INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJLAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

DIGITAL COLONIALISM AND INTERNATIONAL ECONOMIC LAW: WHO OWNS THE WORLD'S DATA?

AUTHORED BY - SAESHA GEHANI
Academic Qualification: Third (IIIrd) year Student at NLIU, Bhopal.
Institution: National Law Institute University, (NLIU) Bhopal.

CO-AUTHOR - IPSA MITTAL
Academic Qualification: Third (IIIrd) year Student at NLIU, Bhopal.
Institution: National Law Institute University, (NLIU) Bhopal.

Abstract

Debates on digital colonialism often rest on sociology and political economy. This paper asks a legal question instead. It asks how the rules of international economic law shape who controls, stores and profits from data. The paper examines the WTO agreements, TRIPS, digital trade chapters in preferential agreements and investment treaties. It argues that these regimes do not give anyone ownership of raw data. They allocate control through indirect rules. These rules protect the firms that hold data and limit the tools States can use to keep data within their borders. The paper tests this claim against India. India has adopted localisation rules in several sectors and has stayed outside the main digital trade templates. Its position is defensible in parts under the GATS exceptions and the security clause. It is also exposed to challenge, especially where a country-based restriction on data transfers could raise most-favoured-nation questions. The paper concludes that developing States should protect regulatory autonomy through careful treaty drafting, narrow and evidence-based localisation rules and regional cooperation. Data should be treated as a development resource and not only as a traded commodity. The paper states the law as at 29 September 2026.

Keywords: Digital colonialism; Cross-border data flows; Data Localisation; WTO and GATS; Regulatory autonomy; India

1. Introduction

Data is the raw material of the digital economy. A few firms in a few States collect most of it. Most of the people who generate it live elsewhere. Scholars call this pattern digital colonialism.[1] The label captures a real worry about extraction and dependence. It also leaves a gap. Colonial relations were built and kept alive through law. If the digital economy repeats that pattern, some body of law must support it.

This paper looks for that law in international economic law. It does not ask who owns data in the sense of private property. It asks how the rules of trade, intellectual property and investment decide who may hold data, who may move it and who may stop it from moving. The paper makes three claims. First, international economic law gives no one a property right in raw data. It gives control to those who hold data by protecting their related assets and by limiting the tools of States. Second, digital trade chapters export rules written by a few States and accepted by many. Third, developing States can still defend measures such as data localisation but the defence is uncertain and costly.

The paper tests these claims against India. India has adopted localisation rules in several sectors. It has also refused to join the main digital trade templates. Its position raises a sharp question. Can a large developing economy protect its regulatory autonomy over data while it holds commitments under the WTO and under older investment treaties?

The method is doctrinal. The paper reads treaty texts, adjudicated disputes and domestic instruments together. It uses critical Third World approaches to international law as a lens.[2] These approaches ask whether neutral rules produce unequal results. The paper also engages scholars who defend open data flows, because a fair account must include them.[3] Part 2 examines data and ownership. Part 3 turns to the WTO. Part 4 studies digital trade agreements. Part 5 covers investment treaties. Part 6 discusses localisation and regulatory autonomy. Part 7 examines India. Part 8 offers reforms. Part 9 concludes.

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019); Nick Couldry and Ulises A Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019); Michael Kwet, 'Digital Colonialism: US Empire and the New Imperialism in the Global South' (2019) 60 Race & Class 3.

[2] Antony Anghie, *Imperialism, Sovereignty and the Making of International Law* (CUP 2005); BS Chimni, 'The Past, Present and Future of International Law: A Critical Third World Approach' (2007) 8 Melbourne Journal of International Law 499.

[3] Anupam Chander, *The Electronic Silk Road: How the Web Binds the World Together in Commerce* (Yale University Press 2013); Anupam Chander and Uyên P Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677.

2. Data, Ownership and the Silence of TRIPS

No treaty says who owns data. TRIPS protects a compilation of data only where the selection or arrangement of its contents is an intellectual creation.[4] The protection covers the compilation and not the data inside it. The Berne Convention takes the same line.[5] National courts agree. The United States Supreme Court in *Feist* refused protection to a telephone directory that lacked original selection. The Indian Supreme Court in *Eastern Book Company* asked for a modicum of creativity and rejected the older test of skill and labour.[6] The European Union went further and created a sui generis database right.[7] It did not carry that right into TRIPS.

Trade secret law fills part of the space. Article 39 of TRIPS requires protection of undisclosed information against dishonest commercial use.[8] A firm that keeps a dataset secret can invoke that rule. Control therefore follows possession. The firm that collects and stores data holds it in practice and the law protects the holding. The person who generated the data holds no comparable right. Privacy law gives that person some interests, but those interests sit outside the trade regime and are weaker against it.[9]

Critics have long read TRIPS as a lesson in how the system works. Drahos and Braithwaite describe a process in which a few States and firms wrote rules on knowledge and then made them global.[10] Developing States accepted TRIPS as part of the Uruguay Round bargain.[11] Okediji shows that their later role has often been reactive.[12] Data follows the same pattern. The rules that matter most for data are not in TRIPS. They sit in later trade agreements.

Two developments link TRIPS to those agreements. First, digital trade chapters protect source code. The CPTPP bars a Party from requiring transfer of the source code of mass market

[4] Agreement on Trade-Related Aspects of Intellectual Property Rights (adopted 15 April 1994, entered into force 1 January 1995) 1869 UNTS 299 (TRIPS Agreement) art 10(2).
[5] Berne Convention for the Protection of Literary and Artistic Works (adopted 9 September 1886, as revised at Paris 24 July 1971) 828 UNTS 221, art 2(5).
[6] *Feist Publications Inc v Rural Telephone Service Co* 499 US 340 (1991); *Eastern Book Company v DB Modak* (2008) 1 SCC 1.
[7] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20, art 7.
[8] TRIPS Agreement (n 4) art 39.
[9] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 17; UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167.
[10] Peter Drahos and John Braithwaite, *Information Feudalism: Who Owns the Knowledge Economy?* (Earthscan 2002).
[11] Carlos M Correa, *Trade Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement* (OUP 2007); Daniel Gervais, *The TRIPS Agreement: Drafting History and Analysis* (4th edn, Sweet & Maxwell 2012).
[12] Ruth L Okediji, 'The International Relations of Intellectual Property: Narratives of Developing Country Participation in the Global Intellectual Property System' (2003) 7 Singapore Journal of International and Comparative Law 315.

software as a condition of import.[13] The USMCA also covers algorithms expressed in source code.[14] These rules shield the assets through which firms exploit data. Second, the moratorium on non-violation and situation complaints under TRIPS lapsed at the close of the Fourteenth Ministerial Conference on 30 March 2026.[15] A non-violation complaint can attack a lawful measure that upsets an expected benefit.[16] Its return is a risk for States that regulate data in ways that affect foreign right holders.

3. The WTO Framework

3.1 Data flows as trade in services

The WTO has no data agreement. Data flows are regulated through the GATS because most digital trade is trade in services.[17] Cross-border flows mostly support supply by mode 1. Hosting a data centre abroad can involve mode 3. Scholars argue that the GATS is flexible enough to reach digital measures.[18]

Two disputes matter. In *US: Gambling* the Appellate Body held that a ban on remote gambling services acted as a zero quota and breached a market access commitment.[19] In *China: Electronic Payment Services* the panel held that scheduled entries cover the services they describe even when technology changes the means of supply.[20] Together the cases support technological neutrality. A localisation rule that stops a foreign supplier from serving customers from abroad can be tested against market access where a State has made commitments. A rule that treats foreign suppliers less favourably in fact can be tested against national treatment.[21] These two rules apply only where commitments exist. This matters for

[13] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (signed 8 March 2018, entered into force 30 December 2018) (CPTPP) art 14.17.
[14] Agreement between the United States of America, the United Mexican States and Canada (signed 30 November 2018, entered into force 1 July 2020) (USMCA) art 19.16.
[15] TRIPS Agreement (n 4) art 64; WTO, 'MC14 Concludes with Adopted Decisions, Progress on Key Outstanding Issues' (30 March 2026) <https://www.wto.org/english/news_e/news26_e/mc14_30mar26_354_e.htm> accessed 29 September 2026. Members were to continue talks in Geneva after MC14, so later decisions should be checked.
[16] General Agreement on Tariffs and Trade 1994 (adopted 15 April 1994, entered into force 1 January 1995) 1867 UNTS 187, art XXIII(1)(b).
[17] General Agreement on Trade in Services (adopted 15 April 1994, entered into force 1 January 1995) 1869 UNTS 183 (GATS); WTO, *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce* (WTO 2018).
[18] Andrew D Mitchell and Neha Mishra, 'Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute' (2019) 22 Journal of International Economic Law 389; Neha Mishra, 'Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows' (2019) 52 Vanderbilt Journal of Transnational Law 463.
[19] Appellate Body Report, *United States: Measures Affecting the Cross-Border Supply of Gambling and Betting Services* WT/DS285/AB/R (7 April 2005).
[20] Panel Report, *China: Certain Measures Affecting Electronic Payment Services* WT/DS413/R (16 July 2012).
[21] GATS (n 17) arts XVI and XVII.

developing States because many made narrow commitments.

3.2 Exceptions

A State that breaches a rule can still invoke Article XIV. It allows measures necessary to secure compliance with laws on the protection of privacy in the processing and dissemination of personal data. It also covers public morals and public order. Article XIV bis covers essential security interests.[22] The word necessary carries a demanding test. The Appellate Body weighs the importance of the interest, the contribution of the measure and its trade restrictiveness. It then asks whether a less restrictive alternative is reasonably available.[23] Later reports refined the test.[24] In *Argentina: Financial Services* Argentina did not succeed in its defence.[25] Mishra argues that privacy and cybersecurity aims fit within Article XIV but that States must design their measures with care.[26] Financial services have a further route. The GATS Annex on Financial Services preserves measures taken for prudential reasons, subject to an anti-circumvention condition.[27]

Security is a special case. In *Russia: Traffic in Transit* the panel held that a Member's use of the security exception is open to review even though the Member has wide discretion in defining its essential security interests.[28] The finding gives States some room. It also means that they cannot rely on a bare assertion.

3.3 The e-commerce work programme and the moratorium

The WTO also handles digital issues through the e-commerce work programme. Ministers adopted a Declaration on Global Electronic Commerce in 1998. It set out the practice of not imposing customs duties on electronic transmissions.[29] The General Council launched the work programme later that year.[30] Ministers renewed the moratorium at almost every conference for

[22] GATS (n 17) art XIV(a) and (c)(ii) and art XIV bis.
[23] Appellate Body Report, *Korea: Measures Affecting Imports of Fresh, Chilled and Frozen Beef* WT/DS161/AB/R, WT/DS169/AB/R (11 December 2000) paras 161 to 164.
[24] Appellate Body Report, *Brazil: Measures Affecting Imports of Retreaded Tyres* WT/DS332/AB/R (3 December 2007).
[25] Appellate Body Report, *Argentina: Measures Relating to Trade in Goods and Services* WT/DS453/AB/R (14 April 2016).
[26] Neha Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?' (2020) 19 World Trade Review 341; Rolf H Weber, 'Regulatory Autonomy and Privacy Standards under the GATS' (2012) 7 Asian Journal of WTO and International Health Law and Policy 25.
[27] GATS (n 17) Annex on Financial Services, para 2(a).
[28] Panel Report, *Russia: Measures Concerning Traffic in Transit* WT/DS512/R (5 April 2019).
[29] WTO, Declaration on Global Electronic Commerce WT/MIN(98)/DEC/2 (25 May 1998).
[30] WTO General Council, Work Programme on Electronic Commerce WT/L/274 (30 September 1998).

28 years. India and South Africa challenged that practice. They argued that the moratorium costs developing States revenue and narrows industrial policy space.[31] Their objections helped lead to a sunset date at the Thirteenth Ministerial Conference in 2024. At the Fourteenth Conference in Yaoundé in March 2026 members could not agree on an extension and the moratorium lapsed.[32]

Reports differ on who blocked a deal. The United States named Brazil and Turkey. Indian reports stress the resistance of India and other developing States to a permanent ban.[33] The result is clear whatever the cause. The multilateral baseline is gone and States regain, at least in law, the option to tax electronic transmissions. Whether they use it is a separate matter. A duty on downloads could also invite retaliation against a State's own digital exports.

Plurilateral rules meanwhile advance. The Joint Statement Initiative on e-commerce began in 2017.[34] Its outcome, the Agreement on Electronic Commerce, was stabilised in 2024. The text is less ambitious than earlier drafts and leaves aside binding rules on data flows and localisation.[35] At MC14 a group of 66 Members announced interim arrangements to implement it.[36] India is not a participant. It argues that a plurilateral text cannot enter the WTO framework without multilateral consensus.[37] The dispute is about process and also about power. Plurilateral outcomes let willing States write rules that others must later accept or face isolation.[38] India and South Africa saw a threat to the consensus rule that protects smaller Members.

IJLAR

[31] WTO, Communication from India and South Africa, *Moratorium on Customs Duties on Electronic Transmissions: Need for a Re-think* WT/GC/W/747 (2019).

[32] WTO, 'Work Programme on E-Commerce, Moratorium' <https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm> accessed 29 September 2026.

[33] Office of the United States Trade Representative, 'Press Release Regarding the WTO's 14th Ministerial Conference' (March 2026) <https://ustr.gov/about/policy-offices/press-office/press-releases/2026/march/press-release-regarding-wtos-14th-ministerial-conference> accessed 29 September 2026; 'WTO's MC14 Concludes without Declaration as Countries Ran Out of Time' Business Standard (30 March 2026) <https://www.business-standard.com/amp/economy/news/wto-mc14-ends-without-declaration-e-commerce-moratorium-to-lapse-126033000991_1.html> accessed 29 September 2026.

[34] WTO, Joint Statement on Electronic Commerce WT/MIN(17)/60 (13 December 2017).

[35] WTO, Agreement on Electronic Commerce (stabilised text, July 2024); Mira Burri, 'Data Flows and Global Trade Law' in Mira Burri (ed), *Big Data and Global Trade Law* (CUP 2021).

[36] WTO, 'E-Commerce: Post-MC14 Briefing Note' <https://www.wto.org/english/thewto_e/minist_e/mc14_e/briefing_notes_e/ecommerce_e.htm> accessed 29 September 2026.

[37] WTO, Communication from India and South Africa, *The Legal Status of 'Joint Statement Initiatives' and Their Negotiated Outcomes* WT/GC/W/819 (19 February 2020).

[38] 'The WTO Joint Initiative on E-Commerce' (Digital Watch Observatory, 11 May 2026) <https://dig.watch/processes/wto-ecommerce> accessed 29 September 2026; Henry Gao, 'Across the Great Wall: E-Commerce Joint Statement Initiative Negotiation and China' in Mira Burri (ed), *Big Data and Global Trade Law* (CUP 2021).

4. Digital Trade Agreements as Rule Exporters

Preferential agreements do the work that the WTO does not. Their digital chapters carry rules on data transfer, localisation and source code.[39] The CPTPP allows cross-border transfer of information for the conduct of business and bars localisation of computing facilities as a condition of doing business. A Party may depart from these rules to achieve a legitimate public policy objective. The measure must not be arbitrary or a disguised restriction on trade and must not impose greater restrictions than required.[40] The USMCA keeps a similar exception for data transfers. Its ban on localisation has no exception of its own.[41] The US-Japan Digital Trade Agreement follows that model.[42] The DEPA adopts similar wording within a modular structure.[43]

The RCEP strikes a different balance. It lets the implementing Party decide what it considers necessary to achieve a legitimate public policy objective. Its security limb is self-judging. Its e-commerce chapter is also excluded from State-to-State dispute settlement.[44] Asian developing States accepted disciplines only on terms that kept their discretion. The European Union takes a third route. It treats data protection as a fundamental right. Its horizontal clauses allow data flows while preserving measures a Party deems appropriate to protect personal data.[45] China stresses sovereignty and security and pairs strict domestic controls with selective external openness.[46] Aaronson and Leblond describe the result as competing data realms.[47]

The colonial reading of this pattern is easy to state. The rule makers are the home States of the large firms. The rule takers gain market access and give up policy tools. Streinz analyses the CPTPP model as a form of megaregulation that sets global expectations for the digital

[39] Mark Wu, 'Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System' (ICTSD and Inter-American Development Bank 2017).
[40] CPTPP (n 13) arts 14.11 and 14.13.
[41] USMCA (n 14) arts 19.11 and 19.12.
[42] Agreement between the United States of America and Japan Concerning Digital Trade (signed 7 October 2019, entered into force 1 January 2020) arts 11 and 12.
[43] Digital Economy Partnership Agreement (signed 12 June 2020, entered into force 7 January 2021) arts 4.3 and 4.4.
[44] Regional Comprehensive Economic Partnership Agreement (signed 15 November 2020, entered into force 1 January 2022) arts 12.14, 12.15 and 12.17.
[45] European Commission, 'Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)' (2018).
[46] Henry Gao, 'Digital or Trade? The Contrasting Approaches of China and US to Digital Trade' (2018) 21 Journal of International Economic Law 297.
[47] Susan Ariel Aaronson and Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 Journal of International Economic Law 245; Susan Ariel Aaronson, 'Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security' (2015) 14 World Trade Review 671.

economy.[48] The counter argument deserves a fair statement. Chander and Lê accept that localisation often has legitimate motives but doubt that it delivers the gains its supporters claim.[49] Industry analysts argue that localisation raises costs and cuts growth.[50] Ferracane shows that restrictions vary widely, from conditional flow rules to outright bans, and that each type has different costs.[51] UNCTAD takes a middle view. It finds that data flows create value but that the gains go mostly to States with the capacity to capture them. It calls for governance that reflects development needs.[52]

Developing regions have started to write their own rules. The African Union adopted a Data Policy Framework in 2022 and the AfCFTA Digital Trade Protocol followed in 2024.[53] The Malabo Convention on cyber security and personal data protection entered into force in 2023.[54] These instruments show that rule making need not follow the CPTPP template.

5. Investment Treaties and Data

Data measures also touch investment law. Most investment treaties protect investments broadly. A data centre, a local subsidiary or a licence can qualify. A localisation order can then be framed as a breach of fair and equitable treatment or as an indirect expropriation.[55] Some newer agreements add another hook. The CPTPP bans performance requirements such as local content and technology transfer. The TRIMs Agreement bans local content requirements that affect trade in goods.[56]

Case law directly on data localisation is thin. Existing awards show how a dispute might go. Tribunals accept that States keep the power to regulate for public welfare. *Saluka* and *Methanex* state the principle that a non-discriminatory regulation adopted in good faith for a public

[48] Thomas Streinz, 'Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy' in Benedict Kingsbury and others (eds), *Megaregulation Contested: Global Economic Ordering After TPP* (OUP 2019).
[49] Chander and Lê (n 3).
[50] Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (Information Technology and Innovation Foundation, 19 July 2021).
[51] Martina F Ferracane, 'Restrictions on Cross-Border Data Flows: A Taxonomy' (ECIPE Working Paper No 1/2017).
[52] UNCTAD, *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow* (United Nations 2021).
[53] African Union, *AU Data Policy Framework* (February 2022); Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade (adopted February 2024).
[54] African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023).
[55] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012).
[56] CPTPP (n 13) art 9.10; Agreement on Trade-Related Investment Measures (adopted 15 April 1994, entered into force 1 January 1995) 1868 UNTS 186, art 2 and Annex para 1(a).

purpose is not compensable expropriation.[57] *Philip Morris v Uruguay* applied it to public health.[58] *Eli Lilly v Canada* rejected a challenge to the way domestic courts applied patent rules.[59] *Tecmed* asked for proportionality between the aim and the burden on the investor.[60] Outcomes therefore turn on treaty wording and on the tribunal. Sornarajah argues that this indeterminacy has historically favoured capital exporters.[61]

India has direct experience. *Deutsche Telekom v India* arose from the cancellation of a satellite spectrum arrangement and produced a finding against India on fair and equitable treatment.[62] *White Industries v India* used the most-favoured-nation clause to import a standard on effective means from another treaty.[63] India then terminated many of its investment treaties and issued a new Model BIT in 2016. The Model uses an enterprise-based definition of investment, narrows the standards of treatment and requires exhaustion of local remedies.[64] It builds regulatory autonomy into the text. Its reach is limited because older treaties often keep operating for years after termination through survival clauses. India also stands apart on investment at the WTO. At MC14 it opposed the Investment Facilitation for Development Agreement, and its trade minister said that India stood alone on the point.[65]

6. Data Localisation and Regulatory Autonomy

Regulatory autonomy means the ability of a State to pursue public goals without treaty limits that it did not accept with full knowledge of their effect. It is often called policy space. Rodrik argues that States need such space to run development strategies and that global rules should leave it in place.[66] Chang shows that today's rich States used tools such as tariffs and technology controls to develop and then discouraged others from doing so. Lang adds that trade law has moved from bargaining over tariffs to disciplining domestic regulation.[67] Data governance sits

[57] *Saluka Investments BV v Czech Republic* (Partial Award) UNCITRAL (17 March 2006); *Methanex Corporation v United States of America* (Final Award) UNCITRAL (3 August 2005).
[58] *Philip Morris Brands Sàrl v Oriental Republic of Uruguay* (Award) ICSID Case No ARB/10/7 (8 July 2016).
[59] *Eli Lilly and Company v Government of Canada* (Final Award) ICSID Case No UNCT/14/2 (16 March 2017).
[60] *Técnicas Medioambientales Tecmed SA v United Mexican States* (Award) ICSID Case No ARB(AF)/00/2 (29 May 2003).
[61] M Sornarajah, *Resistance and Change in the International Law on Foreign Investment* (CUP 2015).
[62] *Deutsche Telekom AG v Republic of India* (Interim Award) PCA Case No 2014-10 (13 December 2017).
[63] *White Industries Australia Ltd v Republic of India* (Final Award) UNCITRAL (30 November 2011).
[64] Government of India, Model Text for the Indian Bilateral Investment Treaty (2016).
[65] 'WTO Debates Five-Year Extension of Global Ban on Ecommerce Tariffs' Business Standard (29 March 2026) <https://www.business-standard.com/amp/economy/news/wto-debates-five-year-extension-of-global-ban-on-ecommerce-tariffs-126032900794_1.html> accessed 29 September 2026.
[66] Dani Rodrik, *The Globalization Paradox: Democracy and the Future of the World Economy* (WW Norton 2011).
[67] Ha-Joon Chang, *Kicking Away the Ladder: Development Strategy in Historical Perspective* (Anthem Press 2002); Andrew Lang, *World Trade Law After Neoliberalism: Reimagining the Global Economic Order* (OUP

at the centre of this shift.

Localisation serves several aims. Privacy and security are the most common. States also seek law enforcement access, tax and supervisory access and local industrial capacity. Each aim has a different legal defence. Privacy and security fit the GATS and treaty exceptions most easily. Industrial aims fit them least. A rule adopted to build a domestic cloud industry looks like protection and will struggle against a necessity test.[68]

Powerful States also restrict data. The European Union limits transfers of personal data unless the destination offers adequate protection or other safeguards apply.[69] The Court of Justice struck down two transatlantic arrangements in *Schrems I* and *Schrems II* because of surveillance concerns.[70] The Commission then adopted a new adequacy decision in 2023.[71] China requires security assessments and local storage for operators of critical information infrastructure and for some transfers of personal information.[72] Russia requires the primary storage of its citizens' data in Russia.[73] More than 160 States now have privacy laws.[74] The point is not that every restriction is wise. The point is that strong States restrict data when they choose and defend the choice as rights protection or security. Developing States face a harder task. They have less bargaining power and less capacity to build the evidence that a tribunal expects.

International human rights law gives a further basis. The right to privacy in the ICCPR and the General Assembly resolution on privacy in the digital age support State action to protect personal data. The Global Digital Compact of 2024 speaks of data governance and of closing digital divides.[75] Some of these instruments are soft law. Their value is interpretive. They can support a reading of exceptions in favour of regulation.

Treaty design matters more than doctrine. Four devices protect autonomy. The first is a broad

2011).

[68] Shin-yi Peng and Han-Wei Liu, 'The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?' (2017) 51 Journal of World Trade 183.

[69] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 44 to 49.

[70] Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650; Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* ECLI:EU:C:2020:559.

[71] Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023] OJ L231/118.

[72] Cybersecurity Law of the People's Republic of China (2016) art 37; Personal Information Protection Law of the People's Republic of China (2021) arts 38 to 40.

[73] Federal Law No 242-FZ of 21 July 2014 on Amending Certain Legislative Acts of the Russian Federation as to Clarification of the Procedure for Personal Data Processing in Information and Telecommunications Networks.

[74] Graham Greenleaf, 'Global Data Privacy Laws 2023: 162 National Laws and 20 Bills' (2023) 181 Privacy Laws & Business International Report 1.

[75] ICCPR (n 9) art 17; UNGA Res 79/1 (22 September 2024) annex I (Global Digital Compact).

exception with self-judging language, as in the RCEP. The second is exclusion from dispute settlement. The third is a schedule of reservations that lets a State list the measures it wants to keep. The fourth is a development clause that gives more time or flexibility. The GATS already holds a version of the fourth device in its provisions on developing country participation and progressive liberalisation.[76] Each device trades predictability for autonomy. A State that wants foreign investment in cloud services must weigh that price.

7. India: Data Localisation and Trade Commitments

7.1 The domestic measures

India has no single localisation law. It has a layer of sectoral rules and a statute that leaves room for more. In 2018 the Reserve Bank of India directed that all payment system data be stored only in India.[77] The Bank later clarified that processing abroad is allowed if the data is deleted abroad and brought back to India within a short period.[78] The insurance regulator requires certain records to be held in India.[79] The CERT-In directions of 2022 require service providers to keep logs within Indian jurisdiction for 180 days.[80] The 2011 rules under the Information Technology Act allow transfer of sensitive personal data abroad if the recipient ensures the same level of protection.[81]

Legislative drafts moved through several stages. The Srikrishna Committee proposed a mirror copy rule for personal data and exclusive storage for critical personal data.[82] The 2018 draft Bill placed these ideas in clause 40.[83] The 2019 Bill softened them in clauses 33 and 34.[84] A Joint Parliamentary Committee reported in 2021 and the Government withdrew the Bill in 2022.[85] The Digital Personal Data Protection Act 2023 took a different course. It permits transfer of personal data abroad except to countries that the Central Government notifies as

[76] GATS (n 17) arts IV and XIX(2).
[77] Reserve Bank of India, Storage of Payment System Data (RBI/2017-18/153, DPSS.CO.OD No 2785/06.08.005/2017-18, 6 April 2018).
[78] Reserve Bank of India, 'FAQs on Storage of Payment System Data' (26 June 2019).
[79] Insurance Regulatory and Development Authority (Maintenance of Insurance Records) Regulations 2015, reg 3(9).
[80] Ministry of Electronics and Information Technology, Directions under Section 70B(6) of the Information Technology Act 2000 relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents (28 April 2022).
[81] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, r 7.
[82] Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology 2018).
[83] Personal Data Protection Bill 2018 (draft), cl 40.
[84] Personal Data Protection Bill 2019 (Bill No 373 of 2019), cls 33 and 34.
[85] Joint Committee on the Personal Data Protection Bill 2019, *Report* (Lok Sabha Secretariat, December 2021). The Government withdrew the Bill in August 2022.

restricted, and it keeps stricter sectoral laws in force.[86] The Rules notified on 13 November 2025 add two features. Rule 15 makes transfers subject to requirements the Government may set on access by foreign States and their agencies. Rule 13 requires significant data fiduciaries to ensure that specified personal data and related traffic data are not transferred outside India.[87] Two policy strands show the wider intent. The draft National e-Commerce Policy of 2019 treated data as a national resource and proposed limits on sending Indian data abroad.[88] The Non-Personal Data committee proposed community rights over data.[89] Both texts frame data as a development asset. That framing matches the critique of digital colonialism. The domestic anchor is *Puttaswamy*, where the Supreme Court recognised privacy as a fundamental right and set a test of legality, legitimate aim and proportionality for State intrusions.[90]

Critics doubt whether localisation delivers its promised gains. Bailey and Parsheera argue that the case for localisation is weak on security and enforcement grounds and that storage in India does not by itself create local value or protect privacy.[91] Basu, Hickok and Chawla map the justifications and find them uneven.[92] These are policy points, but they matter for law. A weak fit between aim and measure makes a necessity defence harder.

7.2 The external commitments

India has taken selective positions. It has made GATS commitments in sectors that matter for digital trade, including financial services. Their scope varies by mode and must be read entry by entry.[93] India is not a party to the CPTPP or the USMCA. It left the RCEP negotiations in November 2019 and cited unresolved concerns.[94] It did not join the Osaka Track on data free flow.[95] It stays outside the e-commerce JSI and disputes its legality. The United States has listed Indian localisation rules among trade barriers.[96]

---

[86] Digital Personal Data Protection Act 2023 (India), ss 16 and 17.
[87] Digital Personal Data Protection Rules 2025, GSR 846(E) (13 November 2025), rr 13 and 15. Rule 15 is due to take effect on 13 May 2027.
[88] Department for Promotion of Industry and Internal Trade, *Draft National e-Commerce Policy: India's Data for India's Development* (2019).
[89] Ministry of Electronics and Information Technology, *Report by the Committee of Experts on Non-Personal Data Governance Framework* (2020).
[90] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
[91] Rishab Bailey and Smriti Parsheera, 'Data Localisation in India: Questioning the Means and Ends' (NIPFP Working Paper No 242, 2018).
[92] Arindrajit Basu, Elonnai Hickok and Aditya Singh Chawla, *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India* (Centre for Internet and Society 2019).
[93] WTO, India: Schedule of Specific Commitments GATS/SC/42 (15 April 1994).
[94] Ministry of External Affairs (India), 'Statement by Prime Minister at the 3rd RCEP Summit' (4 November 2019).
[95] G20, 'Osaka Declaration on Digital Economy' (28 June 2019).
[96] Office of the United States Trade Representative, *2019 National Trade Estimate Report on Foreign Trade Barriers* (2019) (India section).

7.3 Legal analysis

Three GATS questions arise for the payment data rule. The first is coverage. The rule touches financial services, so India's commitments there define the exposure. The second is discrimination. The RBI rule applies to all providers. A complainant would say that it hits foreign firms harder because they run global processing systems. De facto discrimination can suffice under the national treatment rule.[97] The third is justification. India could invoke the prudential carve-out on the ground that the rule supports supervisory access. It could also invoke Article XIV on privacy and public order. Each argument needs proof that the measure is necessary and that less restrictive tools such as access agreements would not work. *Argentina: Financial Services* shows the risk when a State cannot supply that proof.[98]

The DPDP Act raises a different issue. A list of restricted countries is a country-specific measure. Article II of the GATS requires most-favoured-nation treatment among Members. It applies whether or not a State has made commitments, unless the State listed an exemption.[99] A notification that blocks transfers to some Members and not others could be challenged in sectors that the GATS covers. India would then rely on Article XIV or Article XIV bis. The security exception, as read in *Russia: Traffic in Transit*, gives India room if the notification rests on real security grounds.[100] A list built on trade or industrial grounds would be harder to defend. The design of the notification process is therefore a legal matter and not only an administrative one.

Rule 13 is narrower. It targets significant data fiduciaries and only the data that the Government specifies. That targeting improves the necessity case because it ties the measure to risk. It also weakens a discrimination claim because the criteria concern the data and the fiduciary and not the nationality of the supplier. The main risk lies in the delegation. The categories are set later, so a future order could be broad.

Investment law adds a second layer. Older treaties that remain in force protect foreign-owned data centres and payment operators against unfair treatment and expropriation. Tribunals give States space for good faith regulation but they also look for stability and transparency. The Indian record in telecommunications suggests that abrupt change is the main risk.[101]

Litigation risk should not be overstated. The Appellate Body has been unable to function since

[97] GATS (n 17) art XVII(3).
[98] *Argentina: Financial Services* (n 25).
[99] GATS (n 17) art II(1).
[100] *Russia: Traffic in Transit* (n 28).
[101] *Deutsche Telekom v India* (n 62).

December 2019. India lost the ICT tariffs dispute at the panel stage in 2023 and then appealed.[102] A State can use that route against an adverse ruling. The real pressure comes from other channels. The United States has raised localisation in its trade barrier reports and in bilateral talks. These channels work through bargaining power and not through adjudication. That is the situation that the digital colonialism argument describes. The argument also cuts the other way. India is a large exporter of IT services and has its own stake in open data flows. In its case autonomy and access pull in opposite directions.

8. Towards a Development-Sensitive Framework

Three lessons follow. First, India and other developing States should move from ad hoc localisation to principled rules. A framework built on access and accountability is easier to defend than one built on storage location. Conditions such as mirror copies, contractual access commitments and audit rights can meet security and enforcement aims with less restriction on trade. The OECD declaration on government access shows that States can agree on principles for lawful access.[103] That reduces the security case for blanket localisation. Where localisation is needed it should be narrow, sector-specific and backed by public evidence. India should also publish the criteria for any notification of restricted countries.

Second, treaty drafting needs care. Exceptions must be wide enough to protect regulatory choices. Schedules should list existing measures as reservations. Self-judging exceptions and exclusion from dispute settlement work for the State that uses them but they weaken predictability, and partners will price that risk. India's Model BIT and its WTO positions show a steady preference for policy space. It should test that preference against the value of predictable rules for its own digital exporters. The lapse of the moratorium sharpens this point. Once the e-commerce agreement takes effect its parties will be bound to a duty-free rule among themselves.[104] Non-participants may face duties on their software and digital content exports if partners choose to impose them.

Third, collective action offers more than isolated resistance. The African Union framework and the AfCFTA protocol show how a region can set shared standards on data. South-South coordination lets developing States negotiate as a bloc and reduces the pressure of bilateral

[102] Panel Report, *India: Tariff Treatment on Certain Goods in the Information and Communications Technology Sector* WT/DS582/R (17 April 2023).
[103] OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities (14 December 2022).
[104] Digital Watch Observatory (n 38).

talks. A parallel path is to move data governance discussions to forums where developing States have more voice, such as the United Nations process that produced the Global Digital Compact. UNCTAD has called for global data governance that reflects development needs.[105]

9. Conclusion

Digital colonialism is more than a metaphor when it is traced through the rules of international economic law. Those rules do not assign ownership of data. They protect the assets that surround data, limit the policy tools of States and spread template rules through trade agreements. The effect is a system in which control of data follows control of infrastructure and capital.

The picture is not one-sided. Open data flows bring real benefits to developing economies. Powerful States restrict data too. The WTO exceptions and the arbitral case law leave real room for regulation. The problem is the cost of using that room. It falls on States with less capacity and less bargaining power.

India illustrates both sides. Its localisation measures rest on genuine privacy, security and development aims. Their legal position is defensible in parts and exposed in others. The negative list in the DPDP Act and the payment data rule raise the sharpest questions. India's best course is to build rules on access and accountability, to keep localisation narrow and evidence-based and to work with other developing States on treaty design. The lapse of the WTO moratorium shows that the rules are unsettled. That gives developing States a moment to shape them.

[105] UNCTAD (n 52).