection Law) (Argentina); article 16, Law on the Protection of Personal Data No. 6698 (Turkey). See also article 22, Ministerial Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (Indonesia); article 6, Government Regulation No. 71 of 2019 (Indonesia) (a requirement is imposed on all private electronic systems operators in Indonesia to obtain approval from the Government to manage, process and store their data outside the country).

³⁹ See, for example, article 26, Decree No. 1377/2013 (Colombia); section 48, Data Protection Act, 2019 (Kenya).

⁴⁰ See, for example, article 29, Data Protection and Privacy Act 2019 (Uganda); article 21, Data Protection Act, 2019 (Kenya).

⁴¹ See, for example, article 49, GDPR; section 12, Law No. 25326 (Personal Data Protection Law) (Argentina); section 76, Data Protection Act 2018 (United Kingdom); article 29, Law of Ukraine No. 2297 VI "On Personal Data Protection" (Ukraine); section 48(c), Data Protection Act, 2019 (Kenya).

⁴² See, for example, section 12(2)(e), Law No. 25326 (Personal Data Protection Law) (Argentina); article 12(1)(j), Dubai International Financial Centre Data Protection Law, Law No. 1 of 2007; article 20(3), Personal Data Protection Act, Act 8/2005 (Macao, China); article 31(2)(b)(iii), Data Protection Act 2004, Act No. 13 of 2004 (Mauritius).

⁴³ See, for example, article 15, Personal Data Protection Law No. 29733 (Peru).

⁴⁴ See, for example, section 12, Law No. 25326 (Personal Data Protection Law) (Argentina).

⁴⁵ See, for example, article 15, Personal Data Protection Law No. 29733 (Peru); section 12, Law No. 25326 (Personal Data Protection Law) (Argentina); article 45, Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data (Algeria); article 41(2), Law of Georgia on Data Protection (Georgia).

⁴⁶ Article 8 read with article 36, Federal Law on the Protection of Personal Data Held by Private Parties (Mexico).

⁴⁷ Article 37.III, Federal Law on the Protection of Personal Data Held by Private Parties (Mexico).

companies are required to obtain consent from data subjects prior to “exporting”⁴⁸ personal data, but there are no other express prohibitions on data transfers.⁴⁹

iv. Free flow of data

The term “free flow of data” typically refers to regulations that do not impose any specific restrictions on cross-border data flows, although the regulations may contain rules for ex post accountability for companies – i.e. data processors remain accountable for ensuring that all their processing conducted abroad is consistent with the relevant domestic laws. For instance, in Canada, any company that transfers personal data abroad is responsible for ensuring compliance with domestic laws, but there are no express restrictions on such transfers. Instead, organizations are required to designate an individual who can be held accountable, to ensure compliance with domestic data protection laws.⁵⁰ Consent of the data subject is not necessary specifically for transferring data abroad, although organizations should include information in their privacy policies regarding transfer to foreign countries.⁵¹ Similarly, Australia,⁵² Singapore⁵³ and the Philippines⁵⁴ have endorsed the principle of accountability, thereby enabling a relatively free environment for cross-border flows of personal data. Many LDCs have not yet implemented a regulatory framework for data protection and, as such, have not imposed any regulations that affect cross-border data flows, i.e. data flow freely across borders by default as they remain unregulated.⁵⁵

c. Geographical versus accountability approach for personal data flows

Regulations often specifically apply to personal data, and can be roughly categorized as incorporating: (a) an adequacy approach (or geographically-based approach), where data transfers are regulated on the basis of the data protection standards/laws in the recipient country – for instance, the Government may determine which foreign countries have “adequate”, “sufficient” or “equivalent” data protection frameworks, thereby expressly allowing data transfers to such countries or approving transfers on a case-by-case basis; (b) an accountability (or organizationally-based) approach, where data transfers are based on the data “exporter” remaining accountable to the domestic Government and, by extension, to the users, for compliance with data protection standards, irrespective of where the data are transferred, stored or processed (Kuner, 2013). An accountability approach would require cross-border enforcement – i.e. where the data processor located abroad has acted in contravention of the requirements in the domestic law. For example, in Latin America, the trend is based on the adequacy approach.

In practice, a data protection framework could incorporate both an adequacy and accountability approach. For example, in the European Union, in addition to relying upon a positive adequacy finding, companies can conduct cross-border data transfers by using BCRs, SCCs or other approved certification mechanisms, or where such transfers are otherwise authorized by domestic laws (Kuner, 2013). The

⁴⁸ Quotation marks are added to show that this is the wording of the country, not of this Report, as data flows are not exports but outflows. This is the approach followed throughout this Report.

⁴⁹ Article 17(3), Personal Information Protection Act (Republic of Korea).

⁵⁰ Principle 1, schedule I, section 4.1.3, Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (Canada).

⁵¹ Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders*, January 2009, available at www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf.

⁵² Australian Privacy Principle 8, The Privacy Act 1988 (Australia).

⁵³ Section 26, Personal Data Protection Act (Singapore).

⁵⁴ Section 21, Data Privacy Act of 2012 (Republic Act No. 10173) (Philippines).

⁵⁵ For examples of LDCs that have not adopted any framework on data protection, see UNCTAD, *Cyberlaw Tracker*, available at <https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide>.

same holds true for many countries that have incorporated an adequacy approach.⁵⁶ Other countries – such as Canada, Singapore and Australia – rely on an accountability approach for cross-border transfers of personal data, as discussed previously.

3. Domestic policy implications of regulating cross-border data flows

This section examines the various advantages and disadvantages of different forms of regulations on cross-border data flows from a regulatory, economic development and global data governance perspective.

a. *The regulatory perspective: advantages and disadvantages*

While many regulations on cross-border data flows are adopted to achieve various legitimate policy or regulatory objectives, it is also necessary to evaluate the extent to which such measures can be effective in achieving these objectives, and whether they are proportionate to the underlying policy risks and associated costs of implementation.

At a general level, regulations on cross-border data flows suffer from some implementation challenges. First, as multiple government agencies are responsible for managing different dimensions of cross-border data flows (for example, trade, telecommunications, domestic industry and development, home affairs and Internet regulation), the possible overlap and lack of coordination between these agencies can lead to inconsistent and uncoordinated domestic regulations or policy positions on cross-border data flows (Chen et al., 2019). For instance, despite dealing with many overlapping issues related to the data-driven economy, data protection and information and communications technology (ICT), regulators rarely cooperate in practice (ITU, 2018). A recent proposal published by the Ministry of Electronics and Information Technology in India on non-personal data requiring anonymized data collected by big tech companies to be shared with the Government, citizens and other businesses demonstrates such a lack of coordination among different government agencies. This proposal raised concerns about possible conflicts with the jurisdiction of the Competition Commission of India.⁵⁷

Second, many countries deliberately frame their regulations on cross-border data flows ambiguously, to allow for unfettered administrative discretion. For instance, terms such as “critical data”, “important data”, “sensitive personal data”, “critical infrastructure”, “data sovereignty”, “digital/cybersovereignty” – although used in many policy documents and regulations – can have different meanings and contexts. For example, neither India nor Pakistan have defined what they mean by critical personal data. Some experts have also argued that the position of the European Union on “digital sovereignty” is ambiguous and makes the European Union stance on data localization confusing (Christakis, 2020). The definition of critical infrastructure similarly varies across different jurisdictions (OECD, 2019c). Consequently, the lack of clear and consistent definitions of key terms, including personal data and information, can lead to uncertainty and adversely affect both consumer and business interests, not least through higher compliance costs for multinational as well as smaller companies engaging in international trade.

Third, a related implementation challenge is the extent to which data protection laws apply to non-personal data. As most data sets used in business processing contain at least some personal data,⁵⁸ many small companies, without sufficient resources to store these two types of data separately,

⁵⁶ See, for example, article 26, Law 1581/2012 (Colombia); article 11, Personal Data Protection Law No. 29733 (Peru); article 33, General Data Protection Law (LGPD), Federal Law No. 13,709/2018 (Brazil); section 74, Data Protection Act 2018 (United Kingdom); article 29, Law of Ukraine No. 2297 VI “On Personal Data Protection” (Ukraine); article 12(1), Law No. 30 of 2018 with respect to Personal Data Protection (Bahrain); section 1, Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001 (Israel); section 28, Personal Data Protection Act (Thailand); section 129(1), Personal Data Protection Act (Malaysia); article 41, Law of Georgia on Data Protection (Georgia).

⁵⁷ *Bloomberg*, 22 September 2020, Mandatory Sharing Of Non-Personal Data At Odds With Competition Law.

⁵⁸ A survey conducted by the OECD showed that most businesses handled significant amounts of personal data, especially in sectors such as telecommunications, ICT and finance (Casalini and López González, 2019).

are forced to adopt the highest standard for the entire data set, leading to additional costs and reducing their overall competitiveness (WEF, 2020b; Casalini and López González, 2019).

Fourth, sector-specific regulations can entail practical implementation challenges. For example, several countries restrict the outflow of health data of individuals. But it is unclear if health data are limited to medical records, or if they include health-related information that can be tracked by IoT products such as smart watches, or by simply observing the browsing behaviour of individuals (Kavacs and Ranganathan, 2019).⁵⁹ Lastly, implementation and enforcement challenges at the institutional level are related to budgetary constraints and lack of political will. For example, in Latin America, the challenges arise not so much due to a lack of a normative or policy instrument, but rather to the difficulties to implement and enforce some of the legislation without the necessary human and institutional support.⁶⁰

From a technological perspective, location of data storage/processing does not ensure data protection or security per se; rather, privacy/data protection is a function of the underlying technologies and standards used in the data-driven sectors (Chander and Lê, 2014; Komaitis, 2017; Mishra, 2020b). Cyberthreats are global in nature and may even originate domestically. Thus, storing data domestically does not necessarily reduce vulnerability to cyberattacks. Indeed, it may further prejudice the security of data when localization is mandated in countries with poor digital infrastructure. In contrast, strong privacy and cybersecurity standards can help to protect data from intrusion, irrespective of where such data are stored. Moreover, forced data storage in countries where Governments can demand backdoor access to such data facilitates government surveillance. On the other hand, personal data can be better protected with high encryption standards, irrespective of where companies store the data (Chander and Lê, 2014). Other concerns include the possibility of large-scale natural disasters wiping out data servers located in specific regions (Leviathan Security Group, 2015). Finally, localized data sets resulting from restrictions on data flows, as opposed to global data sets combining data from across countries, entail new policy risks; for instance, local data sets make it harder for companies to detect patterns in criminal activities such as money laundering, terrorism financing and fraud (Chander and Ferracane, 2019; GSMA, 2019c).

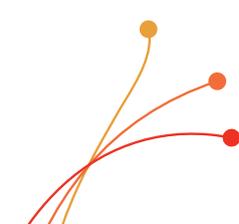
Countries with strong data protection laws are likely to be considered safer destinations for data outflows, especially given the lack of a uniform, international approach to data protection (thus explaining the logic of an adequacy approach). In practice, an adequacy approach can become politicized and usually requires long negotiation periods, as is evident from the recent experience of the adequacy negotiations of the European Union with Japan.⁶¹ Further, most developing countries, including LDCs, are likely to struggle in negotiating an adequacy arrangement with the European Union or most developed countries, as they lack the necessary economic power and capacities to make the required regulatory adjustments (for instance, equivalent to GDPR).

Implementing regulations on cross-border data flows also entails costs which countries should account for in designing domestic regulations – for example, in ensuring compliance with localization requirements in data protection laws, countries need to spend considerable resources to monitor and audit data facilities of these service providers. Few LDCs or other developing countries have sufficient

⁵⁹ Of course, certain domestic laws may specifically define the scope of such regulations.

⁶⁰ In fact, in response to this scenario, in 2019 the Ibero-American Personal Data Network issued a special statement expressing its “concern” for the “increasingly frequent processes of lack of institutional and budgetary support” to the data protection authorities by the respective Governments. *Declaración del XVII EIPD sobre el estado de las Autoridades Iberoamericanas de Protección de Datos*, available at www.redipd.org/sites/default/files/2020-01/declaracion-ripd-estado-autoridades-xvii-encuentro.pdf.

⁶¹ The negotiations between the European Union and Japan started in January 2017, and the adequacy decision was finally reached on 23 January 2019, after a period of two years. See European Commission, “Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions”, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_17_16; European Commission, Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, C/2019/304/, OJ L 76, 19 March 2019.



resources for conducting such intensive regulatory scrutiny. For instance, although Nigeria has imposed several data localization requirements, the Government has struggled to monitor their implementation or impose penalties for violation due to inadequate capacity and resources to monitor data flows.⁶² Further, certain contractual and certification mechanisms for cross-border data transfer – such as BCRs, SCCs and Asia–Pacific Economic Cooperation (APEC) community-based participatory research – are unaffordable for micro-, small and medium-sized enterprises (MSMEs), and require long processing times (Mattoo and Meltzer, 2018; WEF, 2020b), thereby significantly affecting economic opportunities for smaller data-driven businesses in developing countries.

Despite the implementation challenges of data flow regulations, they may be necessary for certain reasons and entail specific regulatory advantages in specific sectors or certain areas of governance. For example, some data localization measures are vital to enable proper regulatory oversight (facilitating immediate and unhindered access to data)⁶³ and law enforcement purposes (such as investigation of domestic criminal offences). A study by the European Commission indicates that more than half of the criminal investigations in the world today require access to cross-border electronic evidence, resulting in a sharp escalation of cross-border data requests by Governments to mainstream digital platforms and data hosting companies.⁶⁴ This issue remains largely unresolved, as processes such as mutual legal assistance treaties and letters rogatory⁶⁵ are slow and largely outdated in the digital world. Few legal initiatives exist to address cross-border data requests, which partly explains the adoption of the CLOUD Act by the United States (chapter IV).

Several regulations on cross-border data flows are aimed at ensuring that any data that move across borders enjoy the same level of data protection, security and confidentiality as those that move domestically. Governments may want to ensure that residents have adequate access to enforce the available domestic remedies if a data breach occurs abroad. This challenge is particularly difficult for LDCs and other developing countries with weak enforcement capacity, even if valid contracts exist between local consumers/companies and foreign companies processing personal data of their citizens abroad. In the absence of any binding international framework,⁶⁶ cross-border enforcement of privacy laws remains one of the most difficult challenges that even the most developed countries face in a digitally interconnected world (Greze, 2019). Therefore, restricting personal data transfers may be seen by Governments as the only practical way to protect the privacy of their citizens in the absence of a more comprehensive shared data protection regime between the countries concerned (Panday, 2017).

National security considerations also increasingly inform regulatory measures adopted by countries on cross-border data flows. Given the strong digital “interdependence” in the world today, countries hosting the biggest technology companies and Internet servers have the ability to “extract informational advantages vis-à-vis adversaries” and even cut off certain “adversaries from network flows” (Farrell and Newman, 2019:46). Owing to the predominance of digital firms from China and the United States, as well as the large number of hyperscale data centres located in these two countries (chapter I), data flows are routed through these regions to a larger extent than to all other countries (Mueller and

⁶² United States Trade Representative, *2020 Investment Climate Statements: Nigeria*, available at <https://www.state.gov/reports/2020-investment-climate-statements/nigeria/>.

⁶³ Interesting examples in this regard are the memorandums of understanding entered into by the financial regulators in Singapore with their counterparts in the United States and Australia to ensure data access. See www.mas.gov.sg/news/media-releases/2000/mas-signs-memorandum-of-understanding-with-the-australian-securities-and-investments-commission--16-may-2000.

⁶⁴ European Commission, Recommendation for a Council Decision authorizing the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, 5 February 2019.

⁶⁵ Letters rogatory are formal requests made by the court of one country to the court of another country for providing assistance in judicial proceedings, such as in relation to evidence.

⁶⁶ For example, the APEC Cross-Border Privacy Enforcement Arrangement, one of the few available frameworks, is a completely voluntary system. See APEC, *Cross-Border Privacy Enforcement Arrangement*, 2015, available at www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement.

Grindal, 2019).⁶⁷ Thus, it is expected that some countries will aim to control their domestic data flows better – including the physical infrastructure, such as data centres, undersea and transatlantic cables, and Internet exchange points – to protect themselves from foreign surveillance, reduce dependence on foreign networks, and enhance their position in global Internet governance (Woods, 2018; Farrell and Newman, 2019; Ciuriak, 2019; Bagchi and Kapilavai, 2018; Hesselman et al., 2020). Additionally, data localization often facilitates intelligence gathering by Governments (Selby, 2017), thereby increasing their control over domestic affairs, which may be considered to be a regulatory advantage in some countries.

In devising regulations on data flows, Governments need to cautiously consider their choice of tools and use strict localization measures sparingly (e.g. limited to highly sensitive sectors, and worded clearly) to avoid adverse economic, social, political and technological consequences, and amplify potential regulatory advantages. For instance, a measure requiring localization of all personal data can be used by Governments to illegally monitor and persecute dissidents or political opponents, in violation of international human rights norms (Freedom House, 2020). In contrast, Governments may be justified in restricting data flows to a country with a known record of cybercrimes and privacy breaches. Further, a cost–benefit analysis of a data flow regulation needs to consider the costs of controlling the network and data infrastructure, especially for smaller developing economies. A key concern is that unreasonably complex regulations on data flows may result in premature load bearing, and divert resources from more meaningful governmental functions. Also, as discussed below, data regulations that interfere with the underlying architecture of the Internet (e.g. data routing protocols), such as forced localization measures, can have severe adverse consequences on global Internet governance, including amplifying data security and other data governance risks. These risks are particularly severe in countries that lack robust domestic data and network infrastructure.

b. The economic perspective: development-related necessities and risks

Regulations on cross-border data flows can be closely tied to economic development objectives, especially in emerging and developing economies. In finding the best ways to tap domestic opportunities from data-driven sectors, Governments need to consider various factors – such as their level of digital readiness, home-grown technological capabilities, digital and regulatory infrastructure, the size of their markets, and the identification of niche markets – where emerging domestic companies are more likely than their foreign counterparts to be successful (UNCTAD, 2017 and 2019a).

Stringent regulations, such as localization measures or hard conditional data transfer requirements, may lead to economic inefficiency. For instance, any country competing in such markets may need to invest significant resources to replicate or store data in local data centres, and restructure their data operations to align with domestic laws (Bennett and Raab, 2020; Internet Society, 2020c). In Latin America, data localization provisions have been found to be one of the key factors constraining the growth of the fintech sector (Aguerre, 2019). In countries without sufficient infrastructure, including high costs of electricity, local data centres are also likely to be less reliable and secure, with limited economic returns to the domestic economy (Chander and Lê, 2015; Leviathan Security Group, 2015), in spite of possible gains from the potential upgrading of other infrastructures (discussed in chapter III). Further, multinational companies are likely to be reluctant to locate their data centres in countries with known histories of illegal surveillance or unsafe cybersecurity practices (Lee, 2018) or with inadequate skills in the domestic market (Badran, 2018; African Union, 2020). Studies have also shown that restrictions on cross-border data flows may reduce productivity and economic profitability in several sectors, including manufacturing industries (Bauer et al., 2016). Even domestic companies may be adversely affected by localization, especially smaller companies that rely on competitively priced data storage facilities and services.

At the same time, local data storage may be an expedient solution in certain scenarios in terms of costs, efficiency and performance; for instance, for applications such as health monitors or

⁶⁷ *Nikkei Asia*, 24 November 2020, China Rises as World's Data Superpower as Internet Fractures, available at https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures?utm_source=CSIS+All&utm_campaign%E2%80%A6.



autonomous vehicles, immediate data access and quick response times are essential factors that can be addressed by keeping data locally (Komaitis, 2017). A similar argument could be made for the use of software-as-a-service solutions in cloud computing, where real-time access made feasible by local storage solutions can enhance the quality of digital services offered to smaller domestic companies (Kathuria et al., 2019). Further, the costs of latency and broad bandwidth required for transmitting massive volumes of data for new generation technologies, such as IoT products over long distances, could be significantly higher than storing data locally. Such local storage solutions could not only be cost-effective, but could also serve other regulatory interests, such as reducing dependence on foreign cloud services and ensuring privacy and security.⁶⁸ Therefore, certain economic incentives exist for facilitating local storage of data in developing countries, especially in Africa and Latin America.

Certain studies have indicated that restrictions on cross-border data flows may breed economic success in very specific contexts. For instance, China has been extremely successful in developing its digital sector, but this is attributable not solely to its strict data localization laws, but to a variety of factors, such as its huge market size, strategic government interventions to increase investments in the digital sector, high regulatory capacity, and availability of technological resources. Similarly, a study in India found that – due to the unusually large size of the market, coupled with the presence of tech start-up firms and adequate number of engineers – data localization is likely to decrease pressure from foreign competitors and improve market opportunities for domestic companies. However, the study also found that such measures entail costs for consumers, such as reducing choices, increasing prices or decreasing quality of digital services (Potluri et al., 2020). Another study conducted in India (Kathuria et al., 2019) found that the data localization requirements would entail high costs, especially for communications and financial services, as domestic options were not as efficient or cost-effective as cloud services provided by Amazon and Google. Some of the costs of migrating to domestic data centres may be passed on to consumers. Nonetheless, the study also indicated the possibility that, with more foreign companies opening up data centres in India, the quality of cloud-based services available for Indian companies could improve in the future.

In devising regulations on data flows, countries should consider the most optimal frameworks for their digital development requirements. In that regard, the digital development models followed by China and India may not be suitable for other developing countries and LDCs with smaller markets, limited digital capabilities and constrained regulatory capacity. For instance, MSMEs in smaller developing economies may have a better opportunity to grow by using international digital platforms and cloud services, rather than by devising local solutions (Chen et al., 2019). In Latin America, several policymakers and entrepreneurs have acknowledged that they are more likely to benefit from the digital economy by integrating their small and medium-sized enterprises (SMEs) into the global supply chain, rather than by building domestic digital unicorn firms through protectionist measures (Aguerre, 2019). Further, especially in smaller markets, highly localized data sets may not be particularly valuable in creating high-quality Big Data or AI products, which by their very nature are driven by the volume, velocity and variety of data.⁶⁹ Therefore, in such small markets, if Governments attempt to create local data champions by restricting data flows, they may ultimately harm consumers by reducing the quality and functionality of digital products and services available locally (Potluri et al., 2020; Aguerre, 2019). Finally, in small markets with strict data localization policies and poor governance and infrastructure, certain foreign companies may decide not to enter the market at all, to avoid regulatory risks and costs (WEF, 2020b).

In contrast, countries adopting strong data protection laws without unreasonable or infeasible restrictions on cross-border data flows may be more attractive to foreign companies (Kuner, 2013). Countries with strong reputation for good regulatory infrastructure, including trustworthy business environments, can benefit from greater data flows and eventually get access to better data in the future (Open Data Institute, 2019b; Chen et al., 2019). Further, compliance with strict data localization policies and complex data

⁶⁸ See “What is edge computing and why it matters”, 13 November 2019, at <https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html>.

⁶⁹ Volume, velocity and variety are the qualities of data that are most often cited in the literature. See, for example, *ZdNet*, 21 March 2018, Volume, velocity, and variety: Understanding the three V's of big data. However, many more qualities have been highlighted in relation to data; see, for instance, Kitchin and McArdle (2016) and Arockia et al. (2017).

regulations that are targeted to limit the power of Big Tech may actually be more affordable for these huge technology companies than for smaller companies with limited resources (Christakis, 2020). This paradox is well-illustrated by the inability of several MSMEs to operate in the European Union due to the complex regulatory compliance requirements under GDPR (Martin et al., 2019). Therefore, countries should aim to avoid data regulations that can adversely affect the growth of smaller businesses or harm consumer interests in their domestic economies.

However, at the same time, developing countries should remain free to adopt appropriate interventions for promoting domestic digital growth, improving their data capabilities and facilitating inclusive digital development. This would ensure equitable access to data for domestic players, as well as a fair distribution of gains in their domestic economies. For instance, Governments may foster the development of home-bred companies that enjoy a competitive advantage in certain data-driven sectors (e.g. the ability to provide customized solutions based on language or cultural preferences), or incentivize investment in domestic data capabilities to facilitate next-generation digital technologies. Similarly, certain countries may choose to impose digital taxes on foreign companies that use the data of their citizens, or they could ensure fair data access and interoperability by implementing relevant competition laws to improve competitive opportunities for domestic players.

c. The technological perspective: implications for global data governance

The governance of cross-border data flows is inextricably linked to global data and Internet governance. Companies that store and process data in globally distributed servers gain from several technological efficiencies, including better protection against data losses and hacking, and ensuring timely access to data, such as by using edge caches, to store content closer to end users.⁷⁰ Further, cross-border data flows also facilitate compliance with basic international human rights norms, such as freedom of expression and access to data (Taylor, 2020). Experts within the Internet community have expressed concerns, especially regarding forced localization measures, as they can reduce resilience and performance of Internet networks (which were not built to align with territorial boundaries), affect the integrity of underlying protocols (e.g. for data routing and transfer) and impede the inherent openness and universal accessibility of the Internet (Internet Society, 2020c; Komaitis, 2017; Drake et al., 2016). Further, as discussed in chapter IV, growing Internet and digital fragmentation resulting from the lack of global consensus on how to govern data flows, technology tensions between leading digital powers such as the United States and China, and conflicting regulatory models on data flows will be particularly harmful to developing countries, and adversely affect their economic welfare and growth in the coming years.

A summary of objectives and risks of different forms of regulations on cross-border data flows from a regulatory, economic development and global data governance perspective is presented in table V.2.

In conclusion, Governments need to carefully assess both the potential benefits and costs arising from cross-border data flow regulations. Countries have varied policy rationales for regulating cross-border data flows, such as protecting citizens' vital interests, including privacy of individuals and ensuring that data flows are secure. Some Governments consider data regulations to be an important tool to stimulate economic development, create competitive opportunities for domestic players, and ensure the equitable distribution of gains within the country. In other cases, Governments consider that certain regulations are necessary due to the absence of adequate international mechanisms on cross-border enforcement of privacy/data protection laws. Finally, depending on the specific political and sociocultural contexts, certain countries may choose to strictly regulate cross-border data flows to ensure national security or maintain greater political control within borders. In the absence of sufficient international consensus on a global regulatory framework on data flows, many countries are compelled to adopt restrictive regulations and policies on data flows to address the market failures of the digital economy, and protect their domestic economic and political interests. In the long run, both underregulation and overregulation of cross-border data flows lead to suboptimal outcomes and, therefore, international dialogues and policymaking on data flows remain highly desirable to find alternative policy options that work for development.

⁷⁰ Lawfare, 22 May 2017, Where Is Your Data, Really? The Technical Case Against Data Localization, available at <https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization>.

Table V.2. Objectives and risks of restrictions on cross-border data flows	
Objectives	Risks
Ensure data protection and privacy	Increase business uncertainty
Reduce data security risks and protect critical government data from foreign intrusions	Increase compliance costs for companies, especially unaffordability for MSMEs
Create one or two local data champions in larger economies (although they may not always be sufficiently competitive)	May be costly to monitor and implement for regulators
Facilitate easier enforcement of claims against foreign companies in domestic laws, e.g. under data protection laws for breach of user privacy	May increase consumer prices and/or reduce choice for consumers in less competitive markets, including for domestic companies
Enable stronger regulatory oversight in sensitive sectors	May facilitate illegal government surveillance and violation of individual privacy rights
Facilitate data access to regulators for law enforcement purposes	Loss of data in natural disasters, where data localization is mandatory
Reduce dependence on foreign networks and services, and address digital sovereignty concerns	Make fraud detection difficult, e.g. for electronic payment services
Reduce latency and bandwidth costs of long-distance transmission of data	May adversely affect the architecture and reduce interoperability of the Internet
	Premature load bearing for LDCs (e.g. when regulations are too complex)
	May create a false sense of trust and security in the domestic ecosystem

Source: UNCTAD.

C. MAPPING NATIONAL REGULATIONS ON CROSS-BORDER DATA FLOWS

Based on the review of domestic regulatory frameworks on cross-border data flows, this section maps the countries analysed in this chapter on a spectrum based on the degree of overall restrictiveness of cross-border data flows (looking at both the scope and depth of relevant regulatory measures in each country). It then offers some high-level perspectives on regulatory trends on cross-border data flows.

1. The regulatory spectrum for cross-border data flows

The regulatory spectrum for cross-border data flows, starting from the lowest level of restrictiveness, consists of the following approaches:

- A *light-touch approach* implies that all data, including personal data, can generally flow freely across borders with minimal regulatory requirements (if any), and thus relates to measures with the least restrictions on cross-border data flows, i.e. free flow of data. The United States stands out as a prominent advocate of this approach. Other economies – such as Mexico, Australia and Singapore – are also more or less aligned with this approach. Countries that adopt a light-touch approach may still impose certain exceptional restrictions on cross-border data flows, e.g. in sensitive sectors such as defence or health.
- A *prescriptive regulatory approach* entails that cross-border data flows are subject to rigorous compliance requirements – for instance, in domestic data protection/privacy laws. Most countries in this category tend to focus on personal data. The prescriptive approach falls in the middle of the regulatory spectrum, and typically comprises conditional transfer requirements. The European Union is the most well known for adopting this approach in the context of transborder personal data transfers. As discussed earlier, several other countries have also started imposing strict requirements for cross-border personal data transfers in their data protection/privacy laws.

- A *restrictive regulatory approach* means a complete or partial ban on cross-border data flows for reasons of public security, national security and establishing absolute political control over the domestic Internet, including the data accessed and produced by the citizens, often dubbed “data sovereignty”.
- Finally, certain countries adopt a *guarded approach*, emphasizing the unequal economic impact of unhindered global digitalization of the economy, thereby focusing on regulatory measures necessary to enable meaningful domestic economic gains from the digital economy, i.e. where the country and its peoples can hold the key to its digital future and development (Jain and Gabor, 2020). Both the restrictive and guarded approaches tend to focus primarily on localization regulations, although their predominant policy rationales are quite different.

The difference between guarded, restrictive and prescriptive approaches is not always clear in practice; for example, with increased regulatory capacity, emerging economies may choose to impose stronger prescriptive requirements, instead of localization measures, for personal data protection. Further, some highly prescriptive compliance requirements for cross-border data flows may effectively amount to a restrictive approach when cross-border data flows are largely impermissible. Similarly, certain countries that adopt a guarded approach to maximize economic gains could also be hoping to achieve political control over domestic data and vice versa. Finally, countries adopting a light-touch approach may impose localization requirements in sensitive sectors.

These approaches typically relate to specific kinds of regulatory measures, i.e. based on their degree of restrictiveness, and thus they can be aligned with the corresponding relevant type of measure(s), as shown in the next section.

2. Mapping regulations on cross-border data flows on the regulatory spectrum

This section highlights how regulatory frameworks on cross-border data flow are being implemented across the world. Table V.3 provides an overview of regulatory frameworks, mapping different economies on the regulatory spectrum based on the assessment of relevant domestic laws, regulations and policies regulating cross-border data flows. With regard to the prescriptive approach in the middle of the spectrum, the table distinguishes between countries that impose soft or intermediate conditional requirements for cross-border data flows (thus making them less prescriptive; see the right side of the spectrum) and those that impose hard conditional requirements (making them more prescriptive; see the left side of the spectrum). Further, as both guarded and restrictive approaches primarily rely on localization measures, they are shown at the extreme left end of the spectrum; however, the specific approach of individual countries is listed in the table for clarity.

While only a few countries have chosen to adopt a light-touch or restrictive/guarded approach, most countries in table V.3 have adopted some form of prescriptive regulatory frameworks on cross-border data flows. Economies with a prescriptive approach are spread across regions, and have different levels of development: Algeria, Argentina, Bahrain, Belarus, Brasil, Colombia, Côte d'Ivoire, Israel, Malaysia, Tunisia and the European Union, to name a few. In these cases, instead of completely restricting cross-border data flows, regulations incorporate compliance requirements for cross-border data transfers (typically for personal data). These compliance requirements can range from highly prescriptive to moderately prescriptive, usually depending on the specific regulatory interests and goals in each country: a strict adequacy approach (coupled with limited derogations); approved contractual or certification mechanisms for cross-border data transfers; case-by-case regulatory assessment of data transfers; consent-based data transfers (whether expressed or implied); and transfers based on legal considerations (e.g. compliance with domestic law or international treaty), or to protect vital public interests. Notably, the majority of prescriptive regulatory frameworks relate to personal data; however, as discussed earlier, such regulations have a potentially broad application, as most data sets contain at least some identifiable personal data. Despite the lack of international consensus on data protection and privacy, several countries are adopting or updating their data protection laws, following some common principles, such as those contained in GDPR.⁷¹

⁷¹ Out of 120 countries outside the European Union, 67 have adopted a GDPR-like law (Srikrishna Committee Report, 2018).

Table V.3. Mapping of regulations on cross-border data flows				
Strict data localization	Partial data localization	Conditional transfer: Hard	Conditional transfer: Intermediate/soft	Free flow of data
Restrictive (R) or guarded (G) approach		Prescriptive approach		Light-touch approach
China (R)		Algeria	Azerbaijan	Australia
India (G)		Argentina	Bahrain	Canada
Indonesia (R/G)		Armenia	Belarus	Mexico
Kazakhstan (R)		Brazil	Ghana	Philippines
Nigeria (R)		Colombia	Japan	Singapore
Pakistan (R/G)		Côte d'Ivoire	Kyrgyzstan	United States
Russian Federation (R)		Egypt	New Zealand	
Rwanda (G)		European Union	Republic of Korea	
Saudi Arabia (R)		Georgia	United Arab Emirates	
Turkey (R)		Israel		
Viet Nam (R)		Kenya		
		Malaysia		
		Morocco		
		Peru		
		South Africa		
		Switzerland		
		Thailand		
		Tunisia		
		Ukraine		
		United Kingdom		

Source: UNCTAD.

Note: The list of regulations reviewed is presented in the online annex to chapter V, available at https://unctad.org/system/files/official-document/der2021_annex2_en.pdf.

Other regulatory trends are also visible in table V.3. First, few countries have adopted a light-touch approach. This approach appears to be favoured mostly by countries with strong regulatory environments and sufficient regulatory resources to monitor compliance of domestic laws, especially by huge foreign companies. Further, economies such as Australia, Singapore and Canada have traditionally been open, liberal economies, and therefore their adoption of a light-touch approach to cross-border data flows is expected. The dependence of the economy of the Philippines on the outsourcing industry may explain its light-touch approach. Finally, being a leading digital power and a strong advocate of a free and open Internet, the United States favours a light-touch approach.

Second, the restrictive approach, adopted by China and the Russian Federation since the turn of the century, is becoming increasingly popular in other developing countries, including Turkey, Viet Nam, Kazakhstan and Pakistan. In these countries, data protection usually relates to data/information security rather than protecting the privacy rights of individuals. The specific political and sociocultural context is usually the main reason behind a restrictive approach. For example, in less democratic countries, there may be a tendency towards stronger sovereign control over activities of their citizens, including content that is available on the Internet, as well as expression of ideas online (Freedom

House, 2020a).⁷² This form of data regulation has raised strong concerns in the international community, especially in relation to human rights.

Finally, some emerging digital economies, most prominently India, appear to be embracing a guarded approach. Although several data regulations can indirectly benefit the domestic sector (e.g. by making overseas data processing more cumbersome), the majority of countries do not impose regulations to restrict data flows with the primary motive of shielding their domestic sector from foreign competition. Data-restrictive policies may be successful in some contexts, but are not a silver bullet solution for all developing economies. For instance, certain developing countries may not have adequate capacity to build high-quality, local digital platforms, and may thus better achieve economic development by adopting regulations that facilitate secure and privacy-compliant cross-border data transfers, such that local companies can access services provided by foreign digital platforms. The design of such regulations would depend on the regulatory culture and resources within the country, the requisite local value creation from the digital economy and other considerations, such as digital connectivity and interdependence with global digital markets.

Finally, countries may shift across these groups; for example, with improved regulatory resources, a country adopting a “guarded” approach may adopt a “prescriptive” approach to minimize economic losses and integrate better with the global digital economy. Countries with minimal or no regulation on cross-border data flows may modernize their laws to adopt more prescriptive, guarded or restrictive approaches, in light of their specific economic and political needs.

D. CONCLUSION

Countries regulate cross-border data flows to address a variety of policy concerns in different domains of governmental regulation, often intending to reach different regulatory outcomes based on a complex interplay of domestic and international factors. In many cases, cross-border data flows are regulated for legitimate reasons in terms of national sovereignty, mostly based on the protection of citizens, national security and the promotion of domestic economic development. However, there are differences among countries, according to the priority given to the various motivations. Regulations on cross-border data flows can be found in different kinds of laws and regulations. The various examples of domestic regulations on cross-border data flows discussed in this chapter include data protection laws; cybersecurity laws, regulations and policies; Internet laws and regulations; regulations pertaining to both hardware and software; government procurement laws; laws related to protecting State secrets; income tax laws; corporate and accounting laws and regulations; policies related to e-commerce and digital development; and data strategies. Thus, as different areas of policymaking are involved, regulating in a silo approach may lead to inconsistent measures in different ministries. This would call for a whole-of-government approach in regard to the governance of cross-border data flows.

In assessing the domestic relevance of different regulatory frameworks, policymakers should holistically consider several factors. At a domestic level, countries need to consider their economic situation, political and sociocultural preferences, domestic regulatory capacities, as well as their state of technological development. From a transnational/global perspective, countries should consider their desired foreign policy, including their international trade relations/commitments and degree of integration with the global digital economy and, more broadly, the distributed architecture of the Internet and the global nature of several Internet policy challenges. Ultimately, the appropriate model for regulating data flows in each country remains a complex policy choice. This holistic balancing exercise is particularly valuable for developing economies to maximize the potential benefits of the digital economy and ensure greater welfare of their citizens.

Taken together, chapters IV and V show that domestic regulatory frameworks on cross-border data flows are extremely diverse, and evolving rapidly with the increased digitalization of the global

⁷² See generally United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/38/35); Human Rights Watch, 23 April 2020, “Vietnam: Facebook, Pressured, Censors Dissent”, available at www.hrw.org/news/2020/04/23/vietnam-facebook-pressured-censors-dissent.

economy. The diversity of approaches, measures and motivations renders the task of finding patterns of regulation among countries difficult. An attempt can be made by looking at the economic motivations and characteristics of countries. Among developed countries, there is a large, developed country – the United States – hosting global digital platforms with strong market power that favours free cross-border data flows, in order for them to be able to get most of the gains from the data collected in their operations worldwide. Smaller developed countries, whose internal markets are not big enough to benefit from restrictions, tend to favour free cross-border data flows. The European Union is a particular case, as it privileges privacy and data protection motivations. Among developing countries, those with large domestic markets mostly favour data localization to promote the development of their digital economies. In the case of China, national security motivations also play a major role. For the rest, smaller developing countries, the picture is mixed. Data localization is not likely to be of use, given the small size of their markets, while free cross-border data flows imply giving away a domestic resource without any return.

The main reasons for this diversity are the absence of an international policy framework in key areas of data regulation (such as privacy and data protection, cybersecurity and online content regulation), as well as concerns related to the equitable distribution of the benefits in the digital economy. In addition, the unique political, cultural and economic preferences within a country, coupled with its state of technological/digital development, strongly impact the design of domestic regulations on cross-border data flows. For instance, a country with strong communitarian values may attribute a different meaning to privacy, as compared with one that places strong emphasis on individual privacy; such different perspectives could lead to a contrasting approach in the regulation of transborder personal data flows. Similarly, certain sectors – such as health, public administration or finance – may be considered more sensitive in certain countries than in others, resulting in tighter regulation of those sectors. Finally, certain countries may be in an optimal position to build their domestic digital sectors through targeted industrial policies, and thus may impose restrictions in sectors where they consider that they have a competitive advantage.

However, while the rising economic importance of data for development has resulted in increased regulation of cross-border data flows, mainly in the form of data localization measures, whose benefits are not so evident, few countries actually have proper strategies to develop their digital economies and process their data domestically. Some exceptions are Digital India and the South African New Draft National Data and Cloud Policy. As discussed in chapter III, having access to the data is a necessary but not sufficient condition for development; it is also necessary to develop domestic capacities to process the data into digital intelligence that can be monetized or used for social value.

Regulations on cross-border data flows should holistically balance a country's unique digital development needs, and regulatory and technological capacity, alongside external considerations.

Given the variety of considerations informing the regulation of cross-border data flows, blindly transplanting regulatory models of data governance from developed to developing countries, and even from one developing country to another, is not likely to produce desirable outcomes. Rather, specific circumstances within each country should play a critical role in determining how the country regulates data flows. Therefore, it makes little sense to argue for neither the adoption of widespread strict localization policies that may be economically and technologically inefficient, nor unrestricted data flows without sufficient privacy and security safeguards and without paying due consideration to economic development concerns and equitable distribution of gains in the digital economy. Further, different countries should be able to choose prescriptive regulatory frameworks (such as in their domestic data protection and cybersecurity laws) based on their specific regulatory capacities and domestic policy requirements.

In an ideal scenario, regulations on cross-border data flows should holistically balance a country's unique digital development needs, and regulatory and technological capacity, alongside external considerations, such as how the country can meaningfully integrate into the global digital economy and incorporate the

relevant norms, standards and policy solutions for addressing global Internet policy problems, including transnational online privacy and cybersecurity concerns. Given the relevance of the policy objectives informing the majority of regulations on cross-border data flows, a one-size-fits-all approach appears both infeasible and undesirable. It remains important for all countries to seek, both individually and collectively, the most effective and equitable – and least disruptive – tools to regulate cross-border data flows. Further, the dynamic nature of the data-driven digital economy necessitates that all countries (whether developed or developing) continuously recalibrate their policy choices on cross-border data flows, so that they can find the optimal balance between promoting domestic economic development, protecting vital public policy interests, and ensuring an integrated global digital ecosystem. In that regard, some form of a high-level international policy framework or instrument on cross-border data flows could be a useful guide to all countries, and facilitate greater alignment between their respective regulatory frameworks, while enhancing trust, interconnectivity and interoperability in the global digital ecosystem. However, as discussed in the next chapter, regional and international regulatory frameworks have not been up to the challenge of enabling cross-border data flows with an equitable sharing of the economic development gains while properly addressing concerns such as privacy, protection of human rights and national security.

Some form of a high-level international policy framework or instrument on cross-border data flows could be a useful guide to all countries, and facilitate greater alignment between their respective regulatory frameworks, while enhancing trust, interconnectivity and interoperability in the global digital ecosystem.

The expansion of cross-border data flows has led to enhanced interest among Governments in complementing their national legislation with commitments at the regional and international levels. To date, however, finding consensus has proven difficult, reflecting different priorities and positions of countries. Even among G20 countries, there are contrasting views on both substance and process.

While regional and international discussions on data flows initially focused on the need to protect privacy, more recently the emphasis has shifted to the trade area. A rising number of bilateral and regional trade agreements now include clauses related to data and digital trade, and negotiations are also underway in the context of the Joint Statement Initiative on e-commerce at the World Trade Organization. The chapter shows that international and regional approaches to regulating cross-border data flows are either too narrow, focusing only on aspects such as trade or privacy, or too limited geographically, as in the case of regional approaches. It emphasizes that, in order to address data flows in a holistic and multidimensional manner, global rules in this area will need to go beyond trade, and consider both economic and non-economic dimensions of data.

REGIONAL AND INTERNATIONAL APPROACHES TO REGULATING CROSS-BORDER DATA FLOWS

VI



CHAPTER VI CROSS-BORDER DATA FLOWS INCREASINGLY GOVERNED AT THE INTERNATIONAL LEVEL BUT NOT HOLISTICALLY



More attention is given to data governance at the international level. However, **diverging views and positions** on their regulation have resulted in an impasse in the international policy debate on cross-border data flows



Cross-border data flows are not trade and need to be governed holistically, factoring in all dimensions

International and regional agreements dealing with data flows

Trade regime

Multilateral

- WTO/Joint Statement Initiative (JSI)

Bilateral

Various bilateral free trade and economic partnership agreements

Other

- Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)
- Regional Comprehensive Economic Partnership (RCEP)
- Trade in Services Agreement (TiSA)
- Pacific Alliance
- United States-Mexico-Canada Agreement (USMCA)

Other agreements and initiatives

- OECD Privacy Guidelines
- OECD Principles for Internet Policy Making
- Council of Europe Convention 108 and 108+
- APEC privacy initiatives
- ASEAN data-related frameworks
- African Union Malabo Convention
- Digital Economy Partnership Agreement
- Ibero-American Data Protection Network (RIPD)
- Digital Agenda for LAC (eLAC)
- G20 Data Free Flow with Trust

Current regional and international regulatory frameworks tend to be either too narrow in scope or too limited geographically, failing to enable cross-border data flows with an equitable sharing of economic development gains while properly addressing risks

NEED FOR A NEW REGULATORY FRAMEWORK

- To be rethought with a view to finding a middle-ground solution
- To factor in both economic and non-economic dimensions



What **international forum** is best equipped to facilitate progress in developing global data governance?

A. INTRODUCTION

As noted in the preceding chapter, the increase in national regulations of data is a reflection of the attempts of Governments to meet various policy objectives. At the same time, such regulations often come into tension with the global nature of the Internet and the digital economy, for which smooth transfers of data across borders are essential. The proliferation of different national approaches to regulating cross-border data flows risks contributing to the fragmentation of the Internet, impacting on its proper functioning (chapter IV), limiting the potential development benefits of data-sharing. To counteract such trends, there have been growing calls to establish adequate mechanisms for the international coordination of data flow regulations (Leblond and Aaronson, 2019; Fay, 2019; Meltzer, 2019; see also chapter VII). There is, however, a lack of agreement on the appropriate forum for such governance, and on what kind of rules and enforcement it should entail. Issues relevant to data flows have been discussed in various bilateral, regional and multilateral forums.

Debates regarding data flows started in the 1970s around privacy concerns. The first intergovernmental outcomes came in 1980 with the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data¹ and in 1981 with Convention 108 of the Council of Europe. Since then, the issue of data flows has been an important topic on the international agenda, notably in the context of Internet governance, such as the United Nations Working Group on Internet Governance, which was set up in 2004, and more recently in the area of international trade.

This chapter examines regional and international developments with regard to the regulation of cross-border data flows, giving special attention to the implications for developing countries. The most recent focus of the international debates and regulations has been in the context of the international trade agenda. However, as explained in previous chapters, considering that cross-border data flows are a different kind of international economic flow, they should not be assimilated into international trade before exploring the relevant regimes. Against this background, section B discusses the rationale for regulating cross-border data flows in trade agreements. Section C then focuses on initiatives for such regulations within the trade regime at different levels. Section D explores selected international and regional initiatives beyond the trade domain. Section E provides the conclusions.

B. IS THERE A RATIONALE FOR REGULATING CROSS-BORDER DATA FLOWS AS INTERNATIONAL TRADE?

Cross-border data flows have become a key component of discussions related to “digital trade”, and have emerged as a key issue in trade negotiations at the multilateral, regional and bilateral levels (Meltzer, 2019; Pohle et al., 2020; Azmeh et al., 2020; Aaronson, 2019b; Ciuriak and Ptashkina, 2018; Kelsey, 2018).

Driven by demands from its digital firms, the United States has been the lead proponent of including cross-border data flows in the trade regime. In 2016, the Trans-Pacific Partnership (TPP) (later renamed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) following the withdrawal of the United States) became the first trade agreement to include binding rules on cross-border data flows. Subsequently, other regional and bilateral agreements have included related clauses (Burri, 2016; Janow and Mavroidis, 2019). In addition, debates around digital trade in the World Trade Organization (WTO) expanded in recent years, with many countries favouring the inclusion of provisions addressing cross-border data flows at the multilateral level (UNCTAD, 2021b; Azmeh et al., 2020).

The rationale for this inclusion rests on the growing role of data flows in facilitating global trade in goods and services, and the impact of national data policies being adopted by different countries. The role of data flows in facilitating trade is undeniable. Indeed, many goods and services are traded either entirely through cross-border data flows, or rely heavily on such flows. This role is likely to increase with the expansion of data-intensive technologies such as autonomous driving, artificial intelligence (AI) and Internet of Things (IoT).

¹ The Guidelines are available at <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>.

Similarly, data policies adopted by countries have important implications for trade. Data localization, for example, has an impact on trade flows in goods and services. Restrictions on data flows might result in a decision by suppliers not to serve a specific market, due to the cost of complying with the measures. Blocking access to certain web applications also has important trade implications, as access to such sites is a prerequisite for accessing goods and services sold on or through such applications. Regulations around privacy and personal data protection also have an important connection to trade. A restriction, for example, by a country on foreign actors collecting or storing data on its citizens could have significant implications for the ability of those actors to sell products to those consumers. However, while cross-border data flows are strongly linked to trade, the rationale for regulating cross-border data flows primarily in trade agreements remains weak at best.

There are two fundamental issues to consider. First, as discussed in chapters I and III, given the different characteristics of data in comparison to goods and services, cross-border data flows are to be considered a new kind of international flow; data flows remain distinct from trade, and treating them as trade can be problematic, for various reasons. While much global data being produced, stored and exchanged are related to commercial transactions, a huge share of these data are not related to such transactions, but to other aspects of human life, and there are challenges facing the distinction between different types of transactions (National Telecommunications and Information Administration (United States), 2016). As such data are produced, collected, stored and transferred, these processes impact issues related to privacy, personal data, social relations and security, among others, and treating these issues just through a “trade lens” implies taking a too-narrow approach. Moreover, this also applies to data products, which can be regulated through the services trade regime, implying that trade regulations in relation to data may need to take place in a broader context. In the words of Rodrik (2020): “The international trade regime we now have, expressed in the rules of the World Trade Organization and other agreements, is not of this world... it is utterly inadequate to face the three main challenges these new technologies pose.” The three challenges refer to geopolitics and national security, concerns about individual privacy, and economics.

• While cross-border data flows are strongly linked to trade, the rationale for regulating cross-border data flows primarily in trade agreements remains weak at best.

In addition, the way data are collected, stored in multiple locations, and used simultaneously by users throughout the world – where ownership and sovereignty become challenging concepts to apply (chapter III) – makes it difficult to regulate cross-border data flows through the State-centric mode of trade. Reflecting these complexities, many emerging definitions of “digital trade” do not include cross-border data flows as part of digital trade. In fact, the Handbook on Measuring Digital Trade, published in 2020, defines digital trade as “all trade that is digitally ordered and/or digitally delivered”, i.e. excluding data flows that are not linked to specific exchanges of a good or a service (OECD, WTO and IMF, 2020).

Second, even ignoring the fact that cross-border data flows are different from trade, there are questions on how suitable the trade regime is as an arena of governing such flows (Leblond and Aaronson, 2019). The history of the trade regime is based on countries negotiating reciprocal concessions in areas such as tariffs and quotas. While other issues have been added to the trade regime in recent decades, it remains largely based on an exchange of benefits between different countries. Issues that are not easy to situate within this framework are hard to deal with in the trade system – such as labour and environmental standards (Suranovic, 2002). As data touch on issues such as personal protection and privacy, addressing them in the trade regime is difficult. Furthermore, the trade regime has historically been less transparent than multi-stakeholder approaches, and it is mainly government-to-government. While such systems were perhaps more relevant when negotiations were concerned with issues such as tariffs and quotas, the inclusion of additional issues is making trade negotiations more challenging.

In recent years, for instance, there has been growing public debate and mobilization on existing or proposed trade agreements focusing on the implications of those agreements on a range of issues, such as the environment, labour, health and agriculture, among others. Such growing public attention to issues governed by the trade regime is making it more difficult to reach agreements without wider public involvement and more transparent processes (Gheyle and De Ville, 2017; Organ, 2017).

Key factors for the inclusion of additional issues into trade negotiations, including cross-border data flows, are that they can offer a forum to accommodate a large number of countries, existing and well-established rules and norms, as well as a relatively high level of enforceability relative to many other forums. Moreover, in addressing the question of why data governance has never been addressed as an issue on its own, Nussipov (2020b) notes that the reasons for linking regulations of cross-border data flows to global trade policy remain a puzzle, arguing that “it was mainly because the U.S. managed to shift data policy debates from domestic regimes to the international trade regime by including them into the negotiations of General Agreement on Tariffs and Trade... The U.S. strategically used forum shopping to rebrand data flows as a trade policy matter”. This rebranding “marked the shift of data policy from telecommunications, data networks and economic development regimes to the regime of international trade. The first three sets of regimes had a technical, inward-looking domestic policy focus. The international trade regime prioritized openness, free trade and economic growth.”

In addition to these broader issues, developing countries in particular face a difficult landscape in the trade arena, where power asymmetries play an important role in shaping outcomes. One of the reasons for the expansion of the trade regime has been the push by more advanced economies to link new issues to the trade regime, in order to leverage their larger market size to obtain desirable outcomes in areas such as intellectual property and investment regimes (Sell, 2009). With regard to data, linking them to issues such as market access might present developing economies with the tough choice of trading away their right (or policy space) to regulate data flows in order to maintain their existing access to the advanced economies’ markets, or to secure enhanced access in some economic sectors (Steinberg, 2002). Developing countries have also been found to be in a weaker position when it comes to dispute settlement in international trade agreements (Mosoti, 2006; Abbott, 2009).

Developing countries in particular face a difficult landscape in the trade arena, where power asymmetries play an important role in shaping outcomes.

The push for expanding the trade regime has been challenged by some countries and non-governmental organizations. Critics have highlighted the lack of capacities by trade negotiators, especially from smaller developing countries, to discuss an ever-expanding agenda of complex and highly technical issues. Due to the ability of those economies to offer better advantages to countries that enter into bilateral and regional agreements, more powerful countries can use such agreements to promote rules that they might struggle to promote multilaterally. As a result, the power of developed economies tends to increase in bilateral and regional forums, as individual developing countries are more likely to accept certain rules that developing countries as a group may be reluctant to accept. This ability is intensified by what some scholars have called fear of exclusion, in which developing countries worry that other developing countries will capture higher shares of trade and investments at their expense, as a result of bilateral trade agreements signed (Shadlen, 2008). Those factors place developed economies in a stronger position in international trade negotiations, as they are capable of using their market size to promote certain rules, and to alternate between the multilateral framework and various regional/bilateral frameworks to weaken resistance to certain rules. This dynamic places developing countries between a “rock and a hard place”, as resisting certain issues multilaterally could drive more regional and bilateral agreements that could further weaken the position of developing countries as a whole.

Overall, there are concerns that regulating the issue of cross-border data flows through trade agreements makes it difficult to take into account the multidimensional nature of data, and to ensure full participation of all stakeholders potentially affected. In view of the relatively weak market power of most developing countries, there is also the risk that any outcome of the negotiations will mainly reflect the interests of companies in more advanced economies, which are currently the best positioned to capture value from the expansion of data flows. While this could reduce the uncertainty with regard to cross-border data flows, it would also reaffirm and reinforce existing imbalances in the data-driven digital economy.

There are concerns that regulating cross-border data flows through trade agreements makes it difficult to take into account the multidimensional nature of data, and to ensure full participation of all stakeholders potentially affected.

For example, Argentina, Colombia and Costa Rica² have indicated their preference for limiting the purview of the discussions on trade negotiations at the WTO to trade-related aspects; that they wish to reconfirm members' rights to regulate, with a view to ensuring the protection of the privacy of individuals, and the security and confidentiality of information; and that participants should be guided by relevant international standards where they exist.

Brazil considered that some of the core topics that would require rule-making were “the degree to and the conditions under which digital data shall be allowed to flow”,³ suggesting that “regulators will find themselves in situations where limitation of dataflow is unavoidable... The general and the security exceptions of GATS Articles XIV and XVI bis are useful provisions... but were not specifically drafted for the digital environment. Therefore, it might be useful to consider how improved disciplines would clarify the general and security exceptions appropriate for the digital environment.” Among the other issues Brasil highlighted as requiring attention are the question of whether the usage of Big Data will require a jurisdictional debate, the ownership of data produced in different jurisdictions, and data portability and non-discriminatory access. Brazil later supported the “typical” provision on cross-border transfer of information: right to own regulatory requirements, shall allow cross-border transfers when activity is for conduct of business and exception for legitimate policy objectives provided not arbitrary discrimination or disguised barrier.⁴

China has stated that issues such as cybersecurity, data safety and privacy are increasingly highlighted, bringing unprecedented security risks and regulatory challenges to members.⁵ The country notes that members differ in national conditions and development stages, having different challenges and concerns, and that “Bearing in mind the aforementioned differences, Members should respect each other's design of the electronic commerce development paths, and the legitimate right to adopt regulatory measures

² See Communication from Argentina, Colombia and Costa Rica on “WTO negotiations on trade-related aspects of e-commerce. Elements of a potential approach under the framework of the Joint Statement on Electronic Commerce” (JOB/GC/174), WTO, 5 April 2018, available at https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=244342&CurrentCatalogueIdIndex=0&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=False&HasSpanishRecord=False.

³ See “Exploratory work on electronic commerce. Non-paper from Brazil” (JOB/GC/176), WTO, 11 April 2018, available at https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=244463&CurrentCatalogueIdIndex=0&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=False.

⁴ See “Communication from Brazil. Joint Statement on electronic commerce” (INF/ECOM/27), WTO, 30 April 2019, available at <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/27.pdf&Open=True>.

⁵ See “Communication from China. Joint statement on electronic commerce” (INF/ECOM/19), WTO, 24 April 2019, available at <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf&Open=True>.

in order to achieve reasonable public policy objectives.” Côte d’Ivoire suggests the establishment of a forum for inter-institutional cooperation to help promote, inter alia, national frameworks for data use.⁶

However, as discussed in previous chapters, given the multidimensional character of data, the implications of cross-border data flows go much beyond international trade issues, with complex and interconnected impacts for society in many economic and other areas. Moreover, as discussed in chapter III, there is an absence of proper multilateral markets for (raw) data, in which data can be exchanged between data providers (often the users), and those demanding the data in exchange for money (since raw data are mostly extracted for free). Thus, there are not data exports or data imports. There is no registry for data flows crossing borders, as in the case of international trade. When looking at the data-driven digital economy, in the international relations among countries, there are data outflows and data inflows, which are a different kind of international flow from trade, and they involve much more than trade. Finally, one of the trade regime’s mains of shortcomings in this context is the failure to distinguish between flows of raw data, which are certainly not trade, and flows of data products, which may be considered as services trade, but whose rules may need to be adapted to the new digital economy context (see chapter I), as the processing of data has become increasingly entangled with other aspects of society, such as privacy and other human rights, as well as security issues. Thus, cross-border data flows need to be addressed from a broader, integrated and more balanced regulatory perspective.

C. REGULATION OF CROSS-BORDER DATA FLOWS IN TRADE AGREEMENTS

This section explores different trade regimes that regulate cross-border data flows at multilateral, regional and bilateral levels.

1. Treatment of data flows in multilateral trade agreements

With the evolving data-driven digital economy, an important area of discussion in recent years in the international economic debate has been the applicability of existing WTO rules and other trade agreements to cross-border data flows. This issue has been raised as the key agreements in the multilateral trade regime were adopted prior to the expansion of the digital economy and the rapid increase in cross-border data flows. As a result, attempts to subsume the treatment of cross-border data flows with existing agreements and principles of the multilateral trade regime have been challenging.

A cornerstone of the multilateral trade regime is the distinction between goods and services. Within the WTO system, goods are governed by the General Agreement on Tariffs and Trade (GATT), while services are governed by the General Agreement on Trade in Services (GATS).

Importantly, both GATT and GATS include “general exception” clauses that are relevant to cross-border data flows. Article XX in GATT allows member States to take measures that are “necessary to protect public morals”, while article XXI of GATT allows members to take “any action which it considers necessary for the protection of its essential security interests”. Similarly, article XIV of GATS allows members to take measures that are “necessary to protect public morals or to maintain public order”, and measures needed for the “the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts”. The main condition in these provisions is that such measures are not applied “in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services”.

However, the conditions that must be fulfilled for countries to use the exceptions can be quite difficult to meet. The “necessity test” included in both GATT Article XX and GATS Article XIV is not easy to meet. If a dispute settlements panel finds that another measure was available, even if it was more costly and burdensome to the country imposing the measure, then this other measure would have been preferred.

⁶ See “Communication from Côte d’Ivoire. Joint statement on electronic commerce” (INF/ECOM/46), WTO, 14 November 2019, available at <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/46.pdf&Open=True>.

Meltzer (2019) explains how this could be applied to a data localization measure. The exception clause and associated necessity test have been summarized by Geist (2018): “The general exception must therefore meet four requirements: i. it must achieve a legitimate public policy objective; ii. it cannot be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination; iii. it can not be a disguised restriction on trade; and iv. it must not impose restrictions greater than required to achieve the objective (i.e., a minimal impairment requirement on the use or location of computing facilities).” This author also notes that “the historical record suggests that reliance on this exception is rarely accepted... as the GATT and GATS exceptions have only ever been successfully employed to actually defend a challenged measure in one of 40 attempts”, concluding that “the benefits of the general exception may be illusory since the requirements are so complex (each aspect must be met) that countries have rarely managed to meet the necessary conditions”.

Moreover, usually, the fact that the exceptions are loosely defined ultimately leaves it to these agreements’ dispute settlement mechanisms to determine what is a “legitimate public policy objective” as a justification for restricting cross-border data flows. The same applies for the “necessity” provision: e.g. it “does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective”. This would leave something as important as data regulations to be decided by panels of three experts, should member States bring about disputes.

The implications of these measures for cross-border data flows are not yet fully clear (UNCTAD, 2017). In principle, a large number of measures that countries are taking to restrict cross-border data flows can be justified through security or public moral reasons (Mitchell and Hepburn, 2017). Data localization measures, for example, that require domestic storage of data are often adopted on security grounds, whether for national security or to limit foreign surveillance. The public interest in the issue of cross-border data flows has, for example, increased following the publications of the revelations of former analyst of the National Security Agency of the United States Edward Snowden, alleging that the agency and other surveillance agencies were engaged in massive global online surveillance. This undermined the privacy of many individuals in the United States and abroad, leading some countries to adopt strategies to restrict the flow of data (Aaronson, 2015).

Discussions on these issues at the WTO began relatively early, and they have been on the agenda of the Work Programme on Electronic Commerce, adopted in 1998. Since then, there has been little substantive progress through this work programme. However, some WTO members have submitted proposals with a view to expand the work in this area. In 2011, the United States and the European Union submitted a joint communication that included a set of “trade-related principles designed to support the expansion of information and communication technology (ICT) networks and services, and enhance the development of electronic commerce”.⁷ The principles included “cross-border information flows” and that “Governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries”.

This was developed further in subsequent years. In 2014, for example, the United States submitted a communication to the Work Programme, arguing that data localization requirements restrict cross-border data flows, and that “Countries that adopt measures that require consumer’s personal data to be processed and stored within their borders may be well-intentioned, but these measures have the potential to impede economic activity and do not necessarily provide the data security that they ostensibly seek to achieve”. Such data security, the submission argued, “may be enhanced through external storage, where economies of scale in specialized security practiced by best-in-class data processors may surpass what is available in storage facilities within one particular jurisdiction”. On privacy and protection of data, the United States acknowledged that “all Members share an interest in the protection of privacy and the security of data”, but that such measures are subject to appropriate discipline. “In the view of the United States, there is little evidence to support the need for restricting

⁷ See Communication from the European Union and the United States, “Contribution to the Work Programme on Electronic Commerce” (S/C/W/338), WTO, 13 July 2011, available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/S/C/W338.pdf&Open=True>.

data from being exported to a particular country's territory solely because the destination country does not share a formal privacy or data security regime with the source country". Members, as such "must take great care that any measures that prevent data exports or that mandate local storage must not constitute an unjustified barrier to trade, unduly discriminating against the foreign supply of any information-intensive service, including but not limited to data processing".⁸

The United States consolidated these proposals in a non-paper submission by in 2016⁹ that outlined examples of "positive contributions to a flourishing digital economy". These examples included "enabling cross-border data flows" that allow companies and consumers "to move data as they see fit", calling for trade rules to combat discriminatory barriers to free flow of data by protecting the movement of data, subject to reasonable safeguards such as the protection of consumer data when exported. Another major example was preventing data localization barriers that "add unnecessary costs and burdens on providers and consumers alike" and call for trade rules to help "to promote access to networks and efficient data processing".

These proposals were supported by some other members. In 2016, the so-called MIKTA group of countries in the WTO (Mexico, Indonesia, Republic of Korea, Turkey and Australia) held a workshop on e-commerce at the WTO, and issued a statement arguing that the WTO should focus more attention on the digital trade agenda. This effort, according to the group, should also include "newer E-Commerce issues that have only come onto the trade policy radar in recent years, such as data flows and data localisation" (MIKTA, 2016). Discussions on e-commerce in the WTO intensified in the build-up to the eleventh WTO Ministerial Conference in Buenos Aires in 2017.

Proposals for incorporating free cross-border data flows in the WTO regime were, however, opposed by some developing country members – such as India, Indonesia and South Africa – and by the African Group. These members expressed concerns that binding rules on cross-border data flows would limit the policy space for those countries to adopt data and digital policies that could help their economies achieve industrialization and technological development. The African Group, for example, argued that "it is perplexing that some members are advocating for new multilateral rules on e-commerce" and that "the multilateral rules as they are, are constraining our domestic policy space and ability to industrialize".¹⁰ The communication by the African Group underlined its strong opposition to new multilateral rules on data issues, particularly the free flow of data and a ban on data localization requirements. In addition to issues around policy space and digital industrial policy, some countries also expressed fears that a commitment to the free flow of data would provide free market access to digitally delivered goods and services, which would deprive developing economies of substantial tariff revenues as more goods are traded online, and threaten their domestic services industry as more services are traded online.

The proposals for rules requiring free cross-border data flows also lacked support from some advanced economies. While the European Union as a whole was generally supportive of this direction, some influential European countries, Germany and France in particular, expressed concerns about a commitment to the free flow of data (Azmeah et al., 2020). Such a lack of support reflected both economic and technological concerns by those countries on the impact of such clauses on the European economy in the context of the dominance of large digital firms from the United States, and also concerns about the implications of such rules on privacy and data protection in Europe, expressed by the adoption of the General Data Protection Regulation (GDPR).

Faced with difficulties in reaching consensus among the WTO membership on expanding discussions in this area, proponents of e-commerce rules (potentially covering cross-border data flows) began to move toward plurilateral negotiations on the issue. On the occasion of the Buenos Aires Ministerial

⁸ See Communication by the United States, "Work Programme on Electronic Commerce" (S/C/W/359), WTO, 17 December 2014, available at <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W/359.pdf&Open=True>.

⁹ See Non-paper from the United States, "Work Programme on Electronic Commerce" (JOB/GC/94), WTO, 4 July 2016.

¹⁰ See Statement by the African Group, "The Work Programme on Electronic Commerce", WT/MIN(17)/21, WTO, 6 December 2017, available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/21.pdf&Open=True>.

Conference in 2017, 71 countries issued the Joint Statement on E-Commerce, reaffirming the importance of e-commerce and the goal of advancing electronic commerce work in the WTO. Led by Australia, Japan and Singapore, the group announced that they would begin exploratory work toward WTO negotiations on trade-related aspects of electronic commerce. Throughout 2019, the group held negotiations through different focus groups with the objective of reaching an outcome of the negotiations by the time of the Twelfth Ministerial Conference, which was to be held in Kazakhstan in 2020, but had to be postponed due to COVID-19, and is now expected to be held in Geneva at the end of 2021.

Cross-border data flows are one of the important issues in these negotiations (Ismail, 2020). A communication from Singapore, for example, suggested two main clauses with regard to cross-border data flows. The first is that “members shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business”, with the qualification that “nothing in this Article shall prevent a member from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade”. Second, with regard to location of computing facilities (data localization), the clause states that “members shall not require the use or location of computing facilities in its territory as a condition for conducting business in that territory”, with a qualification similar to that of the previous clause.¹¹

Participation from LDCs and by members from the African, Caribbean and Pacific regions in the Joint Statement Initiative (JSI) process has been limited (table VI.1). This may reflect not only concerns related to the specific issues covered by the negotiations, but also broader concerns with the plurilateral nature of the process and the rationale for prioritizing e-commerce over other negotiating topics. Some issues highlighted as a reason for this limited participation include:¹²

- Fears of the impact of a plurilateral approach toward weakening multilateralism: As argued in the communication “This approach allows Members to ignore the development interests of low-income countries whose involvement within these agreements is not of the slightest interest to the major trading powers. Our countries therefore run the risk of being left to take or leave whatever others decide.”
- Fears that an isolated agreement on e-commerce without progress on other issues that are important for developing countries, such as agriculture, will undermine an inclusive multilateral system.
- Limited benefits experienced by low-income countries from trade digitalization on their economic development.
- Limited negotiation capacities of developing countries that have small delegations in Geneva, and cannot afford to send experts in all areas of negotiations and to draw on technical support the way more advanced economies can; it is normal, thus, to focus those limited resources on issues of more importance to those economies, rather than tackling issues related to e-commerce.

Proponents for the inclusion of measures aimed at preserving free cross-border data flows in the WTO have used various approaches to achieve this, including by stating that these flows are already covered by existing agreements and commitments (such as GATS Mode 1), even though the drafters of these agreements could not have foreseen the types of flows that are being witnessed today. In view of the resistance of many WTO members to this line of argument, these proponents moved to propose negotiations (initially multilateral negotiations and subsequently the Joint Statement Initiative) for new trade rules that would address these data flows. Irrespective of the forum in which these attempts are taking place, discussions continue in a context of insufficient knowledge about the issues at stake, including those beyond the trade domain. Views on this matter diverge widely, and have a strong political component. At

¹¹ See Communication from Singapore, “Joint Statement on Electronic Commerce” (INF/ECOM/25), 30 April 2019, available at https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=253794.

¹² See Communication from Côte d’Ivoire, “Joint Statement on Electronic Commerce”, (INF/ECOM/49), WTO, 16 December 2019, available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/49.pdf&Open=True>.

Table VI.1. Participants in the Joint Statement Initiative 2019 (as of November 2020)

Developed countries	Transition economies	Latin America	Asia	Africa
Australia	Albania	Argentina	Bahrain	Benin*
Canada	Georgia	Brazil	Brunei Darussalam	Burkina Faso*
European Union 27 member countries	Kazakhstan	Chile	China	Cameroon
Iceland	Montenegro	Colombia	Indonesia	Côte d'Ivoire
Israel	Republic of Moldova	Costa Rica	Kuwait	Kenya
Japan	Russian Federation	Ecuador	Lao People's Democratic Republic*	Nigeria
Liechtenstein	North Macedonia	El Salvador	Malaysia	
New Zealand	Ukraine	Guatemala	Mongolia	
Norway		Honduras	Myanmar*	
Switzerland		Mexico	Philippines	
United Kingdom		Nicaragua	Qatar	
United States		Panama	Republic of Korea	
		Paraguay	Saudi Arabia	
		Peru	Singapore	
		Uruguay	Thailand	
			Turkey	
			United Arab Emirates	
			Hong Kong, China	
			Taiwan Province of China	

Source: UNCTAD (2021b).

Note: Countries with * are LDCs.

the same time, the complexity of the issues, the lack of common definitions and measurement difficulties provide an insufficiently solid ground for the discussions. As a result, policymakers risk taking decisions that are not adequately informed by statistics or backed by proper analyses.

The outcome of the negotiations can have important implications for the future development of e-commerce and for the evolution of the multilateral trading system. Strong heterogeneity in digital capacities and regulatory preferences among the participating WTO members makes finding common ground on issues such as cross-border data flows a daunting challenge. Non-participation of a significant number of developing countries also raises systemic questions on what kind of format a future agreement could take within the WTO architecture, and what effect it could have on non-participating countries (UNCTAD, 2021b).

It is difficult to predict the outcome of these processes at the WTO. An important factor in determining this outcome, however, will be the degree to which similar clauses are inserted in regional and bilateral agreements. As discussed earlier, benefits to individual developing countries from accepting such clauses in regional and bilateral trade agreements with the advanced economies could be higher, which could weaken the opposition to such rules at the multilateral level.

2. Treatment of data flows in preferential trade agreements

Regional, bilateral and transnational trade agreements have become increasingly important instruments for addressing issues related to cross-border data flows (Monteiro and Teh, 2017). This trend is particularly visible in such agreements signed by developed economies, while low-income countries are

rarely signatories to agreements that address data flows. The content of preferential trade agreements may signal in what direction the multilateral agenda on data flows may move, considering the role of some major powers in shaping the international economic relations agenda. In what follows, data clauses in trade agreements by some major economies are discussed. Special attention is paid to those by the United States and the European Union, as they are highly active in the negotiation and signing of regional and bilateral agreements that include cross-border data flows.

a. United States trade agreements

As the leader in the digital economy and home to the most powerful global leading digital firms, the United States has been pushing for binding trade rules on data flows. Over recent decades, the global expansion of leading digital firms from this country took place in the absence of a clear regulatory framework governing their operations across the world. While they were subject to United States national laws, those firms lacked a clear regulatory framework in many regions in which they were operating and expanding rapidly. This exposed them to a high level of uncertainty as a result of potential regulatory changes by Governments around the world. While a company such as Google, for example, might invest huge amounts in data storage and cable infrastructure, regulatory changes by Governments could have major implications for the economic feasibility of such investments.

Therefore, these companies were early proponents of incorporating cross-border data flows in United States trade agreements (Azmeah et al., 2020). Examples of such efforts include a 2010 paper by Google that argued that “governments should not treat Internet policy and international trade as stand-alone silos, and recognize that many Internet censorship-related actions are unfair trade barriers” (Google, 2010:16). In 2012, the Business Software Alliance (BSA), an industry lobby group, published a report that framed some of the issues facing the digital sectors as “digital protectionism”, and argued that such issues should become part of the regional, bilateral and multilateral trade agenda (BSA, 2012). These demands were adopted by the United States Trade Representative through the “digital trade agenda”. Among other measures, free flow of data and a ban on data localisation were key clauses in this agenda (Azmeah et al., 2020).

The first success in this agenda was inserting such clauses in a digital trade chapter in the Trans-Pacific Partnership (TPP) agreement; it was signed in 2016 by the United States with several countries in Asia and the Pacific (Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Viet Nam), which account for 40 per cent of global gross domestic product. This was a significant step in the direction of expanding such rules. The subsequent withdrawal of the United States from the agreement undermined this effort to a degree, although the clauses on data flows and the digital economy remained largely unchanged in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). In addition to TPP/CPTPP, the revised United States–Mexico–Canada Agreement (USMCA) included a binding commitment to the free flow of data and a ban on data localization.

In TPP/CPTPP, article 14.11 commits parties to allowing “the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person”. However, parties are allowed to adopt measures inconsistent with free cross-border flows “to achieve a legitimate public policy objective”, provided that the measure is “not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade”, and “does not impose restrictions on transfers of information greater than are required to achieve the objective”. Similarly, in article 14.13, parties commit not to “require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory”, with a qualification for measures inconsistent with this clause to “achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective”. USMCA follows similar language on cross-border data flows (article 19.11), but eliminates the exception clause for the location of computing facilities (article 19.12).

The United States pursued similar discussions with the European Union in the framework of a proposed Trans-Atlantic Trade and Investment Partnership. Such clauses can be expected in any future trade

agreements the United States negotiates. Recent announcements for a United States–Kenya free trade agreement included digital economy as one of the issues of negotiations (Foster, 2020). The negotiation objectives published by the United States include the establishment of “state-of-the-art rules to ensure that Kenya does not impose measures that restrict cross-border data flows and does not require the use or installation of local computing facilities” (United States Trade Representative, 2020).

The inclusion of data issues in a future United States–Kenya bilateral agreement is significant, as it will be the first time an African country signs an agreement that includes a commitment to the free flow of cross-border data. The United States sees this agreement “as a model for U.S. FTAs with other African countries”. Reflecting what was discussed earlier on the cost–benefit trade-off between multilateral and regional/bilateral agreements, such an agreement might be attractive to Kenya. The benefits of signing a bilateral agreement with the United States could be substantially higher than entering such an agreement through a multilateral or even a regional approach. This is particularly the case as Kenya is a leading digital economy in Africa.

Notwithstanding the potentially significant benefits, a key issue would be which party would be capturing the gains associated with cross-border data flows. Given the different degrees of digital development in the United States and Kenya, data flows between the two economies are most likely to enable global digital platforms in the United States to access Kenyan data and harness them, while Kenyan companies may have more limited abilities to collect and monetize data generated in the United States. Moreover, in view of the evolving African Continental Free Trade Area, and its goal of strengthening regional e-commerce and digital trade, the relatively high degree of digitalization in Kenya may be leveraged by those platforms as a hub for accessing data from the rest of Africa as well.

b. European Union trade agreements

Contrary to the case of the United States, where a clear position to promote the free flow of data exists, the issue of data flows, and particularly their inclusion in trade agreements, has been more controversial in the case of the European Union (Yakovleva and Irion, 2020). Strong voices against the inclusion of a binding commitment to free data flows in trade agreements have reflected several factors. First, a strong campaign against a commitment to free flows of data on the grounds of privacy and protection of personal data took place in the European Union with some non-governmental organizations mobilizing against this issue, and influential member countries adopting a cautious position toward it.¹³ This effort contributed to the adoption of GDPR, which had important implications for any commitment to the free flow of data in international trade agreements. As discussed in chapter IV, GDPR bans the transfer of European personal data outside the European Union, except under certain conditions. The most general of these conditions is the adoption of an “adequacy” decision by the European Commission, which deems a certain jurisdiction safe for transferring personal data to it. In the absence of such an adequacy decision, there are certain mechanisms that businesses or individuals can follow to transfer personal data. Considering the limited number of countries that have received such an adequacy decision, GDPR has important implications for cross-border data flows and for digital trade in goods and services.

Second, economic concerns were raised by some member States, who highlighted that such commitments are likely to benefit the United States digital firms that dominate the European data economy and hinder the efforts of the European Union to catch up in the digital economy (Azmeah et al., 2020). The French Digital Council, an independent advisory commission on digital issues established by the President of France, published a report recommending how to deal with digital issues in the context of the Trans-Atlantic Trade and Investment Partnership negotiations with the United States, and recommended that Europe should play for time in the negotiations, step up construction of Europe’s digital strategy and strengthen the European Union’s bargaining capacity (CNNum, 2014).

Those debates were reflected in a different approach to the inclusion of issues around data and the digital economy in European bilateral and regional trade agreements. The initial position of the European Union – as reflected in the European Union–Japan Economic Partnership Agreement, and in the negotiations for a free trade agreement (FTA) between Mexico and the European Union – was to insert a placeholder

¹³ See, for example, EDRI (2015); Open Rights Group (2014).

clause on cross-border data flows, to enable the parties to revisit this issue in three years. Parallel to this, in 2018, internal debates within the European Union on the best way to facilitate trade through cross-border data flows without compromising privacy and data protection, resulted in the adoption of the “horizontal provisions for cross-border data flows and for personal data protection” (Yakovleva and Irion, 2020). These provisions are designed to be inserted in future trade agreements of the European Union, and aim to allow the free flow of cross-border data, while maintaining strong protections for privacy.

They consist of three articles. Article A on cross-border data flows commits the parties to “ensuring cross-border data flows to facilitate trade in the digital economy”, and outlines four mechanisms the parties commit not to use: (a) requiring the use of computing facilities or network elements in the party’s territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a party; (b) requiring the localization of data in the party’s territory for storage or processing; (c) prohibiting storage or processing in the territory of the other party; (d) making the cross-border transfer of data contingent upon the use of computing facilities or network elements in the parties’ territory, or upon localization requirements in the parties’ territory. Article A also includes a mechanism to review the implementation of this provision three years after the entry into force of the agreement.

Article B commits parties to recognize that the protection of personal data and privacy is a fundamental right, and that “high standards in this regard contribute to trust in the digital economy and to the development of trade”. Personal data are defined in the agreement to mean “any information relating to an identified or identifiable natural person”. The article allows each party to adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, “including through the adoption and application of rules for the cross-border transfer of personal data”, and stresses that “nothing in this agreement shall affect the protection of personal data and privacy afforded by the parties’ respective safeguards”.

The final article of the provisions commits the parties to “maintain a dialogue on regulatory issues raised by digital trade”, including the recognition and facilitation of interoperable cross-border electronic trust and authentication services, the treatment of direct marketing communications, the protection of consumers in the ambit of electronic commerce, and any other issue relevant for the development of digital trade. The focus of such cooperation will be on exchanging information on the parties’ respective legislation on these issues, as well as on the implementation of such legislation. Importantly, this article explicitly excludes provisions related to the protection of personal data and privacy, including on cross-border data transfers of personal data from such dialogue.

Such exclusion reflects the overall view of the European Union that trade negotiations and data adequacy decisions under the GDPR regime are separate and should not be seen as part of the same process. The GDPR adequacy decision is adopted through a proposal by the European Commission, followed by an opinion of the European Data Protection Board, an approval from representatives of European Union countries, and a final adoption by the Commission. Commenting on the decision to grant adequacy to Japan, the European Commission stressed that “For the EU, privacy is not a commodity to be traded. Dialogues on data protection and trade negotiations with third countries have to follow separate tracks” (European Commission, 2019). Through this mechanism, the European Union aims to move toward free flow of data with its trading partners, while maintaining its relatively strong measures in the area of privacy and personal data protection.

c. Other trade agreements

In addition to the trade agreements being signed and negotiated by the United States and the European Union, other trade agreements are starting to include chapters relevant to cross-border data flows.

In November 2020, 15 countries in the Asia–Pacific region – consisting of the 10 Association of Southeast Asian Nations (ASEAN) countries (Brunei Darussalam, Cambodia, Indonesia, the Lao People’s Democratic Republic, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Viet Nam) and 5 partners (Australia, China, Japan, New Zealand and the Republic of Korea) – signed the Regional Comprehensive Economic Partnership (RCEP). RCEP is significant in this regard, as it brings together developing and least developed

countries with much more economically advanced economies (including the three co-convenors of the JSI negotiations), which are also strong proponents of the inclusion of digital trade in trade agreements. Moreover, it is the first trade agreement in which China has agreed to measures on cross-border data flows. Section D of chapter 12 of RCEP addresses the issue of cross-border data flows.

Article 12.14 addresses the issue of location of computing facilities, while article 12.15 addresses the issue of cross-border data flows. Overall, these clauses follow the framework of the TPP/CPTPP agreement, but with changes that provide member States enough power to adopt measures that restrict cross-border data flows (Leblond, 2020). Article 12.15 commits parties not to prevent cross-border transfer of information by electronic means, where such activity is for the conduct of the business of a covered person. This has the qualification that such commitment does not prevent a party from adopting or maintaining inconsistent measures it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade. In a departure from the TPP/CPTPP frameworks, however, it adds that nothing in the article prevents a party from adopting “any measure that it considers necessary for the protection of its essential security interests” and that “such measures shall not be disputed by other parties”. Article 12.14 commits that no “party shall require a covered person to use or locate computing facilities in that party’s territory as a condition for conducting business in that party’s territory”. The article, however, includes qualifications similar to article 12.15, especially giving the right to members to adopt measures that are inconsistent with this commitment if they consider these measures “necessary for the protection of its essential security interests”, and that “such measures shall not be disputed by other parties”.

In sum, RCEP differs from CPTPP in several key aspects. Firstly, while it echoes the CPTPP commitment to data mobility, it preserves each country’s right to determine what it considers necessary to achieve a legitimate public policy objective. While another party may allege that a measure is arbitrary, unjustifiably discriminatory, or a disguised restriction on trade, it cannot claim that it does not pursue a legitimate public policy objective or that it is not necessary. Secondly, measures considered necessary to protect essential security interests are protected from other parties’ scrutiny altogether. Finally, RCEP does not currently provide for the use of State–State dispute settlement for data governance commitments (although it does contemplate that this could get revisited upon review of the agreement), but rather encourages good faith consultations between the parties (Streinz, 2021).

The Trade in Services Agreement negotiations are another forum in which issues relevant to cross-border data flows have been discussed – among 23 countries, including the United States and the European Union. The Agreement included the same proposals around data flows that were included in TPP, including a commitment to the free flow of data and a ban on data localization. Negotiations for the Trade in Services Agreement have, however, stalled in recent years, partly due to disagreements between the United States and the European Union on cross-border data flows (Malcolm, 2016).

In addition to those agreements, some other trade agreements include clauses related to cross-border data flows, although very few of those agreements include binding commitments to the free flow of data. One of those exceptions is the Mexico–Panama FTA, which includes a binding commitment on the cross-border flow of data. Other agreements include regulatory cooperation on cross-border data flows, although without binding commitments. Examples include the Costa Rica–Colombia FTA, the Chile–Colombia FTA, the Panama–Singapore FTA and the Peru–Republic of Korea FTA (Wu, 2017). Another example is the FTA of Canada with Colombia, Honduras, Peru and the Republic of Korea, which commits parties to work together to “maintain cross-border flows of information as an essential element in fostering a vibrant environment for electronic commerce”.

At the regional level in Latin America and the Caribbean, the processes of cooperation and integration have historically been characterized by their subregional scope and fluctuating nature. The digital agenda is no exception, although its nascent nature should be considered as part of the learning efforts to address a new topic, one that is becoming increasingly central for economic and sustainable development. There is scant evidence of the impact of cross-border data flows on the region’s trade, as well as very few references to their impact on economic value (Meltzer, 2018).

The Pacific Alliance is the most dynamic bloc in Latin America for provisions related to digital trade and cross-border data flows. It has established specific provisions in its foundational agreements from a purely normative perspective, and as a reflection of its trade agreements within the framework of CPTPP. The group of countries that make up the Pacific Alliance (Chile, Mexico, Colombia and Peru) have been inclined towards signing agreements with this type of content, both jointly and unilaterally. In fact, the founding regulations of the Pacific Alliance included more than 50 specific provisions with a considerable scope, insofar as they regulate aspects such as the cross-border transfer of information and the location of computer facilities. While “the Parties recognize that they may have their own regulatory requirements for the transfer of information by electronic means” (article 13.11 of the First Amending Protocol to the Additional Protocol to the Framework Agreement), it is made clear that “no Party may require a covered person to use or locate computer facilities in the territory of that Party as a condition of doing business” (article 13.11 bis). In June 2019, Pacific Alliance countries submitted a communication in the context of the JSI, proposing draft text for a provision on cooperation, which reads “Considering the global nature of electronic commerce, the Members affirm the importance of: ... (c) working together to maintain cross-border information flows as an essential element in the promotion of a dynamic environment for electronic commerce.”¹⁴

Southern Cone countries in Latin America, with the exception of Chile, have participated since the end of the 1980s in the Southern Common Market (MERCOSUR). Until recently, it had shown little progress in terms of specific regulations on digital trade, and in particular on cross-border data flows. However, in January 2021, MERCOSUR countries approved the Agreement on Electronic Commerce, institutionally channelled through a Decision of the Common Market Council (CMC Decision 15/20). This agreement fulfils the same role as a chapter on electronic commerce in a trade agreement (as in the case of the Pacific Alliance or the Central America Free Trade Agreement (CAFTA)), following provisions proposed by the Pacific Alliance in 2018. In this sense, it incorporates some elements of interest in the matter of cross-border data flows: the recognition of the importance of avoiding barriers that constitute a disguised restriction to trade carried out by electronic means, the requirement of mechanisms for the protection of personal data, the prohibition of customs duties on digital products from its member countries, and the prohibition of requirements for locating computer facilities. Parties to MERCOSUR, on the other hand, with the exception of Paraguay, have begun to include specific dispositions on cross-border data flows in their bilateral agreements.

CAFTA is a set of trade agreements that can be classified as a subregional plurilateral agreement, whose membership includes Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and the Dominican Republic, in addition to the United States. As in the case of the Pacific Alliance, it is an agreement generated fundamentally by bilateral and subregional alliances around the United States. CAFTA has served as a platform for the commercial underpinnings of its member countries, and it includes provisions on digital trade. The founding agreement with the United States in 2004 includes a chapter on e-commerce. The agreement concluded in 2011 with Mexico and the one signed in 2012 with the European Union (Title III) also have a similar chapter. With a much more limited chapter on electronic commerce, but a more comprehensive and detailed chapter on telecommunications, it also explicitly mentions that “the development of electronic commerce should be compatible with international data protection standards, with a view to ensuring the confidence of users of electronic commerce”.

Some regional developments in the Caribbean – such as the Revised Treaty of Chaguaramas, the Vision and Roadmap for a Caribbean Community (CARICOM) Single ICT Space, the Regional Information Exchange Initiatives, the Harmonization of ICT Policies and Legislation Across the Caribbean (HIPCAR) Project, and the Caribbean Internet Governance Forum – address and/or facilitate cross-border data flows. While regional harmonization of legislative and regulatory frameworks in the areas of data protection and privacy are gaining traction, apart from general recommendations and guidelines, very few tangible efforts have materialized thus far relating to regional approaches to cross-border data flows (Brathwaite and Remy, 2020).

¹⁴ Communication from Chile, Colombia, Mexico and Peru, Joint Statement on Electronic Commerce, (INF/ECOM/35), 20 June 2019.

However, there is no evidence that any of the above-mentioned Latin American cooperation initiatives have been deepened beyond their initial momentum. Likewise, that first generation of provisions on digital trade, which positioned the Pacific Alliance among the most advanced agreements in this area, has not given rise to a second wave of joint policies. Strictly speaking, there is a great diversity in terms of external partners and international insertion strategies, whose evolution will be key to the future of the Pacific Alliance. For example, Chile is deepening the approach initiated in CPTPP through the Digital Economy Partnership Agreement (DEPA) (see section D), the first trade agreement entirely dedicated to the digital economy (with Singapore and New Zealand), while at the same time concluding bilateral agreements with MERCOSUR member countries; Colombia and Peru have concluded an agreement with the European Union, Japan and the Republic of Korea; and Mexico has signed the USMCA and the European Union–Mexico Trade Agreement, the new versions of their respective agreements with the United States and Canada, on the one hand, and with the European Union, on the other. All these include issues related to e-commerce or digital trade.

Regarding Africa, the Decision on the African Continental Free Trade Area (AfCFTA), (Doc. Assembly/AU/4(XXXIII)) of the 33rd Ordinary Session of the Assembly of the African Union, 9–10 February 2020, initially included a decision for Phase III negotiations, focusing on an AfCFTA Protocol on E-Commerce, to begin immediately after the conclusion of Phase II negotiations (investment, intellectual property and competition policy). The decision “urges Member States to critically review approaches that are being made to them by bilateral partners to enter into bilateral e-Commerce legal instruments with them in order to ensure that Africa is able to negotiate and implement an AfCFTA Protocol on e-Commerce where Africa has full authority on all aspects of e-commerce such as data”. The African Union Assembly has since decided to bring the e-commerce negotiations forward, and has set the deadline for both Phase II and III negotiations for 31 December 2021.

The African Union Digital Transformation Strategy (2020–2030) – which must be actualized by implementing strategies at national level – can give some hints as to the position of African countries on some issues related to data flows. Among the strategy’s specific objectives are the entry into force of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), and the promotion of open standards and interoperability for cross-border trust frameworks, personal data protection and privacy. The strategy cites a lack of supervisory frameworks for data protection and data storage/processing/handling as a weakness of the continent. Further, the strategy notes that realizing the vision of digital transformation for Africa requires appropriate policies and an enabling environment that it describes as including “regulation aimed at enabling free flow on non-personal data”. Elsewhere, the strategy discusses digital infrastructure, and suggests that Africa needs data centre infrastructure in order to ensure cost savings, but also for data sovereignty purposes, to ensure localization of all personal data of African citizens.

3. Results of regulating cross-border data flows through trade agreements

Despite growing efforts by an expanding number of countries to regulate the issue of cross-border data flows in trade agreements, it has been difficult to achieve consensus at the multilateral level. Instead, there has been more progress in selected bilateral and regional agreements. But even in these cases, there is a lack of involvement of countries with less digitally advanced economies. At the time of drafting this report, for example, no African country had entered into any trade agreement containing commitments related to data flows.

Many developing countries remain hesitant to relinquish control over their data through binding commitments in trade agreements without a good understanding of the full implications of such a measure. With the global concentration of platforms, the facilitation of “free flow of data” – as dealt with in trade agreements – may, under current circumstances, effectively result in a “one-way flow” from less digitally advanced economies.

As discussed earlier in this chapter, it may be difficult for trade negotiations to deliver an outcome that both helps to ensure an effective functioning of a global Internet and at the same time takes into

account the multidimensional development opportunities and challenges associated with data flows. First, while the outcome of trade agreements can have significant implications for Internet governance, non-governmental actors typically do not have access to the trade negotiation process in the way they have in multi-stakeholder discussions around Internet governance.

Second, treating cross-border data flows mainly as a trade issue puts developing countries in a difficult position, as most of them lack the capacities needed to engage with this issue in the trade arena. They may consequently come under pressure to accept certain rules on data flows as part of a bargain involving gains in other trade areas. While bargaining across issue areas and economic sectors may be a valid way of moving ahead in negotiations and striking a deal, it is less conducive to providing holistic solutions to complex multidimensional problems such as data flows (Burri, 2017).

Third, by including binding commitments on data flows in trade agreements, it is left to trade dispute settlement mechanisms to determine whether national measures on data are – using language from CPTPP – “applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade”, and “do not impose restrictions on transfers of information greater than are required to achieve the objective”. Ultimately, the extent to which parties commit to free data flows in trade agreements will determine whether, for example, data privacy is to be protected by sovereign countries and the European Union, or is pulled into a supranational legal order on trade (Yakovleva and Irion, 2020).

Against this background, the next section considers some international processes beyond the trade domain that address the regulation of cross-border data flows.

D. INTERNATIONAL AND REGIONAL INITIATIVES ON CROSS-BORDER DATA FLOWS BEYOND THE TRADE DOMAIN

In addition to the trade regime, discussions on cross-border data flows are taking place in other international and regional forums. At the regional level, some developing countries are now relying on regional blocs such as the African Union and ASEAN to develop coordinated regional mechanisms for cross-border digital interoperability and trust, and common regional frameworks for data flows.¹⁵ In the developed world, the European Union is another example of a bloc seeking to increase its digital competitiveness through regional initiatives such as GAIA-X (as discussed in chapter IV). One of the common motivations for such cooperation mechanisms is to facilitate the development of the digital sector in the region, and create more tailored market opportunities for regional players to reduce the dependence on companies from the United States and China. Meaningful regional cooperation on data governance could increase the digital competitiveness of developing economies, and give them some leverage against dominant technology companies (Foster and Azmeh, 2020), although, ultimately, an internationally coordinated approach on data flows is both necessary and desirable. This section provides an overview of some of these international forums, as well as various regional initiatives, with a bearing on cross-border data flows. It first focuses on forums within the broad economic domain, and then examines forums and initiatives beyond the economic domain.

1. Initiatives on cross-border data flows within the broad economic domain

a. *The G20 and “Data Free Flow with Trust”*

In a speech in Davos in 2019, the Prime Minister of Japan highlighted the need for global governance of data, and called on world leaders to start discussions on what he called “data free flows with trust”. He proposed to tackle this issue by calling on the Osaka G20 meeting to “set in train a new track for

¹⁵ See African Union, 2020; and “1st ASEAN Digital Ministers’ Meeting (ADGMIN) 2020 Implementing Guidelines for ASEAN Data Management Framework and ASEAN Cross Border Data Flows Mechanism”, available at https://asean.org/storage/1-Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows_Final.pdf.

looking at data governance, called the Osaka Track, under the roof of the World Trade Organization” (Hurst, 2019). The leaders’ declaration stressed the importance of data flows, while acknowledging the challenges related to privacy, security and data protection. The declaration called for facilitating free data flows, while strengthening consumer and business trust, in order to create data free flow with trust. The declaration also reaffirmed the importance of the interface between trade and the digital economy, noted the ongoing discussion under the Joint Statement Initiative on electronic commerce, and reaffirmed the importance of the work programme on electronic commerce at WTO.¹⁶

Some of the ideas for how to deal with this issue were discussed in the task force for trade, investments and globalization, which was part of Think-20 (T20), one of the engagement groups through which the G20 communicates with international think tanks. A policy brief on “the digital economy for economic development: free flow of data and supporting policies” (Chen et al., 2019) proposed a range of policies relevant to the digital economy. In terms of cross-border data flows, it called for a free flow of data to be the default position, and that public policy intervention should only be allowed under certain conditions, including possible impact on important values or social concerns other than economic efficiency, such as privacy protection, public morals, human health or national security. The policy brief called for a multilateral trade agreement at the WTO to be the ultimate objective, but acknowledged that the difficulty in achieving it suggests countries might pursue alternative routes.

The initiative, however, lacks consensus within the G20, with Indonesia, India and South Africa refusing to sign, arguing that it undermines multilateral negotiating processes based on consensus-based decision-making in global trade negotiations, and denies policy space regarding the digital economy to developing countries (Kanth, 2019).

While this initiative remains to be materialized, its potential impact strongly depends on the definition of trust. Not much progress has been witnessed in the context of the G20; at the Riyadh Summit on 21–22 November 2020, the leaders declared, “We acknowledge the importance of data free flow with trust and cross-border data flows. We reaffirm the role of data for development. We support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, in accordance with relevant applicable legal frameworks, we can further facilitate data free flow and strengthen consumer and business trust.”¹⁷ The G20 is supported by the OECD, which appears to be working on the operationalization of the concept of “data free flow with trust”.¹⁸

However, at the G7 Digital and Technology Ministers’ meeting on 28 April 2021, they declared “Building on the 2019 G20 Osaka Leaders’ Declaration, the 2019 G20 Ministerial Statement on Trade and Digital Economy, and the 2020 G20 Leaders’ Riyadh Declaration, we will draw upon our shared values as like-minded, democratic, open and outward looking nations to support a plan of work which realises the benefits of data free flow with trust. To deliver this, we endorse a Roadmap for Cooperation on Data Free Flow with Trust (Annex 2) which sets out our plan for delivering tangible progress on this agenda, building confidence for businesses and individuals to use technology, as well as driving economic and social value”.¹⁹

¹⁶ See speech by Prime Minister Abe at the World Economic Forum Annual Meeting, Toward a New Era of “Hope-Driven Economy”, 23 January 2019, at G20 Osaka Leaders’ Declaration, available at https://www.mofa.go.jp/ecm/ec/page4e_000973.html; see also https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html; and Osaka Declaration on Digital Economy, available at https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf.

¹⁷ See Leaders’ Declaration G20 Riyadh Summit, 21–22 November 2020, available at https://www.consilium.europa.eu/media/46883/g20-riyadh-summit-leaders-declaration_en.pdf; and G20 Digital Economy Ministers Meeting Ministerial Declaration, 22 July 2020, available at http://www.g20.utoronto.ca/2020/G20SS_Declaration_G20_Digital_Economy_Ministers_Meeting_EN.pdf.

¹⁸ See, for instance, OECD (2020) and Casalini et al., (2021). This topic has also been taken up by the World Economic Forum (WEF, 2020d and 2021).

¹⁹ See Ministerial Declaration, G7 Digital and Technology Ministers, 28 April 2021, available at <http://www.g8.utoronto.ca/ict/2021-digital-tech-declaration.html>.

b. Digital Economy Partnership Agreement

The Digital Economy Partnership Agreement (DEPA) was signed in June 2020, and entered into force in January 2021, between New Zealand, Chile and Singapore. The agreement addresses a range of issues relevant to the digital economy. More specifically, articles 4.2, 4.3 and 4.4 tackle issues related to cross-border data flows and data localization. Recognizing the importance of protection of personal information, article 4.2 commits each party to adopting a legal framework that provides for the protection of personal information, and lists certain criteria for such a framework. The agreement also requires countries to promote compatibility and interoperability between their different regimes for protecting personal information, and provides some possible mechanisms to achieve this comparability. Article 4.2 also includes commitments to transparency and non-discrimination in the adoption of a legal framework for protection of personal data.

Article 4.3 focuses on cross-border data flows, and commits each party to allow the cross-border transfer of data, including personal information, when this activity is for the conduct of the business of a covered person, but it provides for exceptions in which member States can restrict these flows. Article 4.4 commits members not to mandate the use of local computing facilities for data storage as a condition for conducting business, but allows members to adopt measures that violate this principle to achieve a legitimate public policy objective, as long as those measures are not discriminatory or represent disguised restrictions on trade, and as long as these measures do not impose restrictions on the use or location of computing facilities greater than what are required to achieve the objective. Underpinning those commitments, DEPA provides access to a dispute settlement mechanism in cases of violation.

The membership of Singapore in DEPA is part of a broader effort by that country to sign similar agreements. In addition to DEPA, Singapore and Australia signed the Singapore–Australia Digital Economy Agreement, and are negotiating a similar agreement with the Republic of Korea. Reflecting the small and highly open economy of Singapore, the country sees important advantages in positioning itself as a hub for the free flow of cross-border data.

c. Asia–Pacific Economic Cooperation

Discussions around the governance of the digital economy and cross-border data flows have been taking place in the context of Asia–Pacific Economic Cooperation (APEC), a forum for 21 economies in the Asia–Pacific region.²⁰ An early outcome was the adoption in 1998 of the APEC Blueprint for Action on Electronic Commerce, and the subsequent establishment in 1999 of the APEC Electronic Commerce Steering Group. Other important milestones were the adoption of the Action Agenda for New Economy, and the creation of the Ad Hoc Steering Group on the Internet Economy.

More specific to cross-border data flows, various APEC initiatives aim to facilitate the flow of data, while maintaining strong protections for privacy. The APEC Internet and Digital Economy Roadmap adopted in 2017 highlighted the facilitation of the free flow of data within APEC and the importance of promoting interoperability and regulatory cooperation in areas relevant to the digital economy.

One of the important initiatives of APEC is the Cross-Border Privacy Rules (CBPR) system. Based on the APEC Privacy Framework adopted in 2005, the CBPR system was adopted in 2011. The CBPR system is a privacy certification system that companies can join to demonstrate compliance with data privacy protections. It has specific requirements for member States, and also for companies that wish to be certified. At a national level, it requires member States to demonstrate enforceability of measures against violations by any certified company, and it includes a mechanism for cross-border cooperation. For companies to be certified, they need to implement security safeguards for personal data, a mechanism for receiving and investigating complaints, and a mechanism for consumers to access and correct their personal data, among other requirements. The CBPR system was recognized in USMCA, and was also adopted by Japan in 2017 as a valid transfer mechanism (Harris, 2018). Another system developed by APEC is the Privacy Recognition for Processors system, which focuses on certifying data processors.

²⁰ For the list of members of APEC, see <https://www.apec.org/about-us/about-apec>.

To enforce those measures, APEC created the Cross-Border Privacy Enforcement Arrangement. This provides a framework for regional cooperation in enforcing privacy laws by linking the privacy enforcement authorities in each member, and provides a mechanism for sharing information between these authorities.

Through these different protocols and programmes, APEC is playing an important role in creating a regulatory framework for cross-border data flows. Importantly, however, membership in these programmes remains voluntary and member States can choose to join in a specific agreement or programme. For example, only nine APEC members are currently members in the CBPR system.²¹

d. The Association of Southeast Asian Nations

ASEAN is another Asian forum in which regional cooperation on the issue of cross-border data flows is taking place. The ASEAN Economic Community Blueprint 2025 highlights the importance of e-commerce as a channel for cross-border trade and foreign investments. This focus was translated into the ASEAN Agreement on E-Commerce, which was signed in 2019. This agreement included the recognition by member States of the importance of allowing information to cross borders, “provided that such information shall be used for business purposes, and subject to respective laws and regulations”.²² Based on this recognition, member States agreed to facilitate cross-border e-commerce by working toward eliminating or minimizing barriers to the flow of information across borders, subject to safeguards to ensure security and confidentiality of information, and when other legitimate public policy objectives require.

The agreement also includes a restriction on members not to require companies and individuals from other member States to locate computing facilities in their jurisdictions as a condition for operating businesses (with the exception of financial services). In addition, it commits member States to adopt measures to protect personal information. In terms of data protection, in 2016, ASEAN adopted the Framework on Personal Data Protection, which aims to “strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and global trade and the flow of information”.

The framework functions as a record of the participants’ intentions, and does not constitute enforceable legal obligations. It includes some principles that member States recognize and aim to take into account when developing their domestic laws.²³ More specifically to cross-border data transfers, the framework entails that “Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles”. Building from this, ASEAN adopted the Framework on Digital Data Governance, endorsed in 2018, “as an initiative that is intended to enhance data management, facilitate harmonisation of data regulations among ASEAN Member States and promote intra-ASEAN flows of data”.²⁴ In January 2021, the first ASEAN Digital Ministers’ Meeting approved the ASEAN Data Management Framework and Model Contractual Clauses for Cross-Border Data Flows. It also approved the ASEAN Digital Masterplan 2025.²⁵

²¹ See Participation in the APEC Cross-Border Privacy Rules (CBPR) System affords Asia-Pacific Economic Cooperation members a unique opportunity to work, available at <http://cbprs.org/government/>.

²² See ASEAN Agreement on Electronic Commerce, available at <http://agreement.asean.org/media/download/20190306035048.pdf>.

²³ These principles include consent, notification and purpose for the collection of personal data; accuracy and security of these data; the right of the user to access and correct data; retention of data; and accountability.

²⁴ See ASEAN Telecommunications and Information Technology Ministers Meeting, Framework on Personal Data Protection, available at <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>, and ASEAN Telecommunications and Information Technology Ministers Meeting, Framework on Digital Data Governance, available at https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf.

²⁵ See “1st ASEAN Digital Ministers’ Meeting approves Singapore-led initiatives on ASEAN Data Management Framework, ASEAN Model Contractual Clauses for Cross Border Data Flows and ASEAN CERT Information Exchange Mechanism”, available at <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/1/1st-asean-digital-ministers-meeting>; and “ASEAN Digital Masterplan 2025”, available at <https://asean.org/storage/ASEAN-Digital-Masterplan-2025.pdf>.

2. Initiatives on cross-border data flows beyond the economic and trade domain

While the above initiatives are linked to the broader economic and trade agenda, this section reviews some other initiatives on data governance that are taking place beyond the economic space at international and regional levels.

a. *The OECD Privacy Guidelines*

In addition to the work on cross-border data flows in the context of its Going Digital Project and its support to the G20, transborder data flows with a focus on privacy have been discussed for many decades in the OECD. In 2007, the organization's Council adopted a set of recommendations on cross-border cooperation in the enforcement of laws protecting privacy (OECD, 2007). The recommendations recognized the increase and benefits of cross-border data flows, including personal data, and the challenges and concerns this increase has raised with regard to privacy and data protection. To limit disruption to such flows, the OECD Council highlighted the need for a more global and comprehensive approach to foster closer cooperation on issues of privacy and data protection. The OECD Council recommended that member States take steps to:

- Improve their domestic frameworks for privacy law enforcement to better enable their authorities to cooperate with foreign authorities;
- Develop effective international mechanisms to facilitate cooperation on cross-border privacy law enforcement;
- Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information-sharing, subject to appropriate safeguards; and
- Engage relevant stakeholders in discussion and activities aimed at furthering cooperation in the enforcement of laws protecting privacy.

In 2013, the OECD updated its 1980s guidelines on protection of privacy and transborder flows of personal data (OECD, 2013b). Those guidelines include measures related to protection and limits on the collection of personal data, and rights for users to access their data. Based on such protections, the guidelines call on member countries to refrain from any restrictions on transborder flows of personal data with other member States, as long as the other countries observe these guidelines, and as long as effective enforcement mechanisms of these guidelines exist. In this context, any restrictions on transborder flows of personal data, according to these guidelines, should be proportionate. The guidelines call on member States to develop national privacy strategies; adopt laws protecting privacy; establish privacy enforcement authorities; encourage and support self-regulation through, for example, codes of conduct; and provide reasonable means for users to exercise their rights, among other measures. The guidelines call on member States to develop measures to facilitate cross-border enforcement of privacy measures and support the development of international arrangements that promote interoperability among privacy frameworks.

In 2014, the OECD adopted a set of recommendations, the “Principles for Internet Policy Making”, which highlighted support for the free flow of transborder data and the need to ensure compatibility between different national regimes, to limit any disruption to these flows. The first principle is “Promote and protect the global free flow of information” (OECD, 2014).

b. *Council of Europe Convention 108 and Convention 108+*

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (commonly known as “Convention 108”)²⁶ is the only legally binding multilateral instrument on the protection of privacy and personal data open to any country in the

²⁶ See Details of Treaty No.108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

world. Convention 108 was opened for signature in 1981 and, since then, has influenced various international, regional and national privacy regulations. It currently has 55 State parties, of which 8 are non-European. Furthermore, the Committee of the Convention counts over 25 observers, forming a global forum of over 70 countries working together on data protection.

Convention 108 has recently been modernized to adapt this landmark instrument to the new realities of an increasingly connected world, and to strengthen its effective implementation. The Protocol (CETS No. 223) amending Convention 108 was opened for signature in October 2018, and has since been signed and ratified by numerous countries. Once it enters into force, the amending protocol will deliver two essential objectives: facilitating data flows and promoting respect for human dignity in the digital age.²⁷

Convention 108+ is the only open, legally binding, multilateral international treaty on the right to data protection. Recognizing its unique potential to become the global instrument on data protection, the United Nations Special Rapporteur on the right to privacy has recommended “to all United Nations Member States to accede to Convention 108+”.²⁸

The Convention creates a common, global legal space for privacy and data protection. It grants individuals the possibility to fully exercise their right to private life and to the protection of their personal data and, notably, to know which data are collected, stored and processed, how and by whom; to rectify their data, and request their deletion; and to benefit from the strongest redress mechanisms in case of infringements of their rights.

With its balanced standards, it sets the commonly agreed level of protection that individuals should have in the digital age in order to safeguard their dignity and fully enjoy their right to informational self-determination. Convention 108+ represents a viable tool to facilitate international data transfers while guaranteeing an appropriate level of protection for individuals globally.

c. Malabo Convention

In 2014, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection, generally known as the Malabo Convention (Abass, 2017). It aims to provide a regulatory framework to govern the collection and processing of personal data across member States of the African Union. Signatories to the Convention commit to establishing a legal framework to strengthen the protection of personal data, and to publish violations of privacy “without prejudice to the principle of free flow of personal data” (African Union, 2014). At a national level, it requires every country to establish an independent authority in charge of the protection of personal data. The Convention also provides specific regulations on a range of issues relevant to the collection and processing of personal data, including consent of the data subject, legitimacy of the purpose and the process, and transparency. It also provides the data subject with important rights with regard to the process, including the right to information, right of access, right to object, and right of erasure. However, in comparison with other regulations, such as GDPR in the European Union, African Union members can decide to join the Convention or not. The Convention is not yet in force, as this requires 15 signatory States to ratify it. By June 2020, only eight countries (Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda and Senegal) had ratified the convention.²⁹

d. Regional forums in Latin America

The Organization of American States (OAS) has been a constant reference for the countries of the region in terms of governance of the digital ecosystem. This reference has been based fundamentally on three internal bodies of this organization: the Inter-American Commission on Human Rights, the

²⁷ See Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data Consolidated text, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

²⁸ 2018 Annual Report on the Right to Privacy to the Assembly General (A/73/45712) and Annual Report of 1 March 2019 to the UN Human Rights Council (A/HRC/40/63).

²⁹ See “List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection”, available at <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf>.

Inter-American Juridical Committee, and the Inter-American Committee against Terrorism. The Inter-American Commission on Human Rights has exerted a gravitating influence in matters of defence of freedom of expression in the digital environment and, more recently, its guidelines in matters of moderation of digital content. The Inter-American Juridical Committee has been working since 1996 on the protection of personal data, which in 2000 resulted in a document on “Information law: access to and protection of information and personal data in electronic form”. In 2012, it approved a “Proposed Declaration of Principles on Privacy and Personal Data Protection in the Americas”, with 12 principles on the subject. In 2015, it published the “Legislative Guide on Privacy and Personal Data Protection in the Americas”.³⁰

However, for data protection, the *Red Iberoamericana de Datos Personales* (RIDP) appears as the most relevant forum.³¹ Its focus is based on the integral perspective promoted by the European Union, while the Inter-American Juridical Committee has promoted an approach that is closer to the sector-based perspective predominant in the United States. The main objective of RIDP has been to promote among the countries of the region the adoption of a regulatory framework for data protection as a fundamental right and from an integral perspective, as well as an institutional design centred on authorities responsible for guaranteeing its effective compliance and independent of the executive powers. It has grown in membership, institutional complexity and political gravitation.

Since its third meeting in 2004, RIDP has promoted the adoption of a regime of guarantees on the international transfer of personal data in accordance with European standards. This meant achieving recognition of an adequate degree of protection or, failing that, appealing to standard contractual clauses approved by the European Commission. In 2007, the “Guidelines for the Harmonization of Data Protection in the Ibero-American Community”³² were approved, and accession to Convention 108 of the Council of Europe was recommended.

In 2013, a regulation was adopted that established a new institutional structure. Working groups and a Civil Society Forum were also created. Finally, collaboration with OAS was urged to achieve consensus on a draft model law on data protection. This led to the approval of the OAS Principles on Privacy and Personal Data Protection in 2015, which were updated in April 2021. However, the decision of the European Court of Justice in October 2015, according to which the Safe Harbour agreement was ruled invalid, placed the cooperation between RIDP and OAS in crisis. In 2019, the members of RIDP proposed that the organization should position itself in the face of the new challenges posed by the digital agenda, by virtue of their possible impact on the field of privacy. In this sense, they approved a document on Principles and Recommendations for the Processing of Personal Data in Artificial Intelligence.³³ In sum, RIDP has managed to position itself as a forum with a growing ascendancy among interested parties of the region.

The Digital Agenda for Latin America and the Caribbean (eLAC) is a strategy that proposes the use of digital technologies as instruments of sustainable development. This is the digital agenda promoted by the United Nations Economic Commission for Latin America and the Caribbean, in cooperation with the Latin American Development Bank. The Seventh Ministerial Conference on the Information Society in Latin America and the Caribbean, held in November 2020, established eLAC2022. This includes eight

³⁰ The documents of OAS mentioned in this section can be accessed at Department of International Law, Personal Data Protection, available at http://www.oas.org/en/sla/dil/personal_data_protection.asp.

³¹ RIDP (Inter-American Network on Personal Data), was created in 2003; as of 2020, it comprised 33 entities in the public sphere specializing in data protection, most of them Latin American. Among its members are the authorities of Argentina, Colombia, Costa Rica, Chile, Mexico, Peru and Uruguay, as well as authorities from Spain and Portugal. Its observers include bodies from Ecuador, Brazil, El Salvador, Guatemala, Honduras, Paraguay and the Dominican Republic, together with the OAS itself, the European Data Protection Supervisor and the Council of Europe’s Convention 108 Committee.

³² See “Directrices para la Armonización de la Regulación de la Protección de Datos en la Comunidad Iberoamericana”, available at https://www.redipd.org/sites/default/files/2020-01/directrices_armonizacion_iberoamerica_seminario_2007.pdf.

³³ See “La RIDP aprueba sendos documentos sobre Inteligencia Artificial y Protección de Datos Personales”, available at <https://www.redipd.org/es/noticias/la-ripd-aprueba-sendos-documentos-sobre-inteligencia-artificial-y-proteccion-de-datos>.”

areas of action and identifies 39 specific goals, while also containing a specific chapter on the fight against the pandemic and economic recovery. Goal 11 is centred on the promotion of open standards and the promotion of an interoperable regional environment through data exchange that can ensure digital transformation. More particularly, goal 27 encourages the formation of a regional digital market strategy – an initiative that has been discussed in the past five years and which is now resurfacing. It includes specific language on cross-border e-commerce and digital trade through integration of digital infrastructure, regulatory harmonization and free flow of data with trust, among others. Goal 31 also exhorts for greater digital regulatory coherence and harmonization, especially on data protection, cross-border data flows, cybersecurity, e-commerce and digital trade, consumer protection and rights on online platforms (ECLAC, 2020).

E. CONCLUSIONS

This chapter has examined the governance system for cross-border data flows in various international and regional agreements and forums. In recent years, among the most important trends has been the ongoing effort to move the issue of data governance into the trade arena, with the inclusion of issues such as free flow of data across borders and data localization in different trade negotiations. This trend began with the United States adoption of the “digital trade agenda” and the promotion, together with other developed countries, of the inclusion of these issues in trade agreements at multilateral, regional and bilateral levels. At a multilateral level, several advanced economies have pushed for expanding negotiations on digital trade and cross-border data flows in the WTO. Such demands, however, have faced strong opposition from some developing countries and developing country coalitions, leading to limited progress. The result has been the advancement of the ongoing negotiations under the framework of the Joint Statement Initiative on e-commerce.

The success of some developing countries in limiting multilateral negotiations on the issue, however, has not led to a slowdown of efforts to promote rules on cross-border data flows in the trade arena. The first binding commitments on free flow of data and a ban on data localization have been included in CPTPP and USMCA. Overall, the majority of those agreements aim to promote cross-border data flows and restrict the use of data localization policies. These agreements differ, however, in some important areas, particularly in how issues such as privacy and personal data protection are treated, and in the conditions under which countries could deviate from the principle of the free flow of data. On these issues, there are important differences between the approaches adopted by some of the major economies.

International and regional approaches to regulate cross-border data flows are either too narrow, focusing only on aspects such as trade or privacy, or too limited geographically, as in the case of regional approaches.

The gradual expansion of data clauses in bilateral and regional trade agreements leaves developing countries “between a rock and a hard place” with regard to digital and data governance in the trade regime. If some of them continue to resist the adoption of these rules in the multilateral regime, they risk the expansion of such rules in bilateral and regional agreements weakening further their bargaining position in relation to trade negotiations.

Fundamentally, however, there are serious questions about how suitable the trade regime is to regulate the issue of data. Flows of data may be closely linked to goods and services trade in the evolving digital economy; but data are very different from goods and services, and data flows across borders are a different kind of economic flow. Aligning the issues that emerge from this distinction is highly challenging, as can be seen in the effort to align privacy issues with the free flow of data. Provisions in trade

agreements have implications for domestic policies – such as those related to privacy, national security and industrial development – though these implications are not sufficiently considered (Fay, 2020).

Furthermore, developing countries in particular face tougher choices as a result of the link between data and trade. The trading system enables large economic powers to leverage their market size to extract concessions in other areas. As such, developing countries might face the choice of “trading away their right (or policy space) to regulate data flows” to protect other interests in the trade agenda. This is particularly the case considering the ability of advanced economies to leverage their market power at multilateral – but also regional and bilateral – levels. Developing countries, as well, face structural weaknesses in the trade arena related to dispute settlement and to negotiation capabilities that often place them in a relatively weak position.

• The global landscape of the governance of cross-border data flows is a patchwork of different national, regional and international policies.

Despite the growing number of trade agreements addressing data flows, important divergences continue to exist among the main players in the digital economy. Among members of the G20, there are contrasting views, not only on substance (for example, regarding data localization measures), but also on process (such as on the role of WTO as a suitable negotiation venue, given the abundance of parallel regimes related to data privacy, taxation, law enforcement and platform regulation) (De La Chapelle and Porciuncula, 2021).

The discussions in this chapter show that international and regional approaches to regulate cross-border data flows are either too narrow, focusing only on aspects such as trade or privacy, or too limited geographically, as in the case of regional approaches. In developing countries, regional cooperation on data governance has experienced significant progress in Asia, with fewer advances in Latin America and limited progress in Africa. Regional approaches may be useful as a steppingstone towards global data governance, which should be the ultimate goal, given that dealing with cross-border data flows is a global challenge. Moreover, regional approaches that include members at similar levels of digital development are likely to have an easier way than those in which significant power imbalances emerge. Finally, as discussed in previous chapters, global governance of data should consider the multidimensionality of data, and therefore be approached from a global, integrated perspective.

• Cross-border data flows still lack an international regulatory system that can help bring prosperity for all.

Taken together, this chapter, and chapters IV and V, show that the global landscape of the governance of cross-border data flows is a patchwork of different national, regional and international policies. This is summarized in the online annex table to this chapter,³⁴ which provides the information on these regulations for UNCTAD member States.³⁵

³⁴ The online annex to chapter VI is available at https://unctad.org/system/files/official-document/der2021_annex3_en.pdf.

³⁵ This analysis can be complemented by other useful reviews of regulations on cross-border data flows at different levels, such as: OECD (2020) and Casalini et al. (2021); World Bank, (2021); “Global Data Governance Mapping Project of the Digital Trade and Data Governance Hub”, available at <https://datagovhub.elliott.gwu.edu/>; *Foreign Policy*, 6 October 2020, Global Data Governance Database of Policies, available at <https://foreignpolicy.com/2020/10/06/global-data-privacy-collection-laws-database-surveillance-cybersecurity-governance/>; CSIS, “Data Governance”, available at <https://datagovernance.csis.org/>; and University of Lucerne, “TAPED A New Dataset on Data-related Trade Provisions”, available at <https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/>.

Cross-border data flows still lack an international regulatory system that can help bring prosperity for all. The absence of such a system has several implications. First, it increases the risk that the proliferation of different national regulatory approaches will lead to a fragmentation of the Internet, limiting its contribution to sustainable development as a result. Second, those that are best positioned to capture potential gains from data and data flows will be able to further strengthen their already dominant positions. Third, there is increased risk of further polarization between countries on the issue of data flows.

Any global harmonization of data policy will need to take into account that developing countries require policy space to adopt policies for the promotion of technological and industrial development. The problems and challenges of reaching multilateral consensus at WTO on this issue point to a need to consider alternative routes that may offer greater prospects for producing an outcome that enables data to flow across borders, while addressing the multi-faceted implications of such flows. They should allow for an equitable distribution of the gains from these flows, properly addressing the risks involved. These issues are further examined in chapter VII, which looks at possible options for the way forward towards a balanced approach to global governance of data and data flows.

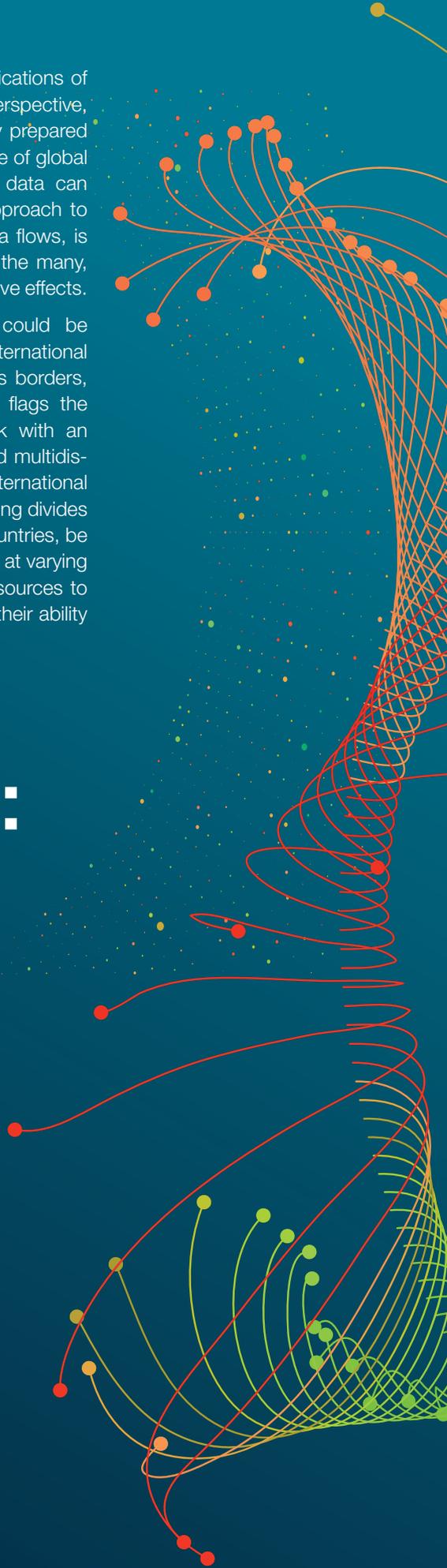


The world is only beginning to understand the implications of the data-driven digital economy. From a regulatory perspective, policymakers and other stakeholders are still poorly prepared to tackle the emerging challenges, many of which are of global reach. Notwithstanding the many ways in which data can contribute to sustainable development, a global approach to the governance of data, including cross-border data flows, is needed to make these flows generate benefits for the many, not just for the few, and address their potential negative effects.

This chapter discusses possible avenues that could be considered, with a view to finding a more holistic, international approach for governing data and their flows across borders, in a way that benefits people and the planet. It flags the possible need for a global institutional framework with an appropriate mix of multilateral, multi-stakeholder and multidisciplinary involvement, possibly to be led by a new international coordinating body. The approach should reflect existing divides and imbalances, ensure the full involvement of all countries, be flexible enough to work for development of countries at varying levels of digital readiness, and devote significant resources to help countries that are trailing behind to strengthen their ability to harness data.

THE WAY FORWARD: IN SEARCH OF A BALANCED APPROACH

VII



CHAPTER VII TOWARDS A BALANCED GLOBAL DATA GOVERNANCE THAT WORKS FOR THE PEOPLE AND THE PLANET

Why is global data governance needed?



How

Key data-related policy areas

- Agree on definitions and taxonomies
- Establish terms of access to data
- Strengthen measurement
- Deal with data as global public good
- Explore emerging forms of data governance
- Agree on rights and principles
- Develop standards
- Increase international cooperation on platform governance



What needs to be done

- **Remedying the underrepresentation** of developing countries in current global and regional initiatives, ensuring local knowledge, needs and views are adequately reflected
- Functioning as a **complement to and in coherence with national policies** for making the data-driven digital economy work for inclusive development
- **Providing sufficient policy space** to ensure countries with different levels of readiness and capacities can benefit from the data-driven digital economy



To enhance the capacities of developing countries to **create and capture value from data domestically**, international support can work to:

Raise awareness of data and their development implications

Build national data strategies

Formulate relevant legal and regulatory frameworks

Ensure their effective participation in international processes

A. RETHINKING REGULATION OF CROSS-BORDER DATA FLOWS

The rapid expansion of digitalization affects all aspects of life, including the way people interact, work, shop and receive services, as well as the ways in which value is created and exchanged. It has revealed the increasing importance of data and data flows, including across borders, in the world economy. Data have become a key economic resource from which value can be created and captured, and they can impact development prospects in various ways. Data can thus play a key role in helping to achieve the Sustainable Development Goals.

While the data-driven digital economy brings significant benefits, it also poses major challenges. It is therefore up to policymakers to shape it in ways that lead to development (UNCTAD, 2019a). But policymakers are struggling to keep pace with the speed of technological advances in an uncertain and fast-evolving context, plagued with numerous unknowns. This has been compounded by the COVID-19 pandemic, which has led to a significant acceleration of digitalization trends, as more and more people have relied on the Internet to continue with their activities, and to cope with the effects of the pandemic. Consequently, there is even more urgency to properly regulate and govern the data-driven digital economy, so that it works for the benefit of people and the planet.

While the data-driven digital economy brings significant benefits, it also poses major challenges. It is up to policymakers to shape it in ways that lead to development.

The pandemic made evident the development lags related to the remaining huge digital divides within and among countries. And as the importance of data grows, a data-related divide is adding to the conventional, connectivity-related, digital divide. Countries with limited capacities to turn data into digital intelligence and business opportunities, and to use them for development, are at a clear disadvantage. Reducing these divides is imperative for achieving development objectives. At the international level, the growing interconnections resulting from progress in digital technologies have led to a new form of international economic interdependence, through cross-border data flows. But this interdependence is asymmetrical, which risks increasing existing inequalities, unless asymmetries are properly addressed. Indeed, the pandemic has accentuated data-related market power imbalances, as global digital corporations have strongly benefited from accelerated digitalization needs, while the rest of the world is struggling to recover from the resulting economic crisis.

The discussions in previous chapters have illustrated the complexity of the many issues at stake, as well as the many trade-offs involved among different players in cross-border data flows in connection to development prospects. Data have particular characteristics that make them different from goods and services. They are intangible and non-rival, but partially excludable; and their value is highly contextual, emerging when they are used, increasing through aggregation and in combination. Thus, data can generate not just private profits, but also social value. As market forces alone cannot ensure the necessary social value creation, there is a need for public policies. The potential social value of data implies that there is a benefit from data-sharing for the society. This would in turn result in the desirability of data flowing freely across borders (when they are of a public nature).

Not all data can be shared, however. When data are kept private, it is those who extract or collect the data who have the capacity to further process them and can appropriate most of their value. This is mainly large global digital corporations based in the United States and China. By contrast, those who can be considered the producers of the data in raw form, the users of the platforms, who are also contributing to that value, do not participate in those gains. As most developing countries are suppliers of raw data, they often fail to capture the benefits from the data generated domestically. Thus, from this

perspective, there is a need for regulating cross-border data flows and platforms, so that the gains are equitably distributed, within and among countries.

There are also non-economic factors to consider in regulating cross-border data flows. Data are multidimensional, as they are also related to privacy, other human rights and national security. This implies the need to regulate these flows to address concerns related to abuse and misuse of data by Governments or the private sector. Indeed, international regulation of cross-border data flows has become one of the major global challenges in the context of the digital economy.

Regulations around the world vary at the national level, and there is little progress at the regional and international levels. Worldwide, there are three main approaches to the governance of the data-driven digital economy, including cross-border data flows, which are becoming major areas of influence: (a) the United States, which focuses on control of the data by the private sector; (b) China, which focuses on control of data by the Government; and (c) the European Union, which favours control of data by individuals on the basis of fundamental rights and values. The current context is one of tensions among these areas, particularly between the United States and China. There is a race for leadership in digital technologies developments, as it is thought that controlling the data and related technologies, particularly artificial intelligence, will secure economic and strategic power.

In this context, there is a risk of fragmentation in the digital space, also often called the “splinternet”. Moreover, global platforms, which in some cases are as big and have as much power and influence as nation States, push for creating their own data ecosystems. These platforms tend to self-regulate, which can also have a significant influence globally. Overall, there is a risk of a siloed data-driven digital economy, which goes against the original spirit of the Internet as a free, decentralized and open network. It is also suboptimal in economic terms as, at the international level, there are more gains to obtain from interoperability.

International regulation of cross-border data flows has become one of the major global challenges in the context of the digital economy.

Countries may have various legitimate public policy reasons to regulate cross-border data flows, such as the protection of privacy and other human rights, national security and economic development objectives. As long as there is not a proper international system to regulate these flows, they do not have any alternative, other than restricting the flow of data as they may deem necessary. Countries also need to adopt different national strategies to develop the data economy. However, data localization is not likely to result in domestic data value addition, because the link between the location of the data storage and value creation is not so clear; there are costs and benefits to take into account. There is no one-size-fits-all policy for regulating cross-border data flows. Policies vary depending on the technological, economic, social, political, institutional and cultural conditions of the different countries.

Given the widely diverging views and positions on the regulation of cross-border data flows, the current state of the international debate is at an impasse. However, as data and cross-border data flows become increasingly prominent in the global economy, there is an urgent need to properly regulate them at the international level. For this to happen, it is necessary to consider data in all their dimensions, both economic and non-economic. However, this should not mean that non-economic factors are used as an excuse to meet economic objectives. Moreover, while data are strongly linked to trade, and can provide strong competitive advantages to those capable of benefiting from them, essentially cross-border data flows are neither e-commerce nor trade, and they should not be regulated as such.

The emphasis placed on privacy varies by country. However, considering that privacy is a human right and that respect for human rights is a core duty, the aim of data-related policies should be to simultaneously respect human rights and promote economic development objectives. Thus, when addressing how

to regulate cross-border data flows, the international community will need to go beyond trade and consider them in a holistic manner; the international policy debate on data should take into account the different perspectives involved, including human rights, security, competition, international taxation and overall Internet governance. This raises the question of which is the appropriate international forum to discuss data-related policies for development.

A global cooperative approach to find common ground for global progress in the data-driven digital economy would be preferable to extreme positions on cross-border data flows, which are suboptimal and cannot be sustained, and would work for inclusive and sustainable development.

Extreme positions on cross-border data flows are suboptimal and cannot be sustained. Thus, there is a need to rethink the regulation of cross-border data flows at the international level, to find the basis for a middle ground and intermediate solutions. This chapter aims to provide a contribution in this direction. A conflict approach is not likely to bring positive results for humanity. A global cooperative approach to find common ground for global progress in the data-driven digital economy would be preferable, and would work for inclusive and sustainable development. Rather than focusing on the differences, efforts should be put into finding common principles and objectives. A balance should be found between national sovereignty claims and the need for the web to be open, and between the diversity that favours innovation and the need for harmonization, to allow data to flow across borders. Also, a balanced distribution of the benefits of cross-border data flows would aim for the reduction of asymmetries and inequalities in the data-driven digital economy.

An international system of regulation of cross-border data flows to benefit people and the planet should ensure that data can flow as freely as possible and necessary, while ensuring more equal distribution of benefits within and between countries, addressing risks related to human rights and national security. This would help ensure the proper functioning of the Internet, and increase trust in the data-driven digital economy.

Special attention needs to be given to the situation of developing countries, which are currently between a rock and a hard place with regard to the governance of cross-border data flows. Officials in smaller or less advanced countries face considerable pressure to choose between dominant realms of data governance. Finding adequate responses to the challenge of governing cross-border data flows requires more international collaboration and policy dialogue, with the full involvement of developing countries. Any consensus will need to incorporate significant flexibilities, considering particular conditions of different countries, to enable all countries to participate in a beneficial manner.

In designing the corresponding regulations, it should be taken into account that data-related risks can emerge from the use of data by the private sector as well as Governments.

Furthermore, in designing the corresponding regulations, it should also be taken into account that data-related risks can emerge from the use of data by the private sector as well as Governments. Data can be used to control or manipulate preferences, choices and decisions. This may eventually lead to pre-designed results to direct society in a particular direction, and may restrict human freedoms. This can happen in economic or political domains, and even threaten democracy. It implies the need for additional balance between the interests of citizens and of Governments, so that individual rights are

respected. Thus, it may be necessary to put in place a proper system of checks and balances, to hold those who control the data accountable.

Against this background, this chapter discusses possible avenues that could be considered, with a view to finding a more holistic, international approach for governing data and their cross-border flows. Section B highlights the imperative of developing a global data governance system. Possible policy options for data governance are presented in section C. Section D explores issues related to the institutional framework that could be needed; it points to the possible need for a new international coordinating body that focuses on data-related matters, and indicates some ways in which this institutional framework could work. For an international approach to work at the national level, it needs to provide for policy space for development, as discussed in section E. Section F discusses capacity-building for data-driven digitalization and policymaking. Finally, section G presents conclusions on the way forward.

B. THE NEED FOR GLOBAL DATA GOVERNANCE

Data governance refers to the ways in which data are managed and regulated to meet different objectives. It can take place at different, interrelated levels:

- The *individual citizen* should handle his or her data with responsibility. It is important to be aware of the risks of digitalization. This awareness can be improved through education and learning. Moreover, individuals can take an active role in claiming their rights. An example is Max Schrems, who has gone far in the defence of privacy rights in the European Union.
- *Communities* also have an important role to play in governing the data of their members in a collective manner. In civil society organizations, individuals and communities can push for progress in data governance through social activism.¹
- The *private sector* should govern data in a way that works not only for private profits, but also for the public interest. Good data governance also helps companies increase their competitiveness as trust is improved. However, there are limits to self-regulation in the private sector, and as this sector's influence and power imbalances in the data-driven digital economy become increasingly evident, the need to strengthen public regulation rises, both nationally and internationally.
- *National and subnational governments*, including cities, in close dialogue with other stakeholders, are responsible for establishing regulations to ensure that data benefit all, while addressing their negative impacts.
- At the *international level* (or regional level as a building block), global governance or international cooperation should aim to reach agreements on the way to facilitate the sharing of social value data globally, for the benefit of people and the planet, as well as enabling cross-border data flows, provided that gains are equitably distributed, and risks properly addressed.

The different levels of data governance are interrelated. Indeed, global data governance is to be understood as being composed of all these interrelated levels of data governance. Thus, it should be a multilayered governance in terms of the actors involved. The relationship among these governance levels goes top-down as well as bottom-up. For the purposes of this Report, the main interest is the international level, without losing sight of the other levels. Policymakers, in close consultation with other stakeholders, should assess which are the data-related regulatory aspects that can remain national (while keeping the global perspective in mind), and which ones require a globally coordinated approach, given the global reach of the digital economy. All levels of data governance should be rooted in global universal values linked to respect for human rights and human dignity – such as equality, equity, development, diversity, freedom, transparency and accountability – so that data work for the well-being of people and the planet.

¹ See UNCTAD, “Social activism needed to rein in tech’s destructive elements”, 13 April 2021, available at <https://unctad.org/news/social-activism-needed-rein-techs-destructive-elements>.

The rationale for a global data governance framework, which complements other levels of data governance, lies in different factors, including the following:²

- Data can provide social value – not only at the country level, but also globally – and support global development. Global data-sharing can help address major global development challenges such as poverty, health, hunger and climate change. The needs for and benefits of global data and information-sharing have been made highly evident as a result of the COVID-19 pandemic; without global cooperation on data and information, research to develop the vaccine and actions to tackle the impact of the pandemic would have been a much more difficult task. Thus, in the same way as some data can be public goods, there is a case for some data to be considered as global public goods, which need to be addressed and provided through global governance.
- The surge in cross-border data flows, the looming implementation of 5G, the Internet of Things and AI, and an acceleration in digitization in the wake of the COVID-19 pandemic create the conditions for vast data collection and monetization globally. However, without a coherent underlying global governance framework to create trust, this could lead to a pullback in data-sharing and amplify already-existing concerns over the lack of transparency in the data value chain, including privacy of personal data, ethical use of AI technologies and monetization of data by social media platforms.
- There is a need for technical coordination across borders to ensure that the world does not end up in fragmentation of the Internet infrastructure and the digital space. This is linked to issues of interoperability of networks and data portability, in order to facilitate data flows.
- The proliferation of national regulations on cross-border data flows leads to confusion over what rules need to be followed, combined with a lack of consistency, coherence and enforcement. This creates uncertainty and elevates compliance costs, which can be particularly pernicious for micro and small enterprises, thus for developing countries in particular.
- Given the interconnected nature as well as the high degree of global interdependence in the data-driven digital economy, national data-related policies have spillovers in other countries.
- The extraterritoriality of some measures may not be suitable for other jurisdictions, which may not be able to influence such regulations, leading to a lack of democratic accountability in those jurisdictions.
- Self-regulation has led to market structures that are defined by the platforms to benefit themselves. This, combined with rules designed for an industrial age, has profound implications for areas such as competition policy and innovation, the distribution of the value from the technologies within and among countries, and social cohesion, nationally and internationally.
- Huge imbalances in market power, as major global digital corporations strengthen their dominance thanks to their privileged access to data, lead to higher global inequality. These platforms have global reach and influence. It is becoming increasingly difficult for countries alone, even developed countries, to address the challenges posed by these imbalances.
- Systemic historical inequalities against developing countries are currently being translated to and even amplified in the data-driven digital space. Their local knowledge and viewpoints are underrepresented in global discussions, while their data are exploited in the absence of proper regulation, and their labour-intensive economies are likely to be the worst affected from the increasing deployment of data-driven digital technologies.
- There is a lack of a comprehensive and coherent assessment of the risks, vulnerabilities and outcomes of the business models of the digital platforms, in particular social media platforms, against a background of rising online harm at the global level. The misuse of private data can, and has, led to widespread social harm, for which there is currently little governance. This is due in part to a lack of access to the data that the platforms gather, which could be used to assess such risks. It is also due to the lack of access to the algorithms used to amplify information.
- Given the interdependencies and the interconnected character of the global architecture of the Internet, the discussion around the future of cross-border data flows cannot be limited to just a few countries.

² This is partly based on Fay (2021).

Thus, global governance of data, as well as the digital economy and digital technologies, is clearly needed because of their global reach and implications on global development. Data-driven digitalization creates global opportunities, as well as global challenges, that require global solutions to harness the positive and mitigate the negative impacts. Effective global governance of data is a prerequisite for data to support the attainment of the economic, social and environmental objectives of the 2030 Agenda for Sustainable Development, having people at the centre.

There is also increasing demand for global data-related cooperation among different stakeholders worldwide.³ The need to improve the handling of data and digital technologies is firmly recognized by the Member States of the United Nations. The declaration by Heads of State and Government representing the peoples of the world at the celebration of the 75th anniversary of the United Nations highlighted digital cooperation as a core area:⁴ “We will improve digital cooperation. Digital technologies have profoundly transformed society. They offer unprecedented opportunities and new challenges. When improperly or maliciously used, they can fuel divisions within and between countries, increase insecurity, undermine human rights, and exacerbate inequality. Shaping a shared vision on digital cooperation and a digital future that show the full potential for beneficial technology usage, and addressing digital trust and security, must continue to be a priority as our world is now more than ever relying on digital tools for connectivity and social-economic prosperity. Digital technologies have a potential to accelerate the realization of the 2030 Agenda. We must ensure safe and affordable digital access for all. The United Nations can provide a platform for all stakeholders to participate in such deliberations.”

C. KEY POLICY AREAS AND PRIORITIES

It follows from the discussion on interdependence in the data-driven digital economy and the cross-sectoral issues at stake that – given the complex interconnections of disciplines, actors, policies and countries involved (influencing each other) – a systems-thinking policymaking approach is needed. It should be interdisciplinary, including aspects related to technology, ethics, economy and development, politics, geography (geopolitics), law, etc. It should also be multi-stakeholder, including all actors involved. At the level of national Governments, it should take a whole-of-government approach, as policy actions in one ministry may affect the objectives of policies in a different area. Overall, global data governance will require a combination of national, regional and international level policymaking, with the full involvement of developing countries.

In the following subsections, a number of key policy areas and priorities – to be considered in a holistic, multidimensional, multi-stakeholder and whole-of-government manner – are discussed. They include working on basic definitions and data classifications; strengthening efforts to measure the value of data and cross-border data flows; establishing terms of access of data; developing data as global public goods; exploring new forms of data governance; defining data rights, principles and data standardization; and coordinating with international cooperation efforts in other economic policy areas related to data.

1. Agreement on a common understanding about definitions of data-related concepts

For international policy debates to reach productive outcomes, it is important that the issues discussed are well defined, and that definitions are agreed among participants. Having different definitions or interpretations poses significant challenges for finding common ground. However, as discussed in chapter II, there is still a lack of definitions of basic concepts related to data and data flows. Knowledge and understanding of the characteristics of data, their 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” (De La Chapelle and Porciuncula, 2021:51).

³ For example, the Committee of the Coordination of Statistical Activities has made a call to action on the need for a new global consensus on data (World Bank, 2021:297). See also MacFeeley (2020b); Pisa et al. (2020); Hill (2020); Ichilevici de Oliveira et al. (2020); Sacks and Sherman (2019); and Carter and Yayboke (2019).

⁴ Declaration on the Commemoration of the Seventy-Fifth Anniversary of the United Nations, available at www.un.org/pga/74/wp-content/uploads/sites/99/2020/06/200625-UN75-highlight.pdf.

From the economic development perspective, the distinction between data (in the sense of raw data) and data products (in the sense of digital intelligence, resulting from the processing of data) become key. Value addition takes place in the data value chain from the collection of data through different phases of organization, analysis and processing into digital intelligence. Given that data value chains expand globally, the different stages of the data value chain can take place in various countries. Thus, it is important to know where value addition is taking place.

There is also room to clarify the meaning of national sovereignty in the context of the data-driven digital economy. In the decentralized, free and open space that the Internet was intended to be, it is difficult to apply the traditional association of national sovereignty to country territories. It is not clear where the border is when it comes to cross-border data flows. Different views and interpretations on what data/digital sovereignty means may lead to confusion on data rights, and raise conflicts with regard to claiming rights over data. Indeed, there is also a need to define what are digital and data-related rights. Also, certainly, some kind of a common understanding needs to be reached on what data governance means and implies at different levels and for different players.

Problems with definitions are common in such a rapidly evolving and complex context, resulting from the fast speed of progress in digital technologies. As the world enters the unknown territory of the data-driven digital economy, many concepts of the conventional economy can directly be transposed by just adding the “adjective” digital, but this does not always apply. Digitalization adds new parameters that significantly change the economic dynamics, and these need to be fully understood. Thus, efforts to reach common definitions need to be redoubled to facilitate policymaking in a challenging context.

The various taxonomies used to classify the type of data are based on different criteria. However, the interface between the different taxonomies and cross-border data flows has not yet been sufficiently explored. While establishing data classifications is not an easy task, it would be advisable to increase efforts to agree on a common taxonomy of types of data that is the most meaningful for the purposes of regulation of cross-border data flows. This would allow the establishment of terms of access to data, as explained in the next subsection, and would also determine which data are to be considered public goods.

2. Establishing terms of access to data

Once a relevant taxonomy of types of data could be agreed upon, agreeing on establishing terms of data for each type could clear the way towards the facilitation of cross-border data flows. Each type of data would flow according to the conditions established in those terms. These terms could determine which data are to remain within national borders and which can flow across borders. They would also determine who has access to data, under which conditions and for which use. Thus, different organizations or individuals would have different access rights to the various types of data. These would require a trustworthy institutional framework for managing, monitoring and enforcing the terms of access (Coyle et al., 2020). These terms would include:

- Who can collect the different types of data, how they can be collected, and for what purposes;
- Who can access the data (access rights) and on what terms (conditions for data to be shared, either nationally or internationally);
- Who is accountable, and how, in case the terms in the collection, sharing, use or control of the data are not met.

3. Strengthening efforts for measuring the value of data and cross-border data flows

Well-informed policymaking needs to be properly based on evidence. As this Report shows, finding data on data is a daunting challenge. Available statistics of data traffic are hard to interpret. Regarding the value of data and cross-border data flows, significant gaps impede the development of a good understanding of what is really happening. Statistics on international bandwidth are widely used when

discussing cross-border data flows. However, they are not a good indicator, even as a proxy. They only reflect the volume of the data that flow, without any sense of direction, and without distinguishing between data and data products. Thus, there is no possibility of discovering what the flow of value related to data across borders is. Indeed, it is not the flow of data that matters, but the flow of value associated with data. Without such evidence, it is not possible to assess the effects of different regulations on cross-border data flows, and their relationship with development.

Moreover, most data on data are handled by the private sector,⁵ which keeps the information proprietary. As data have increasingly become a key economic resource for value creation and capture, determining the course of international economic relations through cross-border data flows, it becomes increasingly urgent to strengthen statistical work to produce more official indicators in this area, to be made publicly available. There is also a need to explore ways to require major digital platforms to share more information on their data that can be of value for policymaking. Otherwise, policymakers lack the necessary evidence compass for their decisions.

4. Data as a (global) public good

As discussed in chapter III, digital public goods, including data when they are of a public good nature, are essential for unlocking the full potential of digital technologies. The scope for creating and capturing value from data is expanded when organizations have a large and diverse data set available to them. Availability of such data globally has often been limited, due to firm control of data, or because such data embed personal details that cannot be shared. Nevertheless, where larger data sets have been made more openly available, this can lead to significant use for social value and potentially strong development impacts. Two recent examples of this are the value of data during the health crises of Ebola and COVID-19 (Moorthy et al., 2020; Wesolowski et al., 2014), and where cities have benefitted from being able to leverage private firms to share urban data.

Such successful examples have led to calls for broader initiatives that support international cooperation on global digital public goods, with mechanisms and platforms that expand such ideas. According to the United Nations High-level Panel on Digital Cooperation, “Many types of digital technologies and content – from data to apps, data visualization tools to educational curricula – could accelerate achievement of the SDGs. When they are freely and openly available, with minimal restrictions on how they can be distributed, adapted and reused, we can think of them as ‘digital public goods.’” It recommended that “a broad, multi-stakeholder alliance, involving the UN, create a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs” (United Nations, 2019).⁶

In terms of data, “digital public goods” could entail large public data pools that are shared under open licences and which have been carefully anonymized to reduce risks of personal identification. The term might also include open source tools and platforms to allow access and processing of such data to provide digital intelligence (Gurumurthy and Chami, 2019). Linked to such calls, the Digital Public Goods Alliance was created. It has identified six key areas relevant to the Sustainable Development Goals in order to build a collection of digital public goods: early grade reading, financial inclusion, climate change adaptation, digital health, digital and job skills, and remote learning.⁷

The notion of data “as a public good” may also provide an important approach for alliances of countries and development-oriented organizations to come together to support cross-border data-sharing. As the previous successes of open government data have shown, useful data are often available within Governments, as well as within firms. However, making them available requires additional activities and support, as well as appropriate tools, in order to support development outcomes. Learning from

⁵ For example, by companies such as Cisco, International Data Corporation (IDC) and TeleGeography.

⁶ See the United Nations Office of the Secretary-General’s Envoy on Technology, available at www.un.org/techenvoy/content/digital-public-goods.

⁷ See Digital Public Goods Alliance, available at <https://digitalpublicgoods.net>.

such data alliances can potentially play an important role in pushing “digital public goods” as a key component for supporting the attainment of development goals.

5. Exploring emerging forms of data governance

Alternative forms of data governance are emerging to enable the sharing of data for public interest purposes. In the current context, it is the large digital corporations extracting the data that control what is done with those data, and therefore privately appropriate most of the benefits. However, given the multiple agents involved as sources of data and/or being impacted by their use, data stewardship needs to be seen in ways that can contribute to development. There is a need to rethink data governance for it to work for people and the planet. Thus, new models of data governance are emerging that allow for different actors to partner and pool together data, allowing the enhancement of the social value of data. These include data cooperatives, data commons, data collaboratives, data trusts, data fiduciaries, indigenous data sovereignty and data marketplaces (UNCTAD, 2019a; Micheli et al., 2020; Mozilla Insights et al., 2020). Data collaboratives, as an emerging form of partnership where participants exchange data for the public good, have huge potential to benefit society and improve AI. They can create value by improving situational and causal analysis; enhancing decision-makers’ predictive capacity; and making AI more robust, accurate and responsive (Verhulst, 2019).

These digital data partnerships – bringing together different organizations, including public agencies, to join forces to collect, exchange, combine and share their data – are multiplying worldwide (Gagnon-Turcotte, Sculthorp and Coutts, 2021). Many practical examples already exist in a variety of areas related to health, environment, research, agriculture and food, and economic development. And they can cover different territories; they may be local, but also work across borders. Inventories of these emerging data governance practices are provided, for example, in the Data Collaboratives Explorer by GovLab, and in the Data for Empowerment project of Mozilla’s Data Futures Lab.⁸ While these initiatives are only at early stages and they are not numerous, they can provide useful insights on the way forward on how to improve the sharing and use of data for the public interest. In this connection, a “responsible data” or “data for good” movement has emerged. It calls on companies to share their data for philanthropic purposes in what is called “data philanthropy” (UNDP, 2020). Further, the European Commission has been exploring the potential of data-sharing across the European Union to help public administrations use private sector data for the public good (European Commission, 2020b).

6. Digital and data-related rights and principles

As discussed above, there is a need to properly define digital and data-related rights. The next stage is to recognize them. In recent years, there has been a proliferation of declarations, charters or manifests on digital and data rights and ethics at various levels (Digital Future Society, 2019). An early example is the 2011 Charter of Human Rights and Principles for the Internet by the Internet Governance Forum (IGF). Some other examples include:⁹

- Digital Justice Manifesto;
- Data for international health emergencies: governance, operations and skills;

⁸ See <https://datacollaboratives.org/explorer.html?#data-pooling> and <https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/>. See also Data Collaboratives, Leveraging Private Data for Public Good. A Descriptive Analysis and Typology of Existing Practices, available at <https://datacollaboratives.org/static/files/existing-practices-report.pdf>.

⁹ For more information on these, see www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf, <https://justnetcoalition.org/digital-justice-manifesto.pdf>, https://rsc-src.ca/sites/default/files/DES7289_3_S7%20Statement_Data_EN_FINAL.pdf, <https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf>, www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html, https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/SEDIA_Carta_Derechos_Digitales.aspx, https://ec.europa.eu/isa2/sites/default/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_.pdf, <https://citiesfordigitalrights.org/declaration> and https://digitaldeclaration.com/img/uploads/EN_DigitalDeclaration_2-Page_R3_WEB_2020-compressed_200225_115932.pdf.

- African Declaration on Internet Rights and Freedoms;
- Digital Charter of Canada;
- Digital Rights Charter in Spain;
- Berlin Declaration on Digital Society and Value-Based Digital Government;
- Declaration of Cities Coalition for Digital Rights;
- Digital Declaration (commitment to responsible business for the digital age).

These and other examples show that there is a need to define and recognize rights in a new context of the data-driven digital economy. These rights declarations and principles are highly aspirational, and do not imply any obligations. However, they are mostly human-centred and can provide a useful guide for progress in finding common ground on data rights at the global level.

Problems regarding data rights are also present in commercial law. As noted by the United Nations Commission on International Trade Law (UNCITRAL, 2020:5), “In the context of data transactions, there appears to be uncertainty not only between parties as to the rights and obligations to be embodied in their contracts, but also on the part of lawyers and judges as to the application of existing rules and principles of contract law.”

It could even be the case that there is a need for revising overall rights frameworks, updating them to the new realities that were not present when they were designed. The need to regulate in the digital economy tends to be seen as just making the new phenomena fit into the existing regulations. For example, cross-border data flows have been considered to fall under the international trade regime, which is where their international regulations are discussed. However, as discussed in this Report, data are very different from goods and services, and regulation of their flows across borders requires a different approach from that of international trade.

Similarly, it is simply understood that human rights in the analog world are to be respected in the digital space. The United Nations Secretary-General, in his call to action for human rights in the middle of the pandemic, highlighted that “we continue to advocate that human rights apply online” (United Nations, 2020c). Certainly, this is the case. But it could be that new human rights violations have emerged in the digital space that did not exist when the Universal Declaration of Human Rights was adopted. For example, nobody could have foreseen that the right to be forgotten would be important in 1948, but currently old information in social media about a person could prevent that person from being selected for a job. Thus, it may be necessary to think outside the box.

7. Data-related standards

Another way to progress in the facilitation of cross-border data flows for inclusive development with the necessary safeguards in place is through standardization. It may help ensure that data can move among different countries and systems, by facilitating necessary features for interconnection such as interoperability and data portability. These also foster trust in the digitalization processes, and set appropriate benchmarks regarding data governance (Girard, 2019, 2020). Standards may be related to different areas, such as technical aspects or privacy. It is also critical to develop “common standards on open data that can guide the private and public sectors on how to provide open access to data sets, ensuring that more data become available as digital public goods, while respecting privacy and confidentiality” (United Nations, 2020a).

As discussed in chapter IV, the main areas of influence globally in terms of data governance are the United States, China and the European Union. All these areas are aiming to set global standards in the data-driven digital economy. However, it is evident that there is no one-size-fits-all approach towards data governance, as technological, economic, political, institutional and cultural conditions vary among countries. Thus, standards need to be flexible enough to be adaptable to the particular conditions in each country. Standards are not to be imposed. They need to be agreed collectively, inclusively and globally.

8. International cooperation efforts on platform governance

Unequal exchanges in the data-driven digital economy are closely related to market power imbalances resulting from the dominance of global digital corporation and their capacity to use tax optimization practices to avoid paying their fair share of taxes (UNCTAD, 2019a). Thus, platform governance involving competition and tax policies has a key role to play to redress those imbalances. Although these policies tend to be applied at the national level, there is significant room for international cooperation. And this cooperation is dearly needed in view of the global reach of the major companies involved. No single country's authority in competition or taxation alone can tackle the challenges posed by big digital corporations. Even developed countries and groups of countries, such as the United States and the European Union, are struggling in these areas.

There is increasing agreement on the need to adapt competition policy to the new reality of the data-driven digital economy (UNCTAD, 2019a; Gökçe Dessemond, 2020). However, progress on international cooperation is slow. International dialogue has taken place, for example, at the UNCTAD Intergovernmental Group of Experts on Competition Law and Policy. Another example is the "Common Understanding" issued by competition authorities of G7 countries in 2019.¹⁰

International cooperation has taken a more active role in relation to taxation in the digital economy context in recent years. Complex negotiations have taken place in the OECD on base erosion and profit shifting. A global and consensus-based solution was expected by mid-2021 (OECD, 2021); in July 2021, 130 countries and jurisdictions of the G20/OECD Inclusive Framework on BEPS (Base Erosion and Profit Shifting) joined a new two-pillar plan to reform international taxation rules and ensure that multinational enterprises pay a fair share of tax wherever they operate. This also includes a global minimum corporate income tax of 15 per cent.¹¹ Although the G20/OECD Inclusive Framework on BEPS counts 139 countries, it still lacks in inclusiveness with regard to the voice and participation of developing countries. This was preceded by the June 2021 agreement reached by the G7 Finance Ministers on global tax reform that could mean that the largest multinational tech giants would have to pay their fair share of tax in the countries in which they operate. They also agreed to the principle of a global minimum rate that ensures multinationals pay tax of at least 15 per cent in each country where they operate.¹²

While these are steps in a positive direction, it is an agreement among a few developed countries. As discussed in UNCTAD (2019a), the United Nations Committee of Experts on International Cooperation in Tax Matters is a more inclusive venue to deal with taxation issues from a development perspective, and should be strengthened. It has continued its work on taxation in the digital economy, with special focus on impacts on developing countries (United Nations, 2021).

In sum, all these policy options highlight that there is a need for increased international policy dialogue in order to progress towards more effective global data governance. Data ethics principles or declarations on data rights, as well as standards, can be considered as initial steps in the right direction. However, these tend to be applied on a voluntary basis. An effective regulation of cross-border data flows may need to go beyond voluntary approaches to ensure compliance. To respond to international cooperation needs, certain aspects of data governance will require new regulatory frameworks to be agreed at the international level, and adopted nationally.

¹⁰ See G7, "Common Understanding of G7 Competition Authorities on 'Competition and the Digital Economy'", available at www.ftc.gov/system/files/attachments/press-releases/ftc-chairman-supports-common-understanding-g7-competition-authorities-competition-digital-economy/g7_common_understanding_7-5-19.pdf.

¹¹ See OECD/G20 Base Erosion and Profit Shifting Project, Statement on a Two-Pillar Solution to Address the Tax Challenges Arising From the Digitalisation of the Economy, 1 July 2021, available at <https://www.oecd.org/tax/beeps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-july-2021.pdf>.

¹² See "G7 Finance Ministers Agree Historic Global Tax Agreement", available at www.g7uk.org/g7-finance-ministers-agree-historic-global-tax-agreement/; and "G7 Finance Ministers and Central Bank Governors' Communiqué", available at www.g7uk.org/g7-finance-ministers-and-central-bank-governors-communique/.

This raises the question of which could be the most appropriate institutional framework at the global level for the development of global data governance. When agreeing on regulations to be applied at the national level, certainly the intergovernmental approach is to play a major role. However, existing intergovernmental bodies may not be well positioned to deal holistically with data governance matters. Given the particular multidimensional character of data, their broad and increasingly critical relevance, the many issues and interest at stake, as well as the rapidly evolving context filled with unknowns, there is a need to consider innovative solutions. It should be meaningfully multilateral, multi-stakeholder and multidisciplinary, to include all the complex interrelations that data bring about. Possibilities for the institutional framework for global data governance are explored in the next section.

D. INSTITUTIONAL FRAMEWORK

Debates concerning data have taken place at different forums of policymaking at a regional or global level and in various forms. Emerging from the birth of the Internet, so-called “Internet governance” organizations were designed to govern technical issues as the Internet expanded globally (such as the domain name system and Internet protocols). In addition, the IGF has sought to foster a multi-stakeholder dialogue on related broader economic and social issues. However, the lack of formal rulemaking power has limited its ability to shape policy directions. Therefore, the question remains about which the appropriate forums for broader global data governance are.

The United Nations High-level Panel on Digital Cooperation set up by the Secretary-General undertook consultations with a wide variety of stakeholders, including on how digital cooperation should take place. In its report (United Nations, 2019:22), it noted that “we heard a great deal of dissatisfaction with existing digital cooperation arrangements: a desire for more tangible outcomes, more active participation by governments and the private sector, more inclusive processes and better follow-up. Overall, systems need to become more holistic, multi-disciplinary, multi-stakeholder, agile and able to convert rhetoric into practice.” The report identified six main gaps:

- Low priority assigned to digital technology cooperation nationally, regionally and globally;
- Lack of inclusivity in work that is underway by technical and standard-setting bodies, and even the lack of capacity of many to participate effectively and meaningfully;
- Overlapping and complex digital cooperation architecture that may affect its effectiveness;
- Insufficient communication and creation of synergies across bodies to respond to digital technologies increasingly cutting across areas in which policies are shaped by separate institutions;
- Lack of reliable data, metrics and evidence upon which to base policy; and
- Lack of trust among Governments, civil society and the private sector, which can make it more difficult to establish the collaborative multi-stakeholder approach needed to develop effective cooperation mechanisms.

The Report also recommended undertaking a consultation process to develop updated mechanisms for an improved global digital cooperation architecture. These consultations were still ongoing at the time of preparing this Report.¹³

Indeed, existing institutional frameworks at the international level are not fit for purpose to address the specific characteristics and needs of global data governance. For it to be effective, a new global institutional framework is most likely needed. This section discusses why such a framework would need to be multilateral, multi-stakeholder and multidisciplinary. Global governance of data may also require the creation of a new international body that would play a globally coordinating role.

¹³ See “Recommendation 5A/B. Options for the Future of Global Digital Cooperation”, available at www.global-cooperation.digital/GCD/Redaktion/EN/Downloads/options-for-the-future-of-global-digital-cooperation.pdf?__blob=publicationFile&v=2; and “Follow-up on Digital Cooperation Architecture”, available at www.global-cooperation.digital/GCD/Navigation/EN/Follow-up/follow-up.html.



1. Multilateral, multi-stakeholder and multidisciplinary framework

The analysis in this Report confirms that addressing the complications resulting from the multiple interconnections and interdependences among the different dimensions of data, the various actors involved and emerging trade-offs requires a combination of a multilateral, multi-stakeholder and multidisciplinary approach to global data governance. Indeed, in a mapping exercise of key issues and interrelationships in global digital governance, data play a core part of all the areas considered: technology, legal, sociocultural, economic, development, human rights and security (Kurbalija and Höne, 2021).

So far, global governance of data and digital technologies has taken place on different tracks. Most issues related to Internet governance, as a communications network, have been dealt with in multi-stakeholder forums. A well-organized and globalized Internet community is deeply invested in approaches to coordinate Internet resources and making the network of networks function efficiently. This is of a highly technical nature, and takes place in various institutional settings, such as the Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C). These processes normally take place on peer-to-peer participation on an equal footing (UNCTAD, 2017).

Among current forums, the extent to which all stakeholders can contribute varies considerably. With the growing role of data in society, other data-related organizations have moved towards improving the multi-stakeholder component. For example, the Council of Europe's Convention 108 includes a forum where national Governments, regulators, private sector stakeholders and civil society representatives can all receive information and share insights on the promotion and improvement of the Convention (UNCTAD, 2016). For the IGF, the United Nations Secretary-General has established a Multi-stakeholder Advisory Group to advise on the programme and schedule its future meetings.

In addition, the United Nations Commission on Science and Technology for Development (CSTD) provides a valuable framework for all stakeholders to articulate the role of digital technologies and data, as enablers of the Sustainable Development Goals, and to inform and advise the policymaking bodies of the United Nations. With its mandate to provide the General Assembly and the Economic and Social Council with high-level advice on science and technology issues for development, it could be further leveraged in exploring the connection between data, Internet governance and development (box VII.1).

Actors in the Internet community may benefit from the views from other socioeconomic policy or human rights areas, to help them better understand what is needed in terms of development. Conversely, policymakers could benefit by engaging with other actors, with a more specialized technical knowledge of the evolving digital context, and a view to ensuring that any agreement relevant to data issues is operationally feasible, politically sustainable and less likely to have any unintended or undesirable consequences (UNCTAD, 2017). It may also be the case that addressing some of the data technologies-related issues needs to be done through technical solutions. In addition, it is not only economic or technical disciplines that need to be considered in the data governance processes, but also other social sciences and humanities related to ethics and human rights.

Finding the appropriate mix for such multilateral, multi-stakeholder and multidisciplinary engagement will require some innovative thinking. It should be as much a top-down as a bottom-up approach; the governance mechanism should aim for these approaches to meet somehow. For practical reasons, this may imply that not all aspects of governance need to be dealt with by all the groups or levels involved at the same time. Some kind of multilayered governance could be envisaged. However, a higher-level coordinating system at global level would be key. New forms of governance for data could be explored, including distributed and polycentric data governance models (Verhulst, 2017; Singh, 2019). Moreover, given the increasing influence of digital technologies in our lives and society, as well as in the world economy and for international relations, technology diplomacy is deemed to play an increasing role (Kurbalija and Höne, 2021; Feijóo et al., 2020).

Box VII.1. The Commission on Science and Technology for Development (CSTD) and international cooperation to address public policy issues related to the Internet

The CSTD, a subsidiary body of the Economic and Social Council, is the prime forum of the United Nations for the treatment of the development implications of science and technology. As such, it provides a global platform for discussions and consensus-building on digital technologies. A major component of its mandate is its role as the focal point for the system-wide follow-up to the World Summit on the Information Society (WSIS), with its core principles and action lines in terms of digital cooperation agreed by the international community. The reports of the CSTD on WSIS provide one of the largest international repositories of knowledge, experiences and international discussions on the development dimensions of digital issues.^a

The CSTD has moved forward in critical aspects of the digitalization of the economy and society, both in terms of policy and practice. It supported a successful working group on improvements of the IGF (2011–2012)^b and two Working Groups on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet (2013–2014 and 2016–2018).^c This work resulted in the identification of high-level characteristics, as well as guiding principles, for implementation of enhanced cooperation when developing international Internet-related public policy. However, in spite of significant convergence of views in important areas of public policy related to digitalization, it also led to recognition of the persistence of different sensitivities and approaches of several others.

The knowledge and experience accumulated by the CSTD in these highly complex and politically sensitive processes could, if member States so decide, serve as valuable inputs to further deliberations within the United Nations on the connections between Internet governance, data governance and development.

Source: UNCTAD.

^a See “ECOSOC Document – WSIS Follow-up”, available at [https://unctad.org/publications-search?f\[0\]=product%3A667](https://unctad.org/publications-search?f[0]=product%3A667).

^b See “Improvements of the Internet Governance Forum (2011–2012)”, available at <https://unctad.org/topic/commission-on-science-and-technology-for-development/igf-2011-2012>.

^c See “Working Group on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet (2013–2014)”, available at <https://unctad.org/topic/commission-on-science-and-technology-for-development/wgec-2013-2014>; and “Working Group on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet (2016–2018)”, available at <https://unctad.org/topic/commission-on-science-and-technology-for-development/wgec-2016-2018>.

2. Is there a need for an international coordinating body dealing with data-related issues?

Despite the recognized need for greater global collaboration on digital governance, there has been little substantive progress on how to achieve it. The above-mentioned Report of the United Nations High-level Panel on Digital Cooperation proposes three different types of models: an “Internet Governance Forum Plus” building on the existing IGF, a “Distributed Co-Governance Architecture” or a “Digital Commons Architecture”. The chosen model would be run by the United Nations.

An alternative to building upon existing organizations that already have their hands full, and that are being pulled in too many directions, would be to recognize that the digital era requires an institution that is focused on, and has the skills for, assessing and developing comprehensive global digital and data governance. It would recognize that our current global institutions were built for a different world, that we are now in a new digital world dominated by intangibles, and that new governance structures are needed. In the words of Medhora and Owen (2020), “we need a Bretton Woods-type model that mitigates the negative implications of the digital revolution and ushers in a new era of shared prosperity”.

One proposal for a possible option to move forward suggests drawing inspiration from the Financial Stability Board, which was set up by the G20 to reign in and reregulate global banks and insurers, following the light touch regulation and regulatory lapses that led to the 2008 global financial crisis. In

a similar manner, a Digital Stability Board could be created to deal with the complex global policy and regulatory issues arising from digital technologies.¹⁴ It could have mandates to:

- Coordinate the development of standards, regulations and policies across the many areas that platforms touch. The areas would include – but not be limited to – governance along the data and AI value chain (including areas such as privacy, ethics, data quality and portability, algorithmic accountability, etc.); social media content; competition policy; and electoral integrity. The objective of coordination would be to develop a set of principles and standards that could be applied globally, while allowing for domestic variation to reflect national conditions.
- Assess vulnerabilities arising from these technologies, including their impact on civil society, and the regulatory and policy actions needed to address them on a timely basis.
- Monitor developments, advise on best practices, and consider regulatory and policy actions needed to address vulnerabilities in a timely manner.
- Ensure that this work feeds into other organizations, which need to modernize rules to reflect big data and AI, but also to develop a framework with which to assess the implications.

Under the auspices of such a board, there would be a clear opportunity for developing and developed countries to work together. Its creation would be a statement, and acknowledgement, that the digital realm needs its own institution and integrated international governance. It would be explicitly outcome-focused – for example, deriving voluntary standards; and implementing, assessing and evaluating changes – in a multi-stakeholder setting, to avoid the capture of vested interests. It would not be treaty-based, at least initially, given that the requirements to create such an institution would be high and could in fact deter its creation. Rather, it would be a forum for discussion.

This proposal contains some useful elements to move in the direction of the creation of an international coordinating body that focuses on data-related issues. However, stability would not be one of the major problems in the digital economy; indeed, capturing the many complexities involved in the data-driven digital economy in one single objective does not seem feasible. Most importantly, it is a proposal focusing just on the G20.

As for the discussions in this Report, much more is needed. For the global debates on data and AI governance – as well as the potential creation of an international body or eventual regulatory frameworks resulting from those debates – to be fully inclusive, they should take place under the auspices of the United Nations, which is the most inclusive international forum in terms of country representation. Currently, developing countries are underrepresented in global and regional initiatives, which results in neglecting local knowledge and the cultural context, as well as their interests and needs, in global discussions, and contributes to increasing inequality (box VII.2).

The international policy debate should also combine intergovernmental with meaningful multi-stakeholder processes. Moreover, inclusiveness should start with the language used. As noted above, there have been voices calling for a new digital Bretton Woods moment or for a Digital New Deal. The Bretton Woods agreements and the New Deal were great achievements in their time, contributing to a prosperous recovery after World War II and much-needed multilateral cooperation. While the current circumstances may be similar in a number of aspects, the situation now is not the same. As many developing countries were not yet independent at the moment the Bretton Woods agreements were reached, they were not part of them. And the New Deal was the policy of just one big power. Besides, the evolving digitalization context is much different. Thus, it would be advisable to use some creativity in finding new terms that more appropriately reflect the current realities and needs of all countries and stakeholders.

Indeed, there are already various initiatives at the United Nations focusing on data governance-related matters. Some have already been discussed in this chapter, such as the United Nations High-level Panel on Digital Cooperation, the IGF and the CSTD. Some other examples are presented in box VII.3, although it is not an exhaustive list; many other agencies, as well as regional economic commissions, are increasingly working on these issues. This would already call for a strong coordinating body in the United Nations system. Data have become a key economic and strategic resource – which

¹⁴ For more details on the Digital Stability Board proposal, see Fay (2019).

Box VII.2. Participation of developing countries in global data governance

For international data governance to respond to the needs of countries at highly different levels of readiness, so that they can engage in and benefit from the data-driven digital economy, they need to have representation and their voices heard in the corresponding debates. Discussions need to be global, with the full involvement of all regions, including developing countries with nascent digital economies. At present, the representation of the least advanced economies is limited in the main forums for the discussion on how to govern data. Some examples include:

- The Council of Europe Convention 108 – the agreement with the broadest support and the greatest potential for driving compatibility – has 55 State parties, only 2 of which are LDCs (Burkina Faso and Senegal).
- In the Joint Statement Initiative negotiations on e-commerce at the World Trade Organization (WTO), as of May 2021, only four LDCs had decided to participate (Benin, Burkina Faso, the Lao People's Democratic Republic and Myanmar).
- The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) has been ratified by only eight countries, including five LDCs (Angola, Guinea, Mozambique, Rwanda and Senegal).
- Fewer than half of the LDCs have adopted data protection and privacy legislation.
- A review of data governance initiatives found relatively few examples of scalable initiatives for more than a handful of data governance approaches that are frequently repeated. Most of them were undertaken in a handful of European countries, Canada and the United States, and primarily in English (Mozilla Insights et al., 2020).
- There are also a number of global initiatives that set norms for the development and use of AI. However, developing countries are largely absent from or not well represented in most of them, although these initiatives could have significant impacts on their economic and social development.

Source: UNCTAD.

affects all actors, sectors, activities and countries – as well as a fundamental ingredient to support the achievement of the Sustainable Development Goals. Thus, their governance needs to be addressed in a cross-sectional manner. However, the rapidly increasing relevance of data and digital technologies in the global economy, and the particular needs for their governance, may necessitate a dedicated international coordinating body focusing on global data governance and development, with a mandate to coordinate the data-related activities in the United Nations system.

The work of such a coordinating body should be complementary to and in collaboration with other regional and global initiatives and proposals related to data governance, including those discussed in chapter VI. Some other global data-related initiatives are presented in box VII.4.

Moreover, there have recently been increasing calls for forming coalitions or alliances of like-minded countries on data and digital technologies-related matters.¹⁵ One example of a recently launched alliance is the Trade and Technology Council between the European Union and the United States to lead values-based global digital transformation.¹⁶ At the country level, China has proposed a Global Initiative on Data Security.¹⁷ For global development purposes, these initiatives may be useful only to the extent that they are thought of as building blocks, with a final purpose of contributing to true global

¹⁵ See, for instance, Fogh Rasmussen (2021), Vestager and Borrell (2021) and Imbrie et al. (2020).

¹⁶ See European Commission “EU-US launch Trade and Technology Council to lead values-based global digital transformation”, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990; and European Council, “EU-US summit statement: ‘Towards a renewed Transatlantic partnership’”, available at www.consilium.europa.eu/en/press/press-releases/2021/06/15/eu-us-summit-statement-towards-a-renewed-transatlantic-partnership/.

¹⁷ See Ministry of Foreign Affairs of the People's Republic of China, “Global Initiative on Data Security”, 8 September 2020, available at www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml.

Box VII.3. United Nations work on data governance-related issues

Beyond servicing the CSTD, UNCTAD also contributes to the international debate on digital and data governance through its three pillars of work. *The Digital Economy Report* is one example in the research and analysis pillar. Regarding consensus-building, the Intergovernmental Group on E-Commerce and the Digital Economy has contributed with extensive discussions on the role of data and associated policies. Finally, technical cooperation activities have looked at data-related regulations – for example, through the UNCTAD Global Cyberlaw Tracker. Moreover, UNCTAD is part of various partnerships working on measurement of the digital economy, including in relation to data.

The *Office of the United Nations High Commissioner for Human Rights* (OHCHR) has been increasingly active in connection with respect to human rights in the digital space, as more and more human activities are taking place through the Internet. For example, the special rapporteur on the right to privacy produces multiple reports on data-related matters, such as data protection, surveillance and open data. The Office is also doing work on the role of new technologies for the realization of economic, social and cultural rights (OHCHR, 2020).

The *United Nations Commission on International Trade Law* (UNCITRAL) plays a central and coordinating role within the United Nations system addressing legal issues related to the digital economy and digital trade. Initially, the focus of its work in the field of electronic commerce was on removing legal obstacles to the use of data as a means to establish legal relations, and to satisfy legal requirements. It has shifted over time to establishing a legal environment enabling data flows, including the use of data as the foundation for the tools of trade. The Notes on the Main Issues of Cloud Computing Contracts map out contractual law issues related to the provision of cloud computing services, addressing several legal issues specific to cross-border data flows, including data localization and data privacy requirements under applicable law, as well as issues related to access and portability. In 2018, UNCITRAL embarked on a project to explore legal issues related to the digital economy. Cross-border data transactions along the “data value chain” were identified early on as a topic of interest. As a “map to guide future work”, the Commission requested the Secretariat to finalize a legal taxonomy of emerging technologies and their applications, which contains a section on data transactions (UNCITRAL, 2020). One of the overarching themes that has emerged from the exploratory work of UNCITRAL is the desirability to develop a harmonized response to legal issues related to the digital economy and digital trade.

The *United Nations Educational, Scientific and Cultural Organization* (UNESCO) prioritizes open solutions, and thus enhanced cross-border data transfer in areas such as climate change, water resources management, transboundary development, oceanographic data, education, culture and biodiversity, among others, facilitating cross-border data flows as they cut across knowledge transactions. By fostering universal access to information and knowledge available to member States, UNESCO advocates for the use of information and communications technology (ICT), open educational resources, open access to scientific information, open data and broadband-enhanced ICTs. The work of UNESCO on cross-border data is based on FAIR (findability, accessibility, interoperability and reusability) data principles, and ensures that it fully harnesses the power of data for innovative and socially beneficial applications. UNESCO has also been leading United Nations inter-agency work for recommendations on the ethics of AI, in which data play a key role (UNESCO, 2020).

The *International Telecommunication Union* (ITU) plays a fundamental role regarding technological and technical aspects of global governance of the network. It has co-led the above-mentioned work on ethics of AI with UNESCO. It has been doing work on data for good. Its Global Initiative on AI and Data Commons is a programme and collaborative platform that supports the implementation of beneficial AI based solutions to accelerate progress towards the Sustainable Development Goals. It has a digital regulation platform that covers multiple areas of governance of emerging technologies (<https://digitalregulation.org>).

United Nations Global Pulse is the Secretary-General's initiative on big data and AI for development, humanitarian action and peace. It works through a network of labs to accelerate the discovery, development and responsible use of big data and AI innovations. Its Global Data Access Framework has as its main objective to enable data-sharing across the public and private sectors in a privacy-protective manner, by helping to develop and scale AI-driven projects.

The *United Nations Group of Governmental Experts on advancing responsible State behaviour in cyberspace* (GGE) in the context of international security, and the *Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security* (OEWG) are the ones concerned with security issues.

The *United Nations Children's Fund* (UNICEF) incubated the Digital Public Goods Alliance (together with the Government of Norway), and is doing work on the governance of children's data.

The *United Nations Statistical Commission* is the highest-ranking decision-making body for international statistical activities, responsible for the setting of statistical standards and the development of concepts and methods, including their implementation at the national and international levels. It decided to create a United Nations Committee of Experts on Big Data and Data Science for Official Statistics. It also convenes the United Nations Data Forum.

Source: UNCTAD.

governance. If they are to be understood as closed groups of countries acting differently from the rest of the world, the contribution to inclusive global development objectives and to leaving no one behind may be limited. Looking for a global consensus in the context of the United Nations would be a better option, preferably with a new international coordinating body. This should take a form to be decided by member States. For example, it could be a mechanism similar to the Economic and Social Council for data-related issues.

Box VII.4. Other initiatives of relevance for global data governance

The *Internet and Jurisdiction Policy Network* is the leading multi-stakeholder organization addressing the tension between the cross-border nature of the Internet and national jurisdictions. Its secretariat facilitates a global policy process, engaging over 400 key entities from Governments, the world's largest Internet companies, technical operators, civil society groups, academia and international organizations, from over 70 countries. It has published a study framing the debate around free flow of data and data sovereignty. Through a series of consultations with stakeholders from Governments, international organizations, business, civil society, the technical community and academia, the study seeks to unpack the concepts of free flow of data and data sovereignty, and explore their implications for governance regimes. It concludes that addressing the challenges related to the governance of the growing "Datasphere" requires organizing a global multi-stakeholder debate across sectors, reframing the discussion towards more nuance and common objectives, and exploring and fostering innovative approaches in tools, frameworks and concepts (De La Chapelle and Porciuncula, 2021).

The *Digital New Deal* is a collaborative project of the Just Net Coalition and IT for Change, with contributions from academics and activists envisioning progressive ways to engage with the digital world in a post-COVID-19 landscape by reclaiming its original promise and building a digitally just world. It advocates for democratic governance and effective regulatory mechanisms across the digital domain, placing people-centred development at the core. A New Convention for Data and Cyberspace is one of the proposals included (Hill, 2020).

The *Global Data Justice project*, based at the Tilburg Institute for Law, Technology and Society in the Netherlands, focuses on the diverse debates and processes occurring around data governance in different regions, to draw out overarching principles and needs that can push data technologies' governance in the direction of social justice.

The *Global Privacy Assembly* brings together data protection and privacy authorities from local, national and international levels. It seeks to be a global forum for privacy and data protection authorities, disseminate knowledge, and provide practical assistance, to help authorities more effectively perform their mandates, provide leadership at the international level in data protection and privacy, and connect and support efforts at domestic and regional levels, and in other international forums, to enable authorities to better protect and promote privacy and data protection.

The *OECD* looks at data and cross-border data flows governance issues as part of its integrated Going Digital project. It supports the work of the G20 on the digital economy. Around a shared commitment to the OECD Recommendation on Artificial Intelligence, the Global Partnership on Artificial Intelligence brings together

engaged minds and expertise from science, industry, civil society, Governments, international organizations and academia to foster international cooperation. It includes a Working Group on Data Governance.

The *World Economic Forum* performs a number of activities on issues related to the governance of data and cross-border data flows. These include the platform *Shaping the Future of Technology Governance: Data Policy*, the *Global Future Council on Data Policy* and the *Global Technology Governance Summit 2021*, which aims to be the foremost global multi-stakeholder gathering dedicated to ensuring the responsible design and deployment of emerging technologies through public–private collaboration.

“*Solid*” (derived from “social linked data”) is a proposed set of conventions and tools for building decentralized social applications based on Linked Data principles. *Solid* is modular and extensible, and it relies as much as possible on existing W3C standards and protocols. It is a new project led by Tim Berners-Lee, inventor of the World Wide Web, taking place at MIT. The project aims to radically change the way web applications work today, resulting in true data ownership, as well as improved privacy.

Source: UNCTAD.

E. POLICY SPACE FOR DEVELOPMENT

While this Report has focused on the international policy framework for cross-border data flows, it is important to emphasize that this needs to be a complement to and coherent with national policies for making the data-driven digital economy work for development. Countries find themselves at different levels of development and readiness to engage in and benefit from the data-driven digital economy. There is no one-size-fits-all approach to regulation of cross-border data flows. Thus, international policies on this matter should include some flexibilities to ensure that developing countries have the necessary policy space for development in the data-driven digital economy; for example, they should allow developing countries to implement industrial policies to support value addition to domestic data. At the same time, they need to continue building the necessary capacities to benefit from the data-driven digital economy, as discussed in the next section.

In the context of the discussions on cross-border data flows in the trade regime, a number of developing countries have called for focusing on the enhancement of their domestic capacities in the digital economy, as well as institutional capacities to negotiate, before cross-border data flows are regulated at the international level. The need to complete the Doha Development Agenda has also been considered a priority, to be done before looking at regulating other issues, such as cross-border data flows in the WTO. While the second argument is correct, the first one may be risky. In the current context, digital technologies are rapidly evolving, and there is a need for some kind of international agreement for data to properly flow. It is likely that such an exclusive focus on development of the domestic data-driven digital economy results in something that is not adapted for a new international regime that may emerge, which may not account for the particularities of different countries. National policies or strategies for development of the data-driven digital economy are likely to fail if they do not keep the global perspective in mind; in the same way, any international regime of data governance should take into account the special circumstances of countries with different levels of readiness and capacities to benefit from data.

F. CAPACITY-BUILDING FOR DATA-DRIVEN DIGITALIZATION AND POLICYMAKING

1. Capacity-building for digitalization

Different countries find themselves at different levels of readiness to engage in and benefit from the data-driven digital economy. Most of them need to build their capacities to digitalize and process their data into digital intelligence. LDCs face particular challenges in this regard. Building capacity for digitalization will help address digital and data-related divides. This will require increased investment

in the development of connectivity and data infrastructure. The promotion of digital entrepreneurship also plays a key role. Interestingly, however, even in developed countries companies still face significant headwinds to becoming data-driven; the ninth annual survey of senior corporate executives on the topics of big data and AI business adoption, covering 85 Fortune 1,000 or industry leading firms, found: “A decade into these efforts, companies still have a long-way to go – only 39.3% are managing data as an asset; only 24.4% have forged a data culture within their firms; only 24.0% have created a data-driven organization” (NewVantage Partners, 2021:7).

Education policies should work for the enhancement of data literacy, digital skills and data talent, as there are significant shortages of these skills. As discussed in chapter III, data analytics and transformation are associated with data science and ICT professionals. In addition, analytics increasingly requires medium- and lower-skilled data work related to data extraction, selection, correction, filtering and labelling, which are essential to the effectiveness of large data-driven organizations. Moreover, it is important to pay attention to innovation and industrial policy to develop the digital economy. All these will contribute to the ability to add domestic value to data, and develop their economies.

For many small developing countries, in order to reach the necessary scale and critical mass for digitalization, capacity-building efforts may be better addressed through a regional approach. One such effort, for example, in the field of data-related skills, is the Recommended APEC Data Science and Analytics Competencies.¹⁸

2. Institutional capacity of Governments to regulate the data-driven digital economy

Existing human and institutional processes of Governments have limited capacity for establishing regulatory processes, for reasons including but not limited to (a) lack of appropriate skill sets in government to follow the scientific and technological developments emerging in this space; and (b) diverging interests and dysfunctional knowledge transfer processes between academic, public and private sector stakeholders.

Lack of appropriate skill sets in government directly results from the insufficient representation of technical and analytics communities in legislative and regulatory framework development processes, which then limits spotting both the opportunities that could be afforded by these technologies, and identifying potential risks and threats that could emerge. The design and implementation of good policy could be severely impaired if Governments lag private actors on understanding the technology properties, behaviour characteristics and emerging threats.

In terms of the diverging interests and dysfunctional knowledge transfer processes between academic and public and private sector stakeholders, data are becoming a major competitive advantage for the private sector (particularly in advanced countries and in China), and cutting-edge research is increasingly conducted with profit-driven incentives rather than consideration of the public good or individual rights. This monopoly of the private sector and the lack of appropriate incentives from the public or the academic sectors also cause the flow of top talent towards the private sector (Abban, 2020). A clear danger in the long term is increased public dependency on the profit-driven private sector, with democratic values and individual human rights significantly undermined. Less developed countries also suffer from losing their top talent to developed countries, and have less representation in setting up the global discussion – contributing further to the growing global inequality.

3. International support

While developing countries will need to allocate more domestic resources to the development of their capacities to create and capture the value of data domestically, financial, technical and other resources may fall short of meeting those needs. This is even more evident for LDCs. While the COVID-19 pandemic and its impact on government revenues have further reduced the availability of public funds, it

¹⁸ See “Big Data Analytics in Critical Demand Across APEC”, available at https://www.apec.org/press/features/2017/0620_dsa; APEC (2017); and Quismorio (2019).

has also made Governments and other stakeholders more aware of the need to improve their readiness to engage in and benefit from the evolving data-driven digital economy. This underscores the need for international support.

Ensuring that digital transformation contributes to more inclusive outcomes, and to helping achieve the Sustainable Development Goals, requires that national efforts in developing countries are better supported by the international community. Official development assistance (ODA) to bolster the development of productive capacity in the digitalization context is critical. This should include efforts to improve countries' technological capabilities, including digital capacities, and their knowledge about the workings of the data-driven digital economy.

Aid policies and decision-makers worldwide are increasingly recognizing that digitalization creates both opportunities and risks, and that there is a need for further exploring how ODA can contribute to digitalization for development. Only a small share of ODA explicitly addresses the development implications of digital transformations. UNCTAD analysis of data from the OECD suggests that the share of aid for ICT in total aid for trade rose from 1.2 per cent in 2017 to 2.7 per cent in 2019 (UNCTAD, 2021e). While the direction is positive, the share is still below the 3 per cent recorded during the period 2002–2005 (OECD and WTO, 2017).

In the context of cross-border data flows, international support could focus on a range of areas. First, it can assist developing countries in terms of formulating relevant legal and regulatory frameworks. For example, less than half of all LDCs have data protection and privacy legislation in place. Second, many countries need to formulate national strategies for dealing with data and data flows in ways that can help reap economic development gains, while at the same time respecting human rights and various security dimensions. Third, various capacity-building activities, such as training and advisory services, are needed to raise awareness of various aspects of data and data flows, and their development implications. Finally, in order to achieve inclusive outcomes of regional and global dialogues related to data governance and platform governance, developing countries need to be able to participate effectively in relevant processes and meetings. This may require additional international support, so that experts from these countries can be at the table when they take place.

G. CONCLUSIONS ON THE WAY FORWARD

As outlined above, there is a clear need for global governance of cross-border data flows that can complement measures taken at other levels of governance. The current landscape is a patchwork of national regulations based on objectives on economic development, protection of privacy, and other human rights and national security concerns. These pose challenges to the free, decentralized and open spirit of the Internet, and create obstacles for a potentially beneficial flow of data across borders. Moreover, while the challenge of regulating these flows is global in nature, there is currently no satisfactory solution at the regional or international level.

To truly work for the benefit of people and the planet, an international data governance framework should seek to enable gains from data flows to be equitably distributed within and between countries, while ensuring that risks and concerns are addressed.

A global, broad policy approach is needed to reflect the multiple and interlinked dimensions of data. It should strike a balance that properly accounts for the different interests and needs involved, in a way that supports inclusive and sustainable development. To truly work for the benefit of people and the planet, an international governance framework should seek to enable gains from data flows to be equitably distributed within and between countries, while ensuring that risks and concerns that may emerge are addressed. Achieving it will require increased policy dialogue that involves all relevant actors, and that

can help design the regulatory framework needed and the associated institutional set-up, possibly resulting in the creation of a new international body that focuses on data-related governance.

The opportunities afforded by data-driven digital technologies are all-pervasive and all-embracing; and the risks and threats are beyond the power of any single nation to address. Governments are relatively used to dealing with new disruptive technologies that cause major process changes in the economy and society, but the data-related disruption goes beyond this, and further introduces existential questions around human cognitive capacity and control, social organization and construction, democratic values and individual rights.

The COVID-19 pandemic has taught the world important lessons in relation to policy–data interactions and the potential role that data can play in fighting global crises. Never have people’s lives been so dependent on real-time data and technology assistance – from monitoring and controlling the spread of the pandemic, to the way we carry out our daily activities (working, shopping, socializing, receiving education, etc.), and to the way scientists developed new vaccines in record time. Crises like this do not obey the national boundaries and borders established, and hence the solutions require cross-border data flows and technology collaborations at a similar scale. The same applies to other major global issues and dynamic societal threats – such as climate change, sustainable development, racial bias and gender-based inequalities, digital inequalities and international security concerns. National interests, along with the existential interests of human beings and the planet, are best served with international collaboration to develop and regulate cross-border data flows.

This Report provides some orientation on the way forward, but does not seek to offer solutions. In the unknown territory of the rapidly evolving data-driven digital economy, many questions remain open. The answers must be found through a global, multidisciplinary and multi-stakeholder policy debate. There is a need to reframe and broaden the international policy debate on this matter, to take into account economic as well as non-economic dimensions of data. The increased interconnection and interdependence challenges in the global data economy require a move away from the silo approach towards a holistic coordinated global approach. This may need to involve innovative ways of global governance, as the old ones may not be well suited to respond to the new context.

There is a need to reframe and broaden the international policy debate on cross-border data flows, to take into account economic as well as non-economic dimensions of data.

The challenges are extremely complex and multidimensional – hence requiring new engagement models between multiple disciplinary traditions and different stakeholders across public and private sectors, as well as individual citizens. Potential solutions should both respect basic universal human rights and be flexible enough to reflect local interests and cultures. Governance will also need to be flexible in time and agile, considering the rapid developments in digital technologies and the technological context; challenges that need to be addressed today may be different to those emerging in a few years. Since many of the challenges are global, global solutions are needed. International or regional rules need to take into account the necessary policy space for capacity-building and development. And when building their digital economies and institutions, as well as when designing their development policies, developing countries should not lose sight of the international dimension of data and their regulation, which have an influence on domestic economic development.

Nevertheless, achieving common ground and global solutions will not be easy. Indeed, in this age of populism, anti-globalization and competing vested interests, associated with the capture of rents from the use of digital technologies and data, it may seem not only surprising, but self-defeating, to propose a new international body. Yet all of these factors make it more essential than ever to embark on a new path for digital, including data, governance. A reinforcement of the data realms or a splintering into multiple spheres would make a chaotic situation even more confusing, and would substantially diminish

the value that can accrue from these technologies, in addition to creating the space for substantial harms related to privacy, cybersecurity and other risks.

In order to ensure the full involvement of all countries of the world in shaping the ways in which data flows are governed at the global level, the United Nations will need to play a central role. Already a large number of United Nations entities are engaged in relevant work – concerning all the dimensions of data – many with their base outside the United Nations headquarters: in Geneva (such as ITU, UNCTAD, OHCHR, the World Health Organization, the World Intellectual Property Organization and WTO); Paris (UNESCO); and Vienna (such as the United Nations Office on Drugs and Crime and UNCITRAL).¹⁹ But for the United Nations to be able to fulfil its role in this context, it will need to ensure effective links to other ongoing processes and initiatives led by civil society, academia and the private sector.

To ensure the full involvement of all countries in shaping the ways in which data flows are governed at the global level, the United Nations will need to play a central role.

¹⁹ For a detailed description of international organization landscape in Geneva, see the Geneva Digital Atlas, available at <https://dig.watch/actors/geneva>.

REFERENCES

- Aaronson SA (2014). Why the US and EU are failing to set information free. VoxEU.org, 14 July. Available at: <https://voxeu.org/article/why-us-and-eu-are-failing-set-information-free>.
- Aaronson SA (2015). Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. *World Trade Review*, 14(4): 671–700.
- Aaronson SA (2019a). Data Is Different, and That's Why the World Needs a New Approach to Governing Cross-Border Data Flows. *Digital Policy, Regulation and Governance*, 21(5): 441–460.
- Aaronson SA (2019b). What are we talking about when we talk about digital protectionism? *World Trade Review*, 18(4): 541–577.
- Aaronson SA and Leblond P (2018). Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. *Journal of International Economic Law*, 21(2).
- Aaronson SA and Maxim R (2013). Data Protection and Digital Trade in the Wake of the NSA Revelations. *Intereconomics*, 48(5): 281–286.
- Abass A (2017). Historical and political background to the Malabo protocol. In: Werle G and Vormbaum M, eds., *The African Criminal Court*, TMC Asser Press, The Hague: 11–28.
- Abban D (2020). The Battle for AI Talent, 4 June. Available at: <https://becominghuman.ai/the-battle-for-ai-talent-e938f4082f94>.
- Abbott FM (2009). Cross-Retaliation in TRIPS: Options for Developing Countries. Issue Paper 8. ICTSD Programme on Dispute Settlement and Legal Aspects of International Trade, International Centre for Trade and Sustainable Development, Geneva.
- Abramova A and Thorne E (2021). Digital Economy Developments Within the EAEU. In: Piskulova NA, ed., *The Economic Dimension of Eurasian Integration*, Palgrave Macmillan: 161–174.
- Access Now (2021). *Shattered dreams and lost opportunities – a year in the fight to #KeepItOn*. The #KeepItOn report on Internet shutdowns 2020, March. Available at: <https://www.accessnow.org/keepiton-report-a-year-in-the-fight/>.
- Ademuyiwa I and Adeniran A (2020). Assessing Digitalization and Data Governance Issues in Africa. CIGI Papers No. 244, Centre for International Governance Innovation, Waterloo, ON.
- African Union (2014). African Union Convention on Cyber Security and Personal Data Protection. African Union, Addis Ababa. Available at: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.
- African Union (2020). The Digital Transformation Strategy for Africa 2020–2030. African Union, Addis Ababa, Ethiopia. Available at: <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>.
- Aguerre C (2019). Digital Trade in Latin America: Mapping Issues and Approaches. *Digital Policy, Regulation and Governance*, 21(1): 2–18.
- Ahmed N and Wahed M (2020). The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research. arXiv:2010.15581, Cornell University, Ithaca, NY, 22 October. Available at: <https://arxiv.org/abs/2010.15581>.
- Aktoudianakis A (2020). Fostering Europe's Strategic Autonomy – Digital sovereignty for growth, rules and cooperation. European Policy Centre and Konrad-Adenauer-Stiftung, 18 December.
- Anwar MA and Graham M (2020). Digital Labour at Economic Margins: African Workers and the Global Information Economy. *Review of African Political Economy*, 47(163): 95–105.
- APEC (2017). Recommended APEC Data Science and Analytics (DSA) Competencies. Asia-Pacific Economic Cooperation, Singapore. Available at: https://apru.org/wp-content/uploads/2019/04/Recommended_APEC_DSA_Competencies_Endorsed-8.pdf.
- Arcesati R (2020). The Digital Silk Road is a development issue. Mercator Institute for China Studies, Berlin. 28 April. Available at: <https://merics.org/en/short-analysis/digital-silk-road-development-issue>.
- Arnold Z, Rahkovsky I and Huang T (2020). Tracking AI Investment. Initial Findings from the Private Markets. Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service,

- Washington, DC, September. Available at: <https://cset.georgetown.edu/wp-content/uploads/CSET-Tracking-AI-Investment.pdf>.
- Arrockia P, Varnekha S and Veneshia K (2017). The 17 V's Of Big Data. *International Research Journal of Engineering and Technology*, 4(9).
- Arora P (2016). Bottom of the Data Pyramid: Big Data and the Global South. *International Journal of Communication*, 10: 1681–1699.
- Arora P (2019). *The Next Billion Users. Digital Life Beyond the West*. Harvard University Press, Cambridge, MA.
- Arrieta-Ibarra I et al. (2018). Should We Treat Data as Labor? Moving beyond “Free”, *American Economic Association Papers and Proceedings*, 108: 38–42.
- Avila R (2018). Digital Sovereignty or Digital Colonialism? *Sur International Journal on Human Rights*, 15(27): 15–27.
- Avila R (2020). Against Data Colonialism. In: Muldoon J and Stronge W, eds., *Platforming Equality: Policy Challenges for the Digital Economy*, Autonomy Research Ltd, Crookham Village, September: 47–57.
- Aydin A and Bensghir TK (2019). Digital Data Sovereignty: Towards a Conceptual Framework. 2019 1st International Informatics and Software Engineering Conference (UBMYK): 1–6. Available at: <https://ieeexplore.ieee.org/document/8965469>.
- Azmeh S and Foster C (2016). The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements. *LSE Working Paper Series* 2016, No. 16–175, London School of Economics and Political Science, London.
- Azmeh S and Foster C (2018). Bridging the Digital Divide and Supporting Increased Digital Trade: Country Case Studies. Discussion Paper, GEGAfrica, Global Economic Governance, Pretoria. Available at: <http://www.gegafrika.org/item/862-bridging-the-digital-divide-and-supporting-increased-digital-trade-country-case-studies>.
- Azmeh S, Foster C and Abd Rabuh A (2021). The Rise of the Data Economy and Policy Strategies for Digital Development. *Digital Pathways at Oxford Paper Series*, No. 10. Oxford, United Kingdom.
- Azmeh S, Foster C and Echavarrri J (2020). The International Trade Regime and the Quest for Free Digital Trade. *International Studies Review*, 22(3): 671–692.
- Back D, Kalenzi C and Yim M (2021). Digital contact tracing apps help slow COVID-19. Here's how to increase trust. Available at <https://www.weforum.org/agenda/2021/05/could-the-governance-required-for-contact-tracing-apps-already-exist/>.
- Badran MF (2018). Economic Impact of Data Localization in Five Selected African Countries. *Digital Policy, Regulation and Governance*, 20(4): 337–357.
- Bagchi K and Kapilavai S (2018). Political Economy of Data Nationalism. 22nd Biennial Conference of the International Telecommunications Society (ITS): “Beyond the Boundaries: Challenges for Business, Policy and Society”, Seoul, 24–27 June. Available at: <http://hdl.handle.net/10419/190347>.
- Barnes J, Black A, Roberts S, Andreoni A, Mondliwa P and Sturgeon T (2019). Towards a Digital Industrial Policy for South Africa: A Review of the Issues. The Industrial Development Think Tank, Johannesburg. Available at: <http://www.thedtic.gov.za/wp-content/uploads/DPIP.pdf>.
- Bauer M, Erixon F, Krol M and Lee-Makiyama H (2013). The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce. European Centre for International Political Economy, Brussels. Available at: https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_Ir.pdf.
- Bauer M, Ferracane MF and van der Marel E (2016). Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization. GCIG (Global Commission on Internet Governance) Paper Series No. 30. Centre for International Governance Innovation, Waterloo, ON and Chatham House, London.
- Bauer M, Lee-Makiyama H, van der Marel E and Verschelde B (2014). The Costs of Data Localisation: Friendly Fire on Economic Recovery. ECIPE Occasional paper, No. 3, European Centre for International Political Economy, Brussels.
- BDI (2017). Grenzüberschreitende Datenflüsse und EU-Handelsabkommen. Positionspapier, Bundesverband der Deutschen Industrie e.V. (BDI) – The Voice of German Industry, Berlin, 27 June. Available at: <https://bdi.eu/publikation/news/grenzueberschreitende-datenfluesse-und-eu-handelsabkommen/>.

- Bennett CJ and Raab CD (2020). Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective. *Regulation and Governance*, 14(3): 447–464.
- Birch K, Chiappetta M and Artyushina A (2020). The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset. *Policy Studies*, 41(5): 468–487.
- Bird and Bird (2017). Guide to the General Data Protection Regulation. Bird and Bird, London.
- Bleeker A (2020). Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: A review of data protection legislation for alignment with the General Data Protection Regulation. *Studies and Perspectives series - ECLAC Subregional Headquarters for the Caribbean*, No. 94, (LC/TS.2020/126-LC/CAR/TS.2020/4), Economic Commission of Latin America and the Caribbean (ECLAC), Santiago.
- Bradford A (2020). The Brussels Effect Comes for Big Tech. Project Syndicate, 17 December. Available at: <https://www.project-syndicate.org/commentary/eu-digital-services-and-markets-regulations-on-big-tech-by-anu-bradford-2020-12>.
- Brathwaite C and Remy JY (2020). E-commerce-related policies, initiatives & legislation across CARICOM: Diagnostic Review 2020. The Shridath Ramphal Centre for International Trade Law, Policy and Services, Barbados.
- Brehmer HJ (2018). Data Localization: The Unintended Consequences of Privacy Litigation. *American University Law Review*, 67(3): 927–969.
- Bria F (2020). Digital Sovereignty for the People in the post-pandemic World. Medium, 24 August. Available at: <https://medium.com/@francescabria/digital-sovereignty-for-the-people-in-the-post-pandemic-world-109472dd736b>.
- BSA (2012). Lockout: How a New Wave of Trade Protectionism Is Spreading through the World's Fastest-Growing IT Markets – and What to Do about it. Business Software Alliance, Washington, DC. Available at: <https://www.bsa.org/files/reports/BSALockout2012.pdf>.
- BSA (2017). Cross-border Data Flows. Business Software Alliance, Washington, DC. Available at: <https://www.bsa.org/policy-filings/cross-border-data-flows>.
- Budnitsky S and Jia L (2018). Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance. *European Journal of Cultural Studies*, 21(5): 594–613.
- Bughin J and Lund S (2017). The ascendancy of international data flows. VoxEU.org, 9 January. Available at: <https://voxeu.org/article/ascendancy-international-data-flows>.
- Burman A (2020). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? Working Paper, Carnegie India, New Delhi, March.
- Burri M (2016). The World Trade Organization as an Actor in Global Internet Governance. SSRN Paper No. ID 2792219, Social Science Research Network, Rochester, NY. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792219.
- Burri M (2017). The Regulation of Data Flows Through Trade Agreements. *Georgetown Journal of International Law*, 48(1): 407–448.
- Bygrave LA (2002). *Data Protection Law: Approaching its Rationale, Logic and Limits*. Kluwer Law International, The Hague, London and New York.
- Carter WA and Yayboke E (2019). Data Governance Principles for the Global Digital Economy. Center for Strategic & International Studies, Washington, DC, 4 June. Available at: <https://www.csis.org/analysis/data-governance-principles-global-digital-economy>.
- Casalini F and López González J (2019). Trade and Cross-Border Data Flows. *OECD Trade Policy Paper*, No. 220, OECD Publishing, Paris.
- Casalini F, López González J and Nemoto T (2021). Mapping commonalities in regulatory approaches to cross-border data transfers. *OECD Trade Policy Paper*, No. 248, OECD Publishing, Paris. Available at: <https://doi.org/10.1787/ca9f974e-en>.
- Casella B and Formenti L (2018). FDI in the Digital Economy: A Shift to Asset-Light International Footprints. *Transnational Corporations*, 25(1): 101–130.
- Castro D and McLaughlin M (2021). Who is winning the AI race? China, the EU, or the United States? 2021 Update. Center for Data Innovation, Washington, DC, January. Available at: <https://www2.datainnovation.org/2021-china-eu-us-ai.pdf>.

- Castro D and McQuinn A (2015). Cross-border data flows enable growth in all industries. Information Technology and Innovation Foundation, Washington, DC. Available at: http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=2.142131440.350197758.1621849794-1974323496.1621849794.
- Cattaruzza A (2019). *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data*. Le Cavalier Bleu, Paris.
- CBInsights (2021). Expert Collection database: Cybersecurity. Investment in cybersecurity companies. Period: 01 January 2016 – 28 January 2021, CBInsights. Dataset downloaded on 28 January 2021. Available at: <https://www.cbinsights.com> (document extracted on 28 January 2021).
- Center for Responsive Politics (2021). Lobbying spending nears record high in 2020 amid pandemic. Center for Responsive Politics, Washington, DC, 27 January. Available at: <https://www.opensecrets.org/news/2021/01/lobbying-spending-nears-record-high-in-2020-amid-pandemic/>.
- CFR (2020). Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms? Council on Foreign Relations, New York, NY. Available at: <https://www.cfr.org/china-digital-silk-road/>.
- Chakravorti B (2018). Why the Rest of the World Can't Free Ride on Europe's GDPR Rules. *Harvard Business Review*, 30 April. Available at: <https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules>.
- Chander A (2020). Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*, Oxford University Press, 23(3): 771–84.
- Chander A and Ferracane M (2019). Regulating Cross-border Data Flows – Domestic Good Practices. In: Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence, White Paper, World Economic Forum, Geneva, December: 7–17. Available at: http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.
- Chander A and Lê UP (2014). Breaking the Web: Data Localization vs. the Global Internet. UC Davis Legal Studies Research Paper, No. 378, University of California, Davis.
- Chander A and Lê UP (2015). Data nationalism. *Emory Law Journal*, 64(3):677–739.
- Chen L, Cheng W, Ciuriak D, Kimura F, Nakagawa J, Pomfret R, Rigoni G and Schwarzer J (2019). The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies. T20 Japan Task Force 8: Trade, Investment and Globalization. Available at: <https://t20japan.org/policy-brief-digital-economy-economic-development/>.
- Chetty M, Sundaresan S, Muckaden S, Feamster N and Calandro E (2013). Measuring Broadband Performance in South Africa. In: Proceedings of the 4th Annual Symposium on Computing for Development (ACM DEV-4 '13). Association for Computing Machinery, New York, NY, Article 1, 1–10. Available at: <http://dl.acm.org/citation.cfm?doid=2537052.2537053>.
- Chin C (2018). AI Is the Future—But Where Are the Women? Available at www.wired.com/story/artificial-intelligence-researchers-gender-imbalance/.
- Christakis T (2020). “European Digital Sovereignty”: Successfully Navigating Between the “Brussels Effect” and Europe's Quest for Strategic Autonomy. Multidisciplinary Institute on Artificial Intelligence and Grenoble Alpes Data Institute, December. Available at: <https://ssrn.com/abstract=3748098>.
- Cisco (2018). Cisco Visual Networking Index: Forecast and Trends, 2017–2022. White paper, Cisco. Available at: <https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf>.
- Cisco (2020). Cisco Annual Internet Report (2018-2023). White Paper, Cisco. Available at: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf>.
- Ciuriak D (2018). Rethinking Industrial Policy for the Data-driven Economy. CIGI Papers, No. 192, Centre for International Governance Innovation, Waterloo, ON.
- Ciuriak D (2019). On the Cusp of Change: Trade and Development in the Age of Data. Presentation at the Egyptian Center for Economic Studies, 23 December. Available at: <https://www.youtube.com/watch?v=vC7Qu2zs-KM>.
- Ciuriak D (2020). Economic Rents and the Contours of Conflict in the Data-driven Economy. CIGI Paper, No. 245, Centre for International Governance Innovation, Waterloo, ON.
- Ciuriak D and Ptashkina M (2018). The Digital Transformation and the Transformation of International Trade. RTA Exchange Issues Paper, Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB). Available at: <https://e15initiative.org/publications/the-digital-transformation-and-the-transformation-of-international-trade/>.

- Clarke R (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, 34(1): 59–80.
- Clinton HR (2010). Remarks on Internet Freedom. United States Department of State, Washington, DC, 21 January. Available at: <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>.
- CNNUM (2014). Strengthening EU's Negotiation Strategy to Make TTIP a Sustainable Blueprint for the Digital Economy and Society: Opinion of the French Digital Council. Conseil National du Numérique (French Digital Council), Paris, April. Available at: <https://cnnumerique.fr/files/uploads/2014/05/Version-web-ANGLAIS-19.05.pdf>.
- Cofone I (2020). Beyond Data Ownership. *ardoza Law Review* (2021, forthcoming). Available at: <https://ssrn.com/abstract=3564480>.
- Correa CM (2020). Data in Legal Limbo: Ownership, Sovereignty, or a Digital Public Goods Regime? Research Paper, No. 117, South Centre, Geneva.
- Cory N (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation, Washington, DC, 1 May. Available at: <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>.
- Cory N (2019). The False Appeal of Data Nationalism: Why the Value of Data Comes from How It's Used, Not Where It's Stored. Information Technology and Innovation Foundation, Washington, DC, 1 April. Available at: <https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where>.
- Cory N (2020). Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers. Information Technology and Innovation Foundation, Washington, DC, 27 January. Available at: <https://itif.org/publications/2020/01/27/surveying-damage-why-we-must-accurately-measure-cross-border-data-flows-and>.
- Cory N and Castro D (2018). Crafting an Open and Innovative Digital Trade Agenda for Latin America. Information Technology and Innovation Foundation, Washington, DC, 26 November. Available at: <https://itif.org/publications/2018/11/26/crafting-open-and-innovative-digital-trade-agenda-latin-america>.
- Couldry N and Mejjas AU (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, 20(4): 336–349.
- Couldry N and Mejjas AU (2021). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It For Capitalism*. Stanford University Press, Stanford, CA.
- Couture S (2020). The Diverse Meanings of Digital Sovereignty. Global Media Technologies & Cultures Lab, Massachusetts Institute of Technology, Cambridge, MA, 5 August. Available at: <https://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/>.
- Couture S and Toupin S (2019). What Does the Notion of “Sovereignty” Mean When Referring to the Digital? *New Media and Society*, 21(10): 2305–2322.
- Coyer K and Higgott R (2020). Sovereignty in a Digital Era: A Report Commissioned by The Dialogue of Civilizations Research Institute Berlin. Dialogue of Civilizations Research Institute, Berlin. Available at: https://doc-research.org/wp-content/uploads/2020/09/Sovereignty-in-a-digital-era____.pdf.
- Coyle D, Diepeveen S, Wdowin J, Kay L and Tennison J (2020). The value of data – Policy implications. The Bennett Institute for Public Policy, Cambridge and the Open Data Institute. Available at: <https://www.bennettinstitute.cam.ac.uk/publications/value-data-policy-implications/>.
- Coyle D and Li W (2021). The Data Economy: Market Size and Global Trade. Presentation at the Allied Social Science Associations (ASSA) Annual Meeting, 3 January, session on Big Data: Competition, Innovation, and Policy. Available at: https://www.aeaweb.org/conference/2021/preliminary/1993?q=eNqrVipOLS7OzM8LqSxIVbKqhnGVrJQMIXSUUstS80qAbCOIWh2IxOLi_GQgx9QYKFOSWpQLZANZKYmVEEZJZm4qhFWWmVoOMqyooFwwZJABCCjV1gJcMD7VH74.
- Coyle D and Nguyen D (2019). Cloud Computing, Cross-Border Data Flows and New Challenges for Measurement in Economics. *National Institute Economic Review*, 249(1): R30–R38.
- Creemers R (2020). China's Approach to Cyber Sovereignty. Konrad-Adenauer-Stiftung, Berlin.
- CRS (2020a). Internet Regimes and WTO E-Commerce Negotiations. CRS Report, R46198, Congressional Research Service, Washington, DC, 28 January.
- CRS (2020b). Digital Trade. In: Focus IF10770, Congressional Research Service, Washington, DC, 3 December.

- CSET (2020). Tracking AI Investment. Initial Findings from the Private Markets. Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service, Washington, DC, September. Available at: <https://cset.georgetown.edu/wp-content/uploads/CSET-Tracking-AI-Investment.pdf>.
- Daskal J (2017). Congress Needs to Fix Our Outdated Email Privacy Law. *Slate*, 26 January. Available at <https://slate.com/technology/2017/01/the-confusing-court-case-over-microsoft-data-on-servers-in-ireland.html>.
- David-West O and Evans PC (2016). The Rise of African Platforms: A Regional Survey. The Emerging Platform Economy Series, No. 2, Center for Global Enterprise (CGE), New York, NY. Available at: https://www.researchgate.net/publication/306401003_The_Rise_of_African_Platforms_A_Regional_Survey.
- Daza Jaller L, Gaillard S and Molinuevo M (2020). The Regulation of Digital Trade: Key Policies and International Trends. World Bank, Washington, DC.
- De La Chapelle B and Porciuncula L (2021). We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty. Internet & Jurisdiction Policy Network (I&JPN), Paris. Available at: <https://www.internetjurisdiction.net/news/aboutdata-report>.
- De Nardis L (2016). Introduction: One Internet: an evidentiary basis for policy making on Internet universality and fragmentation. In *A Universal Internet in a Bordered World. Research on Fragmentation, Openness and Interoperability*. Vol. I. Global Commission on Internet Governance and Chatham House, Ottawa.
- Deardorff AV (2017). Comparative Advantage in Digital Trade. In: Evenett SJ, ed. *Cloth for Wine? The Relevance of Ricardo's Comparative Advantage in the 21st Century*. CEPR Press, London: 35–44.
- Dekker B, Okano-Heijmans M and Zhang ES (2020). Unpacking China's Digital Silk Road. Clingendael Report. Clingendael Institute, The Hague. Available at: https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf.
- Digital Future Society (2019). Toward better data governance for all: Data ethics and privacy in the digital era. Digital Future Society, Barcelona, July. Available at: https://digitalfuturesociety.com/app/uploads/2019/08/060819_Toward_better_data_governance_for_all_dfs_mwcapital_DIGITAL.pdf.
- DigitalEurope, BusinessEurope, ERT and ACEA (2020). Schrems II: Impact Survey Report. DigitalEurope, Brussels, 26 November. Available at: https://www.buinessurope.eu/sites/buseur/files/media/reports_and_studies/2020-11-26_schrems_ii_impact_survey_report.pdf.
- Donovan KP and Park E (2019). Perpetual Debt in the Silicon Savannah. *Boston Review*, 20 September. Available at: <http://bostonreview.net/class-inequality-global-justice/kevin-p-donovan-emma-park-perpetual-debt-silicon-savannah>.
- Drake WJ, Cerf VG and Kleinwächter W (2016). Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper, World Economic Forum, Geneva, January. Available at: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.
- Duch-Brown N, Martens B and Mueller-Langer F (2017). The Economics of Ownership, Access and Trade in Digital Data. Digital Economy Working Paper, 2017–01, Joint Research Centre (JRC) Technical Reports, European Commission and JRC, Seville. Available at: <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf>.
- Ebert I, Busch T and Wettstein F (2020). Business and Human Rights in the Data Economy: A Mapping and Research Study. German Institute for Human Rights, Berlin. Available at: https://www.institut-fuer-menschenrechte.de/fileadmin/user_upload/Publikationen/ANALYSE/Analysis_Business_and_Human_Rights_in_the_Data_Economy.pdf.
- ECLAC (2020). Digital Agenda for Latin America and the Caribbean (eLAC2022). LC/CMSI.7/4. Seventh Ministerial Conference on the Information Society in Latin America and the Caribbean, 23–26 November 2020, Economic Commission for Latin America and the Caribbean, Santiago. Available at: https://conferenciaelac.cepal.org/7/sites/elac2020-2/files/20-00902_cmsi.7_digital_agenda_elac2022.pdf.
- ECLAC (2021). Datos y hechos sobre la transformación digital. Project Documents. LC/TS.2021/20. Economic Commission for Latin America and the Caribbean, Santiago.
- ECLAC and I&JPN (2020). *Internet & Jurisdiction and ECLAC Regional Status Report 2020*. LC/TS.2020/141. Economic Commission for Latin America and the Caribbean and Internet & Jurisdiction Policy Network, Santiago. Available at: https://www.cepal.org/sites/default/files/publication/files/46421/S1901092_en.pdf.
- Eder TS, Arcesati R and Mardell J (2020). Networking the “Belt and Road” – The future is digital. Mercator Institute for China Studies, Berlin. Available at: <https://merics.org/en/tracker/networking-belt-and-road-future-digital>.

- EDRI (2015). Data protection and privacy must be excluded from TTIP. European Digital Rights, Brussels, 8 April. Available at: <https://edri.org/our-work/data-protection-privacy-ttip/>.
- Eferin Y, Hohlov Y and Rossotto C (2019). Digital platforms in Russia: Competition between National and Foreign Multi-sided Platforms Stimulates Growth and Innovation. *Digital Policy, Regulation and Governance*, 21(2): 129–45.
- Elmi N (2020). Is Big Tech Setting Africa Back? *Foreign Policy*, 11 November. Available at: <https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/>.
- Engels B (2019). Data Governance as the Enabler of the Data Economy. *Intereconomics*, 54(4): 216–222.
- Epifanova A (2020). Deciphering Russia's "Sovereign Internet Law". DGAP Analysis, No. 2, German Council on Foreign Relations, Berlin, January. Available at: <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>.
- Equinix (2020). Hyperscale vs. Colocation. Equinix, 27 August. Available at: <https://blog.equinix.com/blog/2020/08/27/hyperscale-vs-colocation/>.
- Ericsson (2020). *Ericsson Mobility Report, November 2020*. Telefonaktiebolaget LM Ericsson, Stockholm, November. Available at: <https://www.ericsson.com/en/mobility-report/reports/november-2020>.
- Erie MS and Streinz T (2021). The Beijing effect: China's "Digital Silk Road" as Transnational Data Governance. *New York University Journal of International Law and Politics* (forthcoming). Available at: <https://cld.web.ox.ac.uk/article/beijing-effect-chinas-digital-silk-road-transnational-data-governance>.
- European Commission (2019). Questions and Answers on the Japan adequacy decision. MEMO/19/422. European Commission, Brussels, 23 January. Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_422.
- European Commission (2020a). *The European Data Market Monitoring Tool: Key Facts and Figures, First Policy Conclusions, Data Landscape and Quantified stories, D2.9 Final Study Report*. European Commission, Brussels. Available at: <https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update>.
- European Commission (2020b). Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing. European Commission, Brussels. Available at: <https://digital-strategy.ec.europa.eu/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more>.
- European Commission (2021). Trade Policy Review – An Open, Sustainable and Assertive Trade Policy. COM/2021/66 final. European Commission, Brussels, 18 February. Available at: https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159438.pdf.
- European Data Protection Board (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted 10 November 2020). European Data Protection Board, Brussels. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
- European Parliament (2020). Digital sovereignty for Europe. European Parliamentary Research Service Ideas Paper Briefing, European Parliament, Brussels. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).
- Evans PC (2016). The Rise of Asian Platforms: A Regional Survey. The Emerging Platform Economy Series, No. 3, Center for Global Enterprise (CGE), New York, NY. Available at: <https://www.thecge.net/app/uploads/2016/11/FINALAsianPlatformPaper.pdf>.
- Fanou R, Francois P, Aben E, Mwangi E, Goburdhan N and Valera F (2017). Four Years Tracking Unrevealed Topological Changes in the African Interdomain. *Computer Communications*, 106: 117–135.
- Farrell H and Newman AL (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 44(1): 42–79.
- Fay R (2019). Digital Platforms Require a Global Governance Framework. A CIGI essay series on Models for Platform Governance, Centre for International Governance Innovation, Waterloo, ON, 28 October. Available at: <https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework>.
- Fay R (2020). CUSMA's Data and Intellectual Property Commitments Could Inhibit Domestic Policy Flexibility. Presentation on 26 February 2020 at the Standing Committee on International Trade, the Canadian Parliament. Centre for International Governance Innovation, Waterloo, ON. Available at: <https://www.cigionline.org/articles/cusmas-data-and-intellectual-property-commitments-could-inhibit-domestic-policy>.

- Fay R (2021). A Model for Global Governance of Platforms. In Moore M and Tambini D, eds., *Regulating Big Tech: Policy Responses to Digital Dominance* (forthcoming), New York: Oxford University Press.
- Feijóo C, Kwon Y, Bauer JM, Bohlin E, Howell B, Jain R, Potgieter P, Vu K, Whalley J and Xia J (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, 44(6): 101988.
- Feldstein S (2019). The Global Expansion of AI Surveillance. Working Paper, Carnegie Endowment for International Peace, Washington, DC, September.
- Ferracane MF, Kren J and van der Marel E (2020). Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries? *Review of International Economics*, 28(3): 676–722.
- Ferracane MF and van der Marel E (2020). Digital Innovation in East Asia: Do Restrictive Data Policies Matter? Policy Research Working Paper, No. 9124. World Bank, Washington, DC.
- Floridi L (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology*, 33(3): 369–378.
- Flyverbom M, Madsen AK and Rasche A (2017). Big Data as Governmentality in International Development: Digital Traces, Algorithms, and Altered Visibilities. *The Information Society*, 33(1): 35–42.
- Fogh Rasmussen A (2021). Building a Democratic High-Tech Alliance. Project Syndicate, 29 March. Available at: <https://www.project-syndicate.org/commentary/democratic-technology-alliance-global-digital-rules-by-anders-fogh-rasmussen-2021-03>.
- Fortune Business Insights (2021). Internet of Things (IoT) Market Size, Share & COVID-19 Impact Analysis, By Component (Platform, Solution & Services), By End Use Industry (BFSI, Retail, Government, Healthcare, Manufacturing, Agriculture, Sustainable Energy, Transportation, IT & Telecom, Others), and Regional Forecast, 2021–2028. Report ID: FBI100307, 21 May. Available at: <https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307>.
- Foster C (2020). Digital trade in the Kenya-US FTA? The Digital Trade Tracker, 28 September. Available at: <https://digitaltradetracker.org/2020/09/28/digital-trade-in-the-kenya-us-fta/>.
- Foster C and Azmeh S (2020). Latecomer Economies and National Digital Policy: An Industrial Policy Perspective. *Journal of Development Studies*, 56(7): 1247–1262.
- Foster C, Graham M, Mann L, Waema T and Friederici N (2018). Digital Control in Value Chains: Challenges of Connectivity for East African Firms. *Economic Geography*, 94(1): 68–86. Available at: <https://doi.org/10.1080/00130095.2017.1350104>.
- Freedom House (2020). User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization. Freedom House, Washington, DC. Available at: <https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty>.
- Gagné JF, Hudson S and Mantha Y (2020). Global AI Talent Report 2020. Blog of JF Gagné. Available at: <https://jfgagne.ai/global-ai-talent-report-2020/>.
- Gagné JF, Kiser G and Mantha Y (2019). Global AI Talent Report 2019. Blog of JF Gagné. Available at: <https://jfgagne.ai/talent-2019/>.
- Gagnon-Turcotte S, Sculthorp M and Coutts S (2021). Digital data partnerships: building the foundations for collaborative data governance in the public interest. Open North, Montreal. Available at: https://assets.ctfassets.net/e4wa7sgik5wa/6mV2HLHbhKbU2sgtXSTMQX/da0ede46238b1809d60b5ba65732fb2b/Digital_Data_Partnerships_Report-EN.pdf.
- Gao HS (2019). Data Regulation with Chinese Characteristics. SMU Centre for AI & Data Governance Research Paper, No. 2019/04. Singapore Management University (SMU), Singapore.
- Gartner (2019). The Data Center is (Almost) Dead. Gartner, 5 August. Available at: <https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead/>.
- Gawer A (2014). Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework. *Research Policy*, 43(7): 1239–1249.
- Geist M (2018). Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. A CIGI Essay Series on Data Governance in the Digital Age, Centre for International Governance Innovation, Waterloo, ON, 4 April. Available at: <https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/>.
- Gheyle N and De Ville F (2017). How Much is Enough? Explaining the Continuous Transparency Conflict in TTIP. *Politics and Governance*, 5(3): 16–28.

- Girard M (2019). Standards for the Digital Economy: Creating an Architecture for Data Collection, Access and Analytics. CIGI Policy Brief, No. 155, Centre for International Governance Innovation, Waterloo, ON, 4 September. Available at: <https://www.cigionline.org/publications/standards-digital-economy-creating-architecture-data-collection-access-and-analytics/>.
- Girard M (2020). Standards for Digital Cooperation. CIGI Papers, No. 237, Centre for International Governance Innovation, Waterloo, ON,. Available at: <https://www.cigionline.org/publications/standards-digital-cooperation/>.
- Global Data Alliance (2020). Cross-Border Data Transfers and Data Localization. Global Data Alliance, Washington, DC. Available at: <https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf>.
- Gökçe Dessemond E (2020). Restoring competition in “winner-took-all” digital platform markets. UNCTAD Research Paper, No. 40. UNCTAD/SER.RP/2019/12. UNCTAD, Geneva.
- Gong S, Gu J and Teng F (2019). The Impact of the Belt and Road Initiative Investment in Digital Connectivity and Information and Communication Technologies on Achieving the SDGs. K4D Emerging Issues Report. Institute of Development Studies, Brighton. Available at: https://assets.publishing.service.gov.uk/media/5c86628940f0b6369b76a372/K4D_Emerging_Issues_-_BRI_Investment_Part_A_-_final.pdf.
- Gonzalez-Zapata F and Heeks R (2015). The Multiple Meanings of Open Government Data: Understanding Different Stakeholders and Their Perspectives. *Government Information Quarterly*, 32(4): 441–452.
- Google (2010). Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information. White paper. Google, Mountain View, CA. Available at: https://static.googleusercontent.com/media/www.google.com/fr//googleblogs/pdfs/trade_free_flow_of_information.pdf.
- Government Office for Science (2020). Evidence and Scenarios for Global Data Systems. The Future of Citizen Data Systems. Government of the United Kingdom of Great Britain and Northern Ireland. Available at: <https://www.gov.uk/government/publications/the-future-of-citizen-data-systems>.
- Graham M, Hjorth I and Lehdonvirta V (2017). Digital Labour and Development: Impacts of Global Digital Labour Platforms and the Gig Economy on Worker Livelihoods. *Transfer: European Review of Labour and Research*, 23(2): 135–162.
- Gray ML and Suri S (2019). *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. Houghton Mifflin Harcourt, Boston, MA.
- Greze B (2019). The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives. *International Data Privacy Law*, 9(2): 109–128.
- GSMA (2017). The Mobile Economy 2017. Global System for Mobile Communications Association, London, February.
- GSMA (2018a). Cross-Border Data Flows: Realising benefits and removing barriers. Global System for Mobile Communications Association, London, September.
- GSMA (2018b). Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation. Global System for Mobile Communications Association, London, September.
- GSMA (2018c). The Data Value Chain. Global System for Mobile Communications Association, London, June.
- GSMA (2019a). The GSMA Guide to the Internet of Things. Global System for Mobile Communications Association, London, July.
- GSMA (2019b). The contribution of IoT to economic growth: Modelling the impact on business productivity. GSMA Intelligence, Global System for Mobile Communications Association, London, April.
- GSMA (2019c). The Impact of Data Localisation Requirements on the Growth of Mobile Money-enabled Remittances. Global System for Mobile Communications Association, London, March.
- GSMA (2020a). The Mobile Economy 2020. Global System for Mobile Communications Association, London, March.
- GSMA (2020b). The State of Mobile Internet Connectivity Report 2020. Global System for Mobile Communications Association, London, September.
- GSMA (2020c). Artificial Intelligence and Start-Ups in Low- and Middle-Income Countries: Progress, Promises and Perils. Global System for Mobile Communications Association, London, October.
- GSMA (2021). Cross-Border Data Flows: The impact of data localisation on IoT. Global System for Mobile Communications Association, London, January.
- Gupta S, Gupta K, Ghosh P and Paul SK (2020). Data Localisation: India’s Double Edged Sword? Consumer Unity & Trust Society (CUTS) International, Jaipur. Available at: <https://ssrn.com/abstract=3665197>.

- Gurumurthy A and Chami N (2019). Digital Public Goods. A Precondition for Realising the SDGs. *Global Governance Spotlight*: 4, the Development and Peace Foundation, Bonn. Available at: https://www.sef-bonn.org/fileadmin/SEF-Dateiliste/04_Publikationen/GG-Spotlight/2019/ggs_2019-04_en.pdf.
- Gurumurthy A and Chami N (2020). The intelligent corporation. Data and the digital economy. In: Buxton N, ed., *State of Power 2020: The Corporation*, Transnational Institute: 10–20.
- Gurumurthy A, Vasudevan A and Chami N (2017). The grand myth of cross-border data flows in trade deals. IT for Change, Bangalore, December. Available at: <https://itforchange.net/sites/default/files/1470/dataflow-11am.pdf>.
- Haskel J and Westlake S (2017). *Capitalism without Capital: The Rise of the Intangible Economy*. Princeton University Press, Princeton, NJ.
- Heeks R and Renken J (2018). Data Justice for Development: What Would It Mean? *Information Development*, 34(1): 90–102.
- Heeks R, Rakesh V, Sengupta R, Chattapadhyay S and Foster C (2021). Datafication, Value and Power in Developing Countries: Big Data in Two Indian Public Service Organizations. *Development Policy Review*, 39(1): 82–102.
- Hesselman C et al. (2020). A Responsible Internet to Increase Trust in the Digital World. *Journal of Network and Systems Management*, 28(4): 882–992.
- Heverly RA (2003). The Information Semicommons. *Berkeley Technology Law Journal*, 18(4): 1127–1190.
- Hilbig S (2018). Handelsrecht – freie Fahrt auf der Datenautobahn. Brot für die Welt, 6 November. Available at: <https://www.brot-fuer-die-welt.de/blog/2018-handelsrecht-freie-fahrt-auf-der-datenautobahn/>.
- Hill JF (2014). The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders. *Lawfare Research Paper Series*, 2(3): 1–41.
- Hill R (2018). Why should data flow freely? Association for Proper Internet Governance (APIG), March. Available at: <http://www.apig.ch/Forum%202018%20Policy%20statement.pdf>.
- Hill R (2020). A New Convention for Data and Cyberspace. In: Sarkar S and Korjan A, eds., *A Digital New Deal: Visions of Justice in a Post-Covid World*, Just Net Coalition and IT for Change: 180–200.
- Hinrich Foundation (2019). The Data Revolution: Capturing the Digital Trade Opportunity at Home and Abroad. Hinrich Foundation, 4 February. Available at: <https://www.hinrichfoundation.com/research/project/digital-trade-research-project/>.
- Hoffmann S, Lazanski D and Taylor E (2020). Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet. *Journal of Cyber Policy*, 5(2): 239–264.
- Huang T and Arnold Z (2020). Immigration Policy and the Global Competition for AI Talent. Center for Security and Emerging Technology, Georgetown University, Washington, DC, June. Available at: <https://cset.georgetown.edu/publication/immigration-policy-and-the-global-competition-for-ai-talent/>.
- Hummel P, Braun M, Tretter M and Dabrock P (2021). Data sovereignty: A review. *Big Data & Society*, 8(1): 1–17.
- Hunt SD and Morgan RM (1995). The Comparative Advantage Theory of Competition. *Journal of Marketing*, 59(2): 1–15.
- Hurst D (2019). Japan Calls for Global Consensus on Data Governance. *The Diplomat*, 2 February. Available at: <https://thediplomat.com/2019/02/japan-calls-for-global-consensus-on-data-governance/>.
- Iazzolino G and Mann L (2019). Harvesting Data: Who Benefits from Platformization of Agricultural Finance in Kenya? *Developing Economics*, 29 March. Available at: <https://developingeconomics.org/2019/03/29/harvesting-data-who-benefits-from-platformization-of-agricultural-finance-in-kenya/>.
- Ichilevici de Oliveira A, Heseleva K and Ramos VJ (2020). Towards a Multilateral Consensus on Data Governance. Policy Brief, Global Solutions Initiative Foundation, Berlin, 20 May. Available at: https://www.global-solutions-initiative.org/wp-content/uploads/2020/05/Towards-a-Multilateral-Consensus-for-Data-Governance_Ramos_deOliveira_Heseleva.pdf.
- IDC (2020a). Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide. International Data Corporation, Needham, MA, 18 June. Available at: <https://www.idc.com/getdoc.jsp?containerId=prUS46609320>.
- IDC (2020b). IoT Growth Demands Rethink of Long-Term Storage Strategies. IDC Media Center, International Data Corporation, Singapore, 28 July. Available at: <https://www.idc.com/getdoc.jsp?containerId=prAP46737220>.

- IDC (2021a). Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts. International Data Corporation, Needham, MA, 24 March. Available at: <https://www.idc.com/getdoc.jsp?containerId=prUS47560321>.
- IDC (2021b). The Role of Satellite as an Augmented Connectivity. Market Perspective - Doc # AP45983020. International Data Corporation, Needham, MA, February. Available at: <https://www.idc.com/getdoc.jsp?containerId=AP45983020>.
- IDC and OpenEvidence (2017). European Data Market, Final Report. SMART 2013/0063. European Commission, Brussels, 1 February. Available at: <https://datalandscape.eu/study-reports>.
- IEA (2020). Data Centres and Data Transmission Networks. Tracking Report. International Energy Agency, Paris. Available at: <https://www.iea.org/reports/data-centres-and-data-transmission-networks>.
- Imbrie A, Fedasiuk R, Aiken C, Chhabra T and Chahal H (2020). Agile Alliances: How the United States and Its Allies Can Deliver a Democratic Way of AI. Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service, Washington DC, February. Available at: <https://cset.georgetown.edu/publication/agile-alliances/>.
- International Chamber of Commerce (2021). Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in WTO Negotiations on E-Commerce. International Chamber of Commerce (ICC), Paris, 26 January. Available at: <https://iccwbo.org/content/uploads/sites/3/2021/01/multi-industry-statement-on-crossborder-data-transfers-and-data-localization.pdf>.
- Internet Society (2015). Policy Brief: Internet Exchange Points (IXPs). Internet Society, 30 October. Available at: <https://www.internetsociety.org/policybriefs/ixps/>.
- Internet Society (2020a). White Paper: Considerations for Mandating Open Interfaces. Internet Society, 4 December. Available at: <https://www.internetsociety.org/wp-content/uploads/2020/12/ConsiderationsMandatingOpenInterfaces-03122020-EN.pdf>.
- Internet Society (2020b). Discussion Paper: An analysis of the “New IP” proposal to the ITU-T. Internet Society, 24 April. Available at: <https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/>.
- Internet Society (2020c). Internet Way of Networking Use Case: Data Localization. Internet Society, September. Available at: <https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-Use-Case-Data-Localization-EN.pdf>.
- Ismail Y (2020). E-commerce in the World Trade Organization: History and latest developments in the negotiations under the Joint Statement. International Institute for International Development (IISD), Winnipeg, 31 January. Available at: <https://www.iisd.org/publications/e-commerce-world-trade-organization-history-and-latest-developments-negotiations-under>.
- ITIF (2019). Submarine Cables: Critical Infrastructure for Global Communications. Information Technology and Innovation Foundation, April. Available at: <http://www2.itif.org/2019-submarine-cables.pdf>.
- ITU (2018). Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security. International Telecommunication Union, Geneva. Licence: CC BY-NC-SA 3.0 IGO. Available at: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf.
- ITU (2020). *Measuring digital development, Facts and figures 2020*. International Telecommunication Union, Geneva. Available at: <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>.
- ITU and UNESCO (2020). *State of Broadband Report 2020: Tackling digital inequalities – A decade for action*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, 2020. License: CC BY-NC-SA 3.0 IGO. Available at: <http://handle.itu.int/11.1002/pub/8165dc3c-en>.
- Jain S and Gabor D (2020). The Rise of Digital Financialisation: The Case of India. *New Political Economy*, 25(5): 813–28.
- James D (2020). Digital Trade Rules: A disastrous new constitution for the global economy written by and for Big Tech. Rosa-Luxemburg-Stiftung, Brussels. Available at: <https://cepr.net/wp-content/uploads/2020/07/digital-trade-2020-07.pdf>.
- Janow ME and Mavroidis PC (2019). Digital trade, e-commerce, the WTO and regional frameworks. *World Trade Review*, 18(S1), S1–S7.
- Jha S and Germann S (2020). How can we make health data a global public good? MMS Bulletin 148, Medicus Mundi Schweiz, Basel and Geneva. Available at: <https://www.medicusmundi.ch/de/advocacy/publikationen/mms-bulletin/digital-health-fluch-oder-segen-fuer-die-globale-gesundheit/neue-herausforderungen-durch-kuenstliche-intelligenz/how-can-we-make-health-data-a-global-public-good>.

- Jurowetzki R, Hain DS, Mateos-Garcia J and Stathoulopoulos K (2021). The Privatization of AI Research(-ers): Causes and Potential Consequences. From university-industry interaction to public research brain-drain? Cornell University, Ithaca, NY, 15 February. Available at: <https://arxiv.org/abs/2102.01648>.
- Kanth DR (2019). India boycotts 'Osaka Track' at G20 summit. *Mint*, 30 June. Available at: <https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html>.
- Kathuria R, Kedia M, Varma G and Bagchi K (2019). Economic Implications of Cross-Border Data Flows. Internet and Mobile Association of India, November. Available at: http://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf.
- Kavacs A and Ranganathan N (2019). Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India. Data Governance Network Working Paper, No. 3, November.
- Kawalek P and Bayat A (2017). Data As Infrastructure. National Infrastructure Commission, 14 December. Available at: <https://aura.abdn.ac.uk/handle/2164/11906>.
- Kelsey J (2018). How a TPP-Style E-Commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO). *Journal of International Economic Law*, 21(2): 273–295.
- Kesan JP, Hayes CM and Bashir MN (2016). A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy. *Indiana Law Journal*, 91(2): 267–352.
- Kilic B and Avila R (2019). Cross border data flows, privacy, and global inequality. Public Citizen, Washington, DC. Available at: <https://www.citizen.org/article/crossborder-data-flows-privacy/>.
- Kimura F (2020). Developing a policy regime to support the free flow of data: A proposal by the T20 Task Force on Trade, Investment and Globalization. VoxEU.org, 7 January. Available at <https://voxeu.org/article/developing-policy-regime-support-free-flow-data>.
- Kitchin R and McArdle G (2016). What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. *Big Data & Society*.
- Komaitis K (2017). The 'Wicked Problem' of Data Localisation. *Journal of Cyber Policy*, 2(3): 355–365.
- Krotova A and Eppelsheimer J (2019). Data governance in der wissenschaftlichen Literatur: Eine Begriffsklärung anhand einer Text-Mining-basierten Literaturrecherche. *IW-Trends-Vierteljahresschrift zur empirischen Wirtschaftsforschung*, 46(3): 55–71, Institut der deutschen Wirtschaft (IW), Köln. Available at: <http://hdl.handle.net/10419/209531>.
- Kukutai T and Taylor J (2016). Data Sovereignty for Indigenous Peoples: Current Practice and Future Needs. In: Kukutai T and Taylor J, eds. *Indigenous Data Sovereignty: Toward an Agenda*, ANU Press, The Australian National University, Canberra: 1–22.
- Kuner C (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD Digital Economy Papers*, No. 187. OECD Publishing, Paris.
- Kuner C (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press, Oxford.
- Kurbalija J and Höne K (2021). 2021: The emergence of digital foreign policy. DiploFoundation, Geneva. Available at: https://www.diplomacy.edu/sites/default/files/2021-03/2021_The_emergence_of_digital_foreign_policy.pdf.
- Kurlantzick J (2020). China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom? *The Diplomat*, 17 December. Available at: <https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/>.
- Kwet M (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4): 3-26.
- Leblond P (2020). Digital Trade: Is RCEP the WTO's Future? Center for International Governance Innovation, Waterloo, ON, 23 November. Available at: <https://www.cigionline.org/articles/digital-trade-rcep-wtos-future>.
- Leblond P and Aaronson SA (2019). A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma. CIGI Papers Series, No. 226. Centre for International Governance Innovation, Waterloo, ON.
- Lee JA (2018). Hacking into Chinese Cybersecurity Law. *Wake Forest Law Review*, 53(1): 57–104.
- Leviathan Security Group (2015). Quantifying the Cost of Forced Localization. Leviathan Security Group, Seattle, WA. Available at: <https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>.
- Lewis D (2020). Why many countries failed at COVID contact-tracing – but some got it right. *Nature*, 588:384–388.

- Linden O and Dahlberg E (2016). Data flows – a fifth freedom for the internal market? Kommerskollegium (National Board of Trade Sweden), Stockholm. Available at: <https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2016/publ-data-flows.pdf>.
- Liu J (2020). China's Data Localization. *Chinese Journal of Communications*, 13(1): 84–103.
- Liu L (2021). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development*, 56: 45–67. Available at: <https://link.springer.com/article/10.1007/s12116-021-09319-8>.
- Lowry A (2020). Russia's Digital Economy Program: An Effective Strategy for Digital Transformation? In: Gritsenko D, Wijermars M and Kopotev M, eds., *The Palgrave Handbook of Digital Russia Studies*, Palgrave Macmillan: 53–76.
- Ly B (2020). Challenge and perspective for Digital Silk Road. *Cogent Business & Management*, 7(1): 1804180.
- MacFeely S (2020a). In search of the data revolution: Has the official statistics paradigm shifted? *Statistical Journal of the IAOS*, 36(4): 1075–1094.
- MacFeely S (2020b). A Global Data Convention? UN World Data Forum, 23 October. Available at <https://theunbrief.com/2020/10/23/a-global-data-convention/>.
- Malcolm J (2016). TISA Proposes New Global Rules on Data Flows and Safe Harbors. The Electronic Frontier Foundation, 24 October. Available at: <https://www.eff.org/deeplinks/2016/10/tisa-proposes-new-global-rules-data-flows-and-safe-harbors>.
- Malik F, Nicholson B and Morgan S (2016). Assessing the Social Development Potential of Impact Sourcing. In: Nicholson B, Babin R and Lacity MC, eds., *Socially Responsible Outsourcing: Global Sourcing with Social Impact, Technology, Work and Globalization*. Palgrave Macmillan UK, London: 97–118.
- Maréchal N (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communications*, 5(1): 29–41.
- Martin N, Matt C, Niebel C and Blind K (2019). How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers*, 21: 1307–1324.
- Mattoo A and Meltzer JP (2018). International Data Flows and Privacy: The Conflict and Its Resolution. *Journal of International Economic Law*, 21(4): 769–789.
- Mayer J (2020). Development strategies for middle-income countries in a digital world – impacts from trade costs, data and innovation policies. TMCD Working paper series No. TMD-WP-80, Technology and Management Centre for Development (TMCD), Oxford Department of International Development, University of Oxford. Available at: <https://www.oxfordtmc.org/publication/development-strategies-middle-income-countries-digital-world-impacts-trade-costs-data>.
- Mayer-Schönberger V and Cukier K (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt, Boston.
- Mazzucato M (2018). Let's make private data into a public good. *MIT Technology Review*, Massachusetts Institute of Technology, Cambridge, MA, 27 June. Available at: <https://www.technologyreview.com/2018/06/27/141776/lets-make-private-data-into-a-public-good/>.
- Mazzucato M, Entsminger J and Kattel R (2020). Public value and platform governance. UCL Institute for Innovation and Public Purpose, Working Paper Series IPP WP 2020-11, University College London, London.
- McKinsey (2014). Global flows in a digital age: How trade, finance, people, and data connect the world economy. McKinsey Global Institute, April.
- McKinsey (2016). Digital Globalization: The New Era of Global Flows. McKinsey Global Institute, March.
- McKinsey (2019). Globalization in transition: The future of trade and value chains. McKinsey Global Institute, January.
- McLaughlin M and Castro D (2019). The Case for a Mostly Open Internet. Information Technology and Innovation Foundation, Washington, DC, 16 December.
- Medhora RP and Owen T (2020). A Post-COVID-19 Digital Bretton Woods. Available at <https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/>.
- Meltzer JP (2015). The Internet, Cross-Border Data Flows and International Trade. *Asia and the Pacific Policy Studies*, 2(1): 90–102.
- Meltzer JP (2018). A Digital Trade Policy for Latin America and the Caribbean. Technical Note, No. IDB-TN-1483, Inter-American Development Bank, Washington, DC.
- Meltzer JP (2019). Governing Digital Trade. *World Trade Review*, 18(S1), S23–S48.

- Meltzer JP (2020). The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security. VoxEU.org, 5 August. Available at: <https://voxeu.org/article/impact-gdpr-data-flows-and-national-security>.
- Micheli M, Ponti M, Craglia M and Berti Suman A (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, 7(2): 1–15.
- Microsoft (2018). A Cloud for Global Good: A policy road map for a trusted, responsible and inclusive cloud – The 2018 Update. Microsoft. Available at: https://news.microsoft.com/cloudforgood/_media/downloads/a-cloud-for-global-good-2018-english.pdf.
- MIKTA (2016). MIKTA E-commerce Workshop Reflections. Mexico, Indonesia, the Republic of Korea, Turkey and Australia (MIKTA). The Ministry of Foreign Affairs MIKTA, 8 August. Available at: <http://www.mikta.org/document/others.php?at=view&idx=235&ckattempt=1>.
- Mishra N (2019). Building Bridges: International Trade Law, Internet Governance and the Regulation of Data Flows. *Vanderbilt Journal of Transnational Law*, 52(2): 463–509.
- Mishra N (2020a). The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance. *Journal of World Trade*. 54(4): 567–90.
- Mishra N (2020b). Privacy, Cybersecurity and GATS Article XIV: A New Frontier for Trade and Internet Regulation? *World Trade Review*, 19(3): 341–64.
- Mitchell AD and Hepburn J (2017). Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. *Yale Journal of Law and Technology*, 19(1): 182–237.
- Mitchell AD and Mishra N (2019). Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. *Journal of International Economic Law*, 22(3): 389–416.
- Monteiro J-A and Teh R (2017). Provisions on Electronic Commerce in Regional Trade Agreements. WTO Working Paper, No. ERSD-2017-11, Economic Research and Statistics Division, World Trade Organization, Geneva, July.
- Moorthy V, Henao Restrepo AM, Preziosi M-P and Swaminathan S (2020). Data Sharing for Novel Coronavirus (COVID-19). *Bulletin of the World Health Organization*, 98(3): 150.
- Morgan Stanley (2020). Space: Investing in the Final Frontier. Research, Morgan Stanley, New York, NY, 24 July. Available at: <https://www.morganstanley.com/ideas/investing-in-space>.
- Morozov E (2017). Digital intermediation of everything: at the intersection of politics, technology and finance. 4th Council of Europe Platform Exchange and Digitisation, Council of Europe, “Empowering Democracy through Culture – Digital Tools for Culturally Competent Citizens”, ZKM Center for Art and Media, Karlsruhe, 19–20 October. Available at: <https://rm.coe.int/digital-intermediation-of-everything-at-the-intersection-of-politics-t/168075baba>.
- Mosoti V (2006). Africa in the first decade of WTO dispute settlement. *Journal of International Economic Law*, 9(2): 427–453.
- Mozilla Insights, van Geuns J and Brandusescu A (2020). Shifting Power Through Data Governance. Mozilla, 16 September. Available at: <https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/>.
- Mueller M (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Polity Press, Cambridge, CB2 and Malden, MA.
- National Telecommunications and Information Administration (2016). Measuring the Value of Cross-Border Data Flows. United States Department of Commerce, Washington, DC, 30 September. Available at: <https://www.ntia.gov/report/2016/measuring-value-cross-border-data-flows>.
- NewVantage Partners (2021). Big Data and AI Executive Survey 2021 Executive Summary of Findings: The Journey to Becoming Data-Driven: A Progress Report on the State of Corporate Data Initiatives. Available at https://c6abb8db-514c-4f5b-b5a1-fc710f1e464e.filesusr.com/ugd/e5361a_76709448ddc6490981f0cbea42d51508.pdf.
- Nguyen D and Paczos M (2020). Measuring the economic value of data and cross-border data flows: A business perspective. *OECD Digital Economy Papers*, No. 297, OECD Publishing, Paris.
- Nicholson JR and Noonan R (2017). Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services. *Current Politics and Economics of the United States, Canada and Mexico*, 19(1): 53–83.
- Noble SU (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press, New York, NY.
- Nocetti J (2015). Contest and Conquest: Russia and Global Internet Governance. *International Affairs*, 91(1): 111–130.

- Nussipov A (2020a). How China Governs Data, Center for Media, Data and Society, The CMDS Blog, 27 April, available at <https://medium.com/center-for-media-data-and-society/how-china-governs-data-ff71139b68d2>.
- Nussipov A (2020b). How Data Became a Trade Issue. The CMDS Blog, Centre for Media, Data and Society, Medium, 16 April. Available at <https://medium.com/center-for-media-data-and-society/how-data-became-a-trade-issue-e4676eb048e8>.
- NVTC (2020). The Impact of Data Centers on the State and Local Economies of Virginia. North Virginia Technology Council, Richmond, VA. Available at: http://biz.loudoun.gov/wp-content/uploads/2020/02/Data_Center_Report_2020.pdf.
- Nyokabi DM, Diallo N, Ntesang NW, White TK and Ilori T (2019). The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa. *Global Campus Human Rights Journal*, 3(2): 147–172.
- O'Hara K (2019). Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship. Web Science Institute White Papers 1, University of Southampton, Southampton.
- OECD (2007). OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. OECD, Paris.
- OECD (2013a). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers*, No. 220, OECD Publishing, Paris.
- OECD (2013b). Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines. *OECD Digital Economy Papers*, No. 229. OECD Publishing, Paris.
- OECD (2014). OECD Principles for Internet Policy Making. OECD, Paris.
- OECD (2015). Data-Driven Innovation: Big Data for Growth and Well-Being. OECD Publishing, Paris.
- OECD (2019a). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. OECD Publishing, Paris.
- OECD (2019b). Unlocking the potential of e-commerce, OECD Going Digital Policy Note, OECD, Paris.
- OECD (2019c). State of Play in the Governance of Critical Infrastructure Resilience. In: *Good Governance for Critical Infrastructure Resilience*, OECD Publishing, Paris: 45–82.
- OECD (2020). Mapping Approaches to Data and Data Flows. Report for the G20 Digital Economy Task Force, Saudi Arabia. OECD, Paris.
- OECD (2021). OECD Secretary-General Tax Report to G20 Finance Ministers and Central Bank Governors – April 2021. OECD, Paris.
- OECD and WTO (2017). *Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development*. WTO and OECD publishing. Geneva and Paris.
- OECD, WTO, and IMF (2020). Handbook on Measuring Digital Trade, Version 1. OECD, Paris. Available at: <https://www.oecd.org/sdd/its/handbook-on-measuring-digital-trade.htm>.
- OHCHR (2020). Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights. A/HRC/43/29. Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General. Human Rights Council, forty-third Session, 24 February–20 March.
- Ohm P (2010). Broken Promises of Privacy: Responding to the Surprising Failures of Anonymization. *UCLA Law Review*, 57(6): 1701–1777.
- Open Data Institute (2019a). Data Trusts: Lessons from Three Pilots. Open Data Institute, London, 15 April. Available at: <https://theodi.org/article/odi-data-trusts-report/>.
- Open Data Institute (2019b). What are the Links Between Data Infrastructure and Trade Competitiveness? Open Data Institute, London, 3 July. Available at: <https://theodi.org/article/what-are-the-links-between-data-infrastructure-and-trade-competitiveness/>.
- Open Rights Group (2014). TTIP's threat to our privacy and culture. London, 14 October. Available at: <https://www.openrightsgroup.org/blog/ttips-threat-to-our-privacy-and-culture/>.
- Organ J (2017). EU citizen participation, openness and the European Citizens Initiative: the TTIP legacy. *Common Market Law Review*, 54(6): 1713–1747.
- Our World is Not for Sale (2019). Civil Society Letter Against Digital Trade Rules in the World Trade Organization (WTO). 1 April. Available at: http://www.ourworldisnotforsale.net/2019/Digital_trade_2019-04-01-en.pdf.
- Pamment J (2019). Accountability as Strategic Transparency: Making Sense of Organizational Responses to the International Aid Transparency Initiative. *Development Policy Review*, 37(5): 657–671.

- Panday J (2017). Rising Demands for Data Localization a Response to Weak Data Protection Mechanisms. Electronic Frontier Foundation, 14 August. Available at: <https://www.eff.org/deeplinks/2017/08/rising-demands-data-localization-response-weak-data-protection-mechanisms>.
- PDPC (2018). Guide to Basic Data Anonymisation Techniques. Personal Data Protection Commission, Singapore, 25 January. Available at: [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf).
- Pew Research Center (2019). Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. Pew Research Center, Washington, DC, 5 February. Available at: <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/>.
- Pisa M, Dixon P, Ndulu B and Nwankwo U (2020). Governing Data for Development: Trends, Challenges, and Opportunities. CGD Policy Paper, No. 190, Center for Global Development, Washington, DC.
- Pisa M and Polcari J (2019). *Governing Big Tech's Pursuit of the "Next Billion Users"*. Harvard University Press, Cambridge, MA.
- Pohle J, Gorwa R and Miller H (2020). The turn to trade agreements in global platform governance. AoIR Selected Papers of Internet Research, Association of Internet Researchers, Annual Conference, Virtual Event, 27–31 October 2020. Available at: <https://doi.org/10.5210/spir.v2020i0.11305>.
- Pohle J and Thiel T (2020). Digital sovereignty. *Internet Policy Review*, 9(4). Available at: <https://doi.org/10.14763/2020.4.1532>.
- Potluri SR, Sridhar V and Rao S (2020). Effects of Data Localization on Digital Trade: An Agent-based Modelling Approach. *Telecommunications Policy*, 44(9): 102022.
- Quismorio BA (2019). Capability building for data analytics and artificial intelligence. Presentation at the Third Session of the Intergovernmental Group of Experts on E-commerce and the Digital Economy. Available at: https://unctad.org/system/files/non-official-document/tdb_ede3_2019_p11_BQuismorio_en.pdf.
- Raghavan C (2018). Development and free data flow rules are incompatible. *Third World Economics: Trends and Analysis*, 678/679: 6–7. Third World Network (TWN), Penang.
- Rentzhog M and Jonströmer H (2014). No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden. Kommerskollegium (National Board of Trade Sweden), Stockholm. Available at: https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2016-och-aldre/no_transfer_no_trade_webb.pdf.
- Rikap C (2021). Intellectual monopoly capitalism and its effects on development. *Developing Economics*, 7 April. Available at: <https://developingeconomics.org/2021/04/07/intellectual-monopoly-capitalism-and-its-effects-on-development/>.
- Roberts A, Moraes HC and Ferguson V (2019). Toward a Geoeconomic Order in International Trade and Investment. *Journal of International Economic Law*, 22(4): 655–76.
- Rodriguez K and Alimonti V (2020). A Look-Back and Ahead on Data Protection in Latin America and Spain. Electronic Frontier Foundation, 21 September. Available at: <https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain>.
- Rodrik D (2020). The Coming Global Technology Fracture. Project Syndicate, 8 September. Available at: <https://www.project-syndicate.org/commentary/making-global-trade-rules-fit-for-technology-by-dani-rodrik-2020-09>.
- The Royal Society (2021). Data for international health emergencies: governance, operations and skills. Statement by the Science Academies of the G7 nations, March. Available at: <https://www.interacademies.org/publication/data-international-health-emergencies-governance-operations-and-skills>.
- Rühlig TN (2020). Technical standardisation, China and the future international order – A European perspective. E-Paper, Heinrich-Böll-Stiftung European Union, Brussels. Available at: <https://eu.boell.org/en/2020/03/03/technical-standardisation-china-and-future-international-order>.
- Sacks S and Sherman J (2019). Global Data Governance: Concepts, Obstacles, and Prospects. New America, Washington, DC. Available at: <https://www.newamerica.org/cybersecurity-initiative/reports/global-data-governance/>.
- Sadowski J (2019). When Data Is Capital: Datafication, Accumulation, and Extraction. *Big Data and Society*, 6(1): 1–12.
- Sandvine (2020). *The Global Internet, Phenomena Report, COVID-19 Spotlight*. Sandvine, May. Available at: https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%2020200507.pdf.

- Sargsyan T (2016). Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security. *International Journal of Communication*, 10: 2221–2237.
- Saveliev A (2016). Russia's New Personal Data Localisation Requirements: A Step-Forward or a Self-Imposed Sanction? *Computer Law and Security Review*, 32(1): 128–145.
- Scassa T (2018). Data Ownership. CIGI papers, No. 187, Center for International Governance Innovation, Waterloo, ON.
- Schneider I (2019). Models for the governance of data economics. Presentation at “Who Governs the Data Economy?” session at MyData Conference, Helsinki, 26 September. Available at: <https://attachment.rrz.uni-hamburg.de/f89c3ccd/Helsinki-MyData-Schneider-Data-Governance-26092019.pdf>.
- Selby J (2017). Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? *International Journal of Law and Information Technology*, 25(3): 213–232.
- Sell SK (2009). Cat and mouse: Forum-shifting in the battle over intellectual property enforcement. Draft prepared for the American Political Science Association Meeting, 3–6 September. Available at: https://ipgovernance.eu/conferences/2009APSAToronto/Sell_APSA2009_Cat_and_Mouse.pdf.
- Shadlen K (2008). Globalisation, Power and Integration: The Political Economy of Regional and Bilateral Trade Agreements in the Americas. *Journal of Development Studies*, 44(1): 1–20.
- Sherman J and Morgus R (2018). The Digital Deciders and the Future of the Internet. New America, Washington, DC, 2 December. Available at: <https://www.newamerica.org/cybersecurity-initiative/in-the-news/digital-deciders-and-future-internet/>.
- The Shift Project (2019). Lean ICT: Towards Digital Sobriety. The Shift Project, Paris, March. Available at: https://theshiftproject.org/wp-content/uploads/2019/03/Lean-ICT-Report_The-Shift-Project_2019.pdf.
- Singh PJ (2018a). Digital Industrialisation in Developing Countries – A Review of the Business and Policy Landscape. Research Paper for the Commonwealth Secretariat, IT for Change, Bangalore, January.
- Singh PJ (2018b). Data Localisation: A Matter of Rule of Law and Economic Development. Policy Brief, IT For Change, Bangalore, September.
- Singh PJ (2019). India Should Aim for a Digital Non-Alignment. IT for Change, Bangalore, July.
- Singh PJ and Vipra J (2019). Economic Rights Over Data: A Framework for Community Data Ownership. *Development*, 62: 53–57.
- Sinha A and Basu A (2019). The Politics of India's Data Protection Ecosystem. *Economic & Political Weekly*, 54(49).
- Slaughter MJ and McCormick DH (2021). Data Is Power. *Foreign Affairs*, May/June 2021.
- Spiezia V and Tscheke J (2020). International agreements on cross-border data flows and international trade: A statistical analysis. *OECD Science, Technology and Industry Working Papers*, No. 2020/09, OECD, Paris.
- Srikrishna Committee Report (2018). Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Ministry of Electronics and Information Technology, Government of India. Available at: https://www.meiti.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
- Srnicek N (2016). *Platform Capitalism*. Polity Press, Cambridge, United Kingdom.
- Statista (2021). Amazon Leads \$130-Billion Cloud Market. 4 February. Available at: <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>.
- Statistics Canada (2019). Measuring investment in data, databases and data science: Conceptual framework. Catalogue No. 13-605-X, 24 June. Available at: <https://www150.statcan.gc.ca/n1/pub/13-605-x/2019001/article/00008-eng.htm>.
- Steinberg RH (2002). In the shadow of law or power? Consensus-based bargaining and outcomes in the GATT/WTO. *International Organization*, 56(2): 339–374.
- Stiglitz JE (2012). *The Price of Inequality: How Today's Divided Society Endangers Our Future*. W.W. Norton and Company, New York, NY.
- Streinz T (2021). RCEP's Contribution to Global Data Governance. *Afronomicslaw*, 19 February. Available at: <https://www.afronomicslaw.org/category/analysis/rceps-contribution-global-data-governance-0>.
- Suominen K (2018). Fueling Digital Trade in Mercosur: A Regulatory Roadmap. Technical note, No. IDB-TN-01549, Inter-American Development Bank, Washington, DC, October.
- Suranovic SM (2002). International labour and environmental standards agreements: Is this fair trade? *World Economy*, 25(2), 231–245.

- Synergy Research Group (2021a). Microsoft, Amazon and Google Account for Over Half of Today's 600 Hyperscale Data Centers. Synergy Research Group, Reno, NV, 26 January. Available at: <https://www.srgresearch.com/articles/microsoft-amazon-and-google-account-for-over-half-of-todays-600-hyperscale-data-centers>.
- Synergy Research Group (2021b). Cloud Market Ends 2020 on a High while Microsoft Continues to Gain Ground on Amazon. Synergy Research Group, Reno, NV, 2 February. Available at: <https://www.srgresearch.com/articles/cloud-market-ends-2020-high-while-microsoft-continues-gain-ground-amazon>.
- Tang C (2021). *Data Capital. How Data is Reinventing Capital for Globalization*. Springer International Publishing. Available at: <https://www.springer.com/gp/book/9783030601911>.
- Taylor RD (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, 44(8): 102003.
- TeleGeography (2015). International Bandwidth Trends in Africa. What Has (and Hasn't) Changed in the Past Five Years, 27 August. Available at: http://isoc-ny.org/afpif2015/AfPIF2015_Teleography.pdf.
- TeleGeography (2019). Back to the Future. Presentation by Alan Mauldin, TeleGeography Workshop at Pacific Telecommunications Council (PTC), 20 January. Available at: <https://www2.telegeography.com/hubfs/2019/Presentations/TeleGeo-PTC2019.pdf>.
- TeleGeography (2021a). *The State of the Network: 2021 Edition*. TeleGeography, San Diego, CA. Available at: <https://www2.telegeography.com/hubfs/assets/Ebooks/state-of-the-network-2021.pdf>.
- TeleGeography (2021b). Exploring the Cloud, Overland and Undersea. Trends in Cloud Infrastructure and Global Networks, 17 February. Available at: <https://www2.telegeography.com/hubfs/2021/Presentations/2021%20Cloud%20Trends.pdf>.
- Tomura E, Ito B and Kang B (2019). Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms. *RIETI Discussion Paper Series*, No. 9-E-088. Research Institute of Economy, Trade and Industry (RIETI), Tokyo. Available at: <https://www.rieti.go.jp/jp/publications/dp/19e088.pdf>.
- Trade Justice Movement (2020). Digital trade (e-commerce). Trade Justice Movement, London. Available at: <https://www.tjm.org.uk/trade-issues/digital-trade-e-commerce>.
- Triolo P, Allison K and Brown C (2020). The Digital Silk Road: Expanding China's digital footprint. Eurasia Group, New York, NY, 29 April. Available at: <https://www.eurasiagroup.net/live-post/digital-silk-road-expanding-china-digital-footprint>.
- UNCITRAL (2020). Legal issues related to the digital economy – data transactions. United Nations Commission on International Trade Law, Fifty-third session. A/CN.9/1012/Add.2. Available at: <https://undocs.org/en/A/CN.9/1012/Add.2>.
- UNCTAD (2016). *Data protection regulations and international data flows: Implications for trade and development*. United Nations publication, UNCTAD/WEB/DTL/STICT/2016/1/iPub. New York and Geneva.
- UNCTAD (2017). *Information Economy Report 2017: Digitalization, Trade and Development*. United Nations publication, Sales No. E.17.II.D.8. New York and Geneva.
- UNCTAD (2019a). *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*. United Nations publication, Sales No. E.19.II.D.17. New York and Geneva.
- UNCTAD (2019b). Competition issues in the digital economy. Note by the UNCTAD secretariat. TD/B/C.I/CLP/54. Trade and Development Board, Intergovernmental Group of Experts on Competition Law and Policy, Eighteenth session, Geneva, 10–12 July.
- UNCTAD (2021a). *COVID-19 and E-commerce: a Global Review*. United Nations publication, Sales No. E.21.II.D.9. Geneva.
- UNCTAD (2021b). *What is at stake for developing countries in trade negotiations? – The case of joint statement initiative*. United Nations publication, UNCTAD/DITC/TNCD/2020/5. Geneva.
- UNCTAD (2021c). *The UNCTAD B2C E-commerce Index 2020: Spotlight on Latin America and the Caribbean*. UNCTAD Technical Notes on ICT for Development, No. 17. Geneva.
- UNCTAD (2021d). *Technology and Innovation Report 2021: Catching technological waves: Innovation with equity*. United Nations publication, sales No. E.21.II.D.8. New York and Geneva.
- UNCTAD (2021e). E-Commerce and Digital Economy Programme: Year in Review 2030: Facilitating inclusive digital economies in challenging times. Available at https://unctad.org/system/files/official-document/dtlistictinf2021d2_en.pdf.

- UNDP (2020). Data Philanthropy, International Organizations and Development Policy: Ethical Issues to Consider. Discussion Paper, United Nations Development Programme, New York, April.
- UNEP (2020). UNEP's contribution to Round Table 1B on Digital Public Goods. Environmental data as digital public goods within a digital ecosystem for the planet. United Nations Environment Programme, Nairobi.
- UNESCO (2020). Outcome document: first draft of the recommendation on the ethics of artificial intelligence. Document code: SHS/BIO/AHEG-AI/2020/4 REV.2. Ad Hoc Expert Group for the preparation of a draft text of a recommendation on the ethics of artificial intelligence, Paris, 7 September.
- United Nations (2019). The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation, New York.
- United Nations (2020a). Roadmap for Digital Cooperation. Report of the Secretary-General. New York.
- United Nations (2020b). Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020–22. New York.
- United Nations (2020c). The Highest Aspiration – A Call to Action for Human Rights. New York.
- United Nations (2021). Tax consequences of the digitalized economy – issues of relevance for developing countries. E/C.18/2021/CRP.1. Co-Coordination Report, Committee of Experts on International Cooperation in Tax Matters, twenty-second session, 19–28 April.
- United States Chamber of Commerce Foundation (2014). The Future of Data-Driven Innovation. U.S. Chamber of Commerce Foundation, Washington, DC.
- United States Department of Justice (2019). Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, Washington, DC. Available at: <https://www.justice.gov/opa/press-release/file/1153446/download>.
- United States Trade Representative (2020). United States–Kenya Negotiations: Summary of Specific Negotiating Objectives. Washington, DC, May. Available at: https://ustr.gov/sites/default/files/Summary_of_U.S.-Kenya_Negotiating_Objectives.pdf.
- Varas A, Varadarajan R, Goodrich J and Yinug F (2021). Strengthening the Global Semiconductor Supply Chain in an Uncertain Era. Boston Consulting Group and Semiconductor Industry Association, April.
- Véliz C (2019). The Internet and Privacy. In: Edmonds D, ed., *Ethics and the Contemporary World*. Routledge, Abingdon: 149–159.
- Verhulst SG (2017). A distributed model of Internet governance. Global Partners Digital, London. Available at: <https://www.gp-digital.org/publication/a-distributed-model-of-internet-governance/>.
- Verhulst SG (2019). Sharing Private Data for Public Good. Project Syndicate, 27 August. Available at: <https://www.project-syndicate.org/commentary/private-data-public-policy-collaboration-by-stefaan-g-verhulst-1-2019-08>.
- Verizon (2016). *2016 Data Breach Investigations Report*. Available at: https://regmedia.co.uk/2016/05/12/dbir_2016.pdf.
- Verizon (2017). *2017 Data Breach Investigations Report*. Available at: <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/highlights-of-the-2017-verizon-dbir-analyzing-the-latest-breach-data-in-10-years-of-incident-trends/>.
- Verizon (2018). *2018 Data Breach Investigations Report*. Available at: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.
- Verizon (2019). *2019 Data Breach Investigations Report*. Available at: <https://enterprise.verizon.com/resources/reports/dbir/2019/data-breaches-by-industry/>.
- Verizon (2020). *2020 Data Breach Investigations Report*. Available at: <https://enterprise.verizon.com/resources/reports/dbir/>.
- Vestager M and Borrell J (2021). Why Europe's Digital Decade Matters. Project Syndicate, 10 March. Available at: <https://www.project-syndicate.org/commentary/europe-digital-decade-by-margrethe-vestager-and-josep-borrell-2021-03?barrier=accesspaylog>.
- Viljoen S (2020). Democratic Data: A Relational Theory for Data Governance. Forthcoming, *Yale Law Journal*, 131.
- Villani C (2018). For a Meaningful Artificial Intelligence: Towards a French and European Strategy. A French parliamentary mission (8 September 2017–8 March 2018), AI for Humanity, Paris. Available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.
- Voss GW (2020). Cross-Border Data Flows, the GDPR, and Data Governance. *Washington International Law Journal*, 29(3): 485–532.

- Washington State Department of Commerce (2018). State of the Data Center Industry. Department of Commerce, Office of Economic Development and Competitiveness, State of Washington, Olympia, WA. Available at: <https://www.commerce.wa.gov/wp-content/uploads/2018/01/Commerce-Data-Center-Study-and-appendices-2017.pdf>.
- Weber S (2017). Data, Development and Growth. *Business and Politics*, 19(3): 397–423.
- WEF (2019). Exploring International Data Flow Governance - Platform for Shaping the Future of Trade and Global Economic Interdependence. White Paper, World Economic Forum, Geneva, December. Available at: http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.
- WEF (2020a). State of the Connected World: 2020 Edition. Insight Report, World Economic Forum, Geneva, December.
- WEF (2020b). A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy. White Paper, World Economic Forum, Geneva, June.
- WEF (2020c). *The Global Risks Report 2020*. Insight Report, 15th Edition. World Economic Forum, Geneva.
- WEF (2020d). Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. White Paper, World Economic Forum, Geneva, May.
- WEF (2021). Rebuilding Trust and Governance: Towards Data Free Flow with Trust (DFFT). White Paper, World Economic Forum, Geneva, March.
- Weller D and Woodcock B (2013). Internet Traffic Exchange: Market Developments and Policy Challenges. *OECD Digital Economy Papers*, No. 207. OECD Publishing, Paris, France.
- Wesolowski A, Buckee CO, Bengtsson L, Wetter E, Lu X and Tatem AJ (2014). Commentary: Containing the Ebola Outbreak – the Potential and Challenge of Mobile Network Data. *PLoS Currents Outbreaks*, Edition 1, 29 September. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205120/>.
- Woods AK (2018). Litigating Data Sovereignty. *Yale Law Journal*, 128(2): 328–406.
- World Bank (2016). *World Development Report 2016: Digital Dividends*. doi:10.1596/978-1-4648-0671-1. World Bank, Washington, DC.
- World Bank (2021). *World Development Report 2021: Data for Better Lives*. doi:10.1596/978-1-4648-1600-0. World Bank, Washington, DC.
- Wu M (2017). Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange, Overview Paper, International Centre for Trade and Sustainable Development and Inter-American Development Bank, Geneva.
- Yakovleva S and Irion K (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, 10(3): 201–221.
- Zhang D, Mishra S, Brynjolfsson E, Etchemendy J, Ganguli D, Grosz B, Lyons T, Manyika J, Niebles JC, Sellitto M, Shoham Y, Clark J and Perrault R (2021). *The AI Index 2021 Annual Report*. AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March.
- Zwetsloot R, Dunham J, Arnold Z and Huang T (2019). Keeping Top AI Talent in the United States: Findings and Policy Options for International Graduate Student Retention. Center for Security and Emerging Technology, Georgetown's Walsh School of Foreign Service, December. Available at: <https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf>.



ISBN 978-92-1-11022-5

