

Data Sovereignty and Cross-Border Data Flows: An International Commercial Law Perspective

Weidong Zhang

North University of China

Corresponding author email: zhang1690846956@163.com

Abstract

Assertive claims of data sovereignty—mandatory localization, extraterritorial processing rules, and security-driven exclusion of foreign access—now sit in direct tension with the data flows on which cross-border commerce depends. The dominant scholarly treatment of this tension proceeds through the lens of fundamental rights and surveillance law. This article proceeds instead from international commercial law: the body of World Trade Organization law and preferential trade agreements, private international law, commercial contract regimes, and dispute-resolution instruments that govern transnational business dealings. The article first develops a taxonomy of data-sovereignty claims and shows why, as a matter of legal structure, such claims operate not as dominion over data itself but as jurisdiction over persons and infrastructure. It then maps the three principal regulatory models—the European Union's rights-based unilateralism, the United States' market-driven default with security-driven edges, and China's security-development dualism—together with the collisions among them. Against the developments of 2024–2026, including the expiry of the WTO customs-duty moratorium, the interim arrangements for the WTO Agreement on Electronic Commerce, the unsettled USMCA joint review, the EU Digital Omnibus proposal, and the recalibration of China's export-review thresholds, the article evaluates how trade law disciplines the *form* of data-sovereignty measures while leaving their substance intact, and how contract, choice-of-law, and arbitration regimes have become carriers of public regulatory law. It closes with a framework for reconciling regulatory competence with data mobility: differentiation by data type and risk, interoperable recognition mechanisms, and a rebuilt private-law infrastructure for data transactions.

Keywords: data sovereignty; cross-border data flows; digital trade; data localization; GDPR; standard contractual clauses; private international law; WTO; data governance

1. Introduction

Consider a transaction that has become ordinary. A multinational enterprise operating enterprise-resource-planning software for its subsidiaries in Germany, the United States, and China synchronizes a database containing customer records, employee information, and telemetry from industrial equipment. Four bodies of law attach to the movement of that database, and each asserts a different command. Regulation (EU) 2016/679 (the GDPR) conditions the export of personal data on Chapter V transfer mechanisms and, by Article 48, refuses recognition of third-country authority orders absent an international agreement such as a mutual legal assistance treaty. The Clarifying Lawful Overseas Use of Data (CLOUD) Act obliges US-based providers to disclose data within their possession, custody, or control regardless of storage location. China's Data Security Law, Article 36, and Personal Information Protection Law (PIPL), Article 41, prohibit provision of data to foreign judicial or law-enforcement authorities without approval of the competent Chinese authority. And the

US Department of Justice's Data Security Program, codified at 28 C.F.R. Part 202, prohibits or restricts covered transactions that would make bulk sensitive personal data accessible to jurisdictions designated as countries of concern. No architecture of compliance can satisfy all four commands simultaneously in every configuration; the enterprise can only sequence its exposure, contract around the margins, and litigate the residue.

This configuration—the collision of regulatory claims over the same transborder data—is conventionally analyzed as a problem of constitutional law, human rights law, or international security. That literature is substantial and necessary, but it is incomplete for commercial actors and their counsel, because the operative disciplines that structure most cross-border data movements are not constitutional texts. They are the General Agreement on Trade in Services (GATS) and the new generation of digital trade chapters; the standard contractual clauses that carry much of the lawful traffic in EU personal-data exports; the Rome I Regulation and the Hague instruments on choice of law and judgments; and the arbitration clauses embedded in cloud, data-processing, and joint-venture agreements. This article addresses the data-sovereignty problem from the standpoint of this body of international commercial law, understood as the law governing cross-border trade and business transactions: multilateral and plurilateral trade law, private international law, transnational contract law, and the institutions of commercial dispute resolution.

Three developments in 2024–2026 make the question newly urgent, and newly tractable. First, at the World Trade Organization (WTO), the moratorium on customs duties on electronic transmissions—renewed continuously since 1998—lapsed at the Fourteenth Ministerial Conference in March 2026 when members could not agree on extension, while the Joint Statement Initiative on electronic commerce produced a stabilized text in July 2024 that, after the withdrawal of the United States from its core data-flow commitments, was carried forward through interim arrangements adopted on 28 March 2026 by a group of approximately 66–67 members (WTO, 2024; WTO, 2026). Second, the United States, historically the chief proponent of free-data-flow disciplines, has turned selective restrictor: the Data Security Program took full effect in 2025, the divest-or-ban statute upheld in *TikTok Inc. v. Garland* (2025) survived constitutional review, and at the USMCA joint review on 1 July 2026 the United States declined to confirm the 16-year extension, placing the strongest operational data-flow commitments inside the most unsettled trade agreement in the system (White & Case, 2026). Third, the two states most associated with restrictive regimes have each begun to differentiate: China's Cyberspace Administration of China (CAC) lowered its export-review thresholds and authorized free-trade-zone negative lists in March 2024, with Beijing and Shanghai relaxing those lists further in 2026, and India's final Digital Personal Data Protection Rules of 13 November 2025 adopted a negative-list transfer model under which no country has yet been listed (CAC, 2024; Legal 500, 2026).

The argument proceeds in five stages. Section 2 disentangles the concept of data sovereignty, tracing its genealogy and proposing a four-part taxonomy of the claims actually made under its banner, and shows that data sovereignty operates as jurisdiction over persons and infrastructure rather than dominion over data as a res. Section 3 maps the three principal regulatory models and their secondary variants, and constructs the collision matrix that any reconciliation must address. Section 4 evaluates the trade-law channel: what GATS and the new plurilateral and preferential instruments discipline, and what they deliberately leave to regulatory discretion. Section 5 examines the private-law channel—contract, choice of law, and dispute resolution—through which public regulatory norms now travel across borders. Section 6 draws the strands together into a framework for reconciling regulatory competence with data mobility, and Section 7 concludes.

The article's contributions are threefold. Descriptively, it offers a taxonomy of data-sovereignty claims that maps each claim type onto the commercial-law discipline that in fact governs its incidence. Doctrinally, it analyzes the 2024–2026 transformation of the digital trade architecture—the expiry of the moratorium, the

interim arrangements for the Agreement on Electronic Commerce, the USMCA review, the EU Digital Omnibus proposal (COM(2025) 837), and the recalibration of Chinese and Indian transfer regimes—much of which post-dates the existing literature. Normatively, it defends a position that is unfashionable in both the sovereignty and the free-flow camps: the conflict is not between sovereignty and its absence, but between two allocations of regulatory competence, and international commercial law's realistic promise is not to abolish data sovereignty but to discipline its form—through necessity and non-arbitrariness review, risk-based differentiation, and interoperable recognition—while private law quietly supplies the operational infrastructure that keeps data commerce functional.

2. Data Sovereignty: Concept, Claims, and Legal Structure

2.1. A genealogy

"Sovereignty" entered the data-governance vocabulary from three distinct directions. The first is an extension of the Westphalian state's claim to regulate within its territory to the informational layer of that territory. On this account, which entered Chinese doctrine as 网络主权 (network sovereignty) and Russian practice as the "sovereign internet," the state asserts the same authority over data flows crossing its borders that it asserts over goods, services, and capital (Goldsmith and Wu, 2006; Mueller, 2017). The second direction is resource sovereignty: the analogy between data and the natural resources over which the 1962 General Assembly Resolution on Permanent Sovereignty over Natural Resources asserted national control, an analogy now explicit in Chinese policy documents treating data as a "factor of production" (生产要素) subject to allocation and pricing by the state. The third direction, chronologically first, is the claim of Indigenous peoples to govern the collection and use of data about themselves, articulated in the Indigenous data sovereignty movement (Kukutai and Taylor, 2016); this usage grounds collective authority over data in the interests of data subjects rather than of states, and has been partially absorbed into mainstream governance through the language of "data colonialism" critique. A fourth, European usage—"digital sovereignty" and "technological sovereignty"—is less a territorial claim than a strategic one: the capacity of the Union to act autonomously in the digital sphere, expressed through instruments such as the Data Governance Act and the gatekeeping provisions of the Digital Markets Act (Bradford, 2020).

These lineages share a word but not a claim. It is analytically useless to ask whether "data sovereignty" is, in the abstract, good or bad; the operative question is what specific legal claims are asserted under its banner, and how those claims interact with the obligations states have assumed in their commercial-law instruments.

2.2. A taxonomy of claims

Four ideal types capture the claims actually litigated, negotiated, and legislated under the label of data sovereignty. Table 1 summarizes the taxonomy with representative instruments and the commercial-law discipline each claim principally engages.

Table 1. Four types of data-sovereignty claims and their commercial-law touchpoints

Claim type	Content	Representative instruments	Principal commercial-law touchpoint
Territorial storage (localization)	Data of category X must be stored/processed within the state's territory	China, Cybersecurity Law (2017), art. 37; Russia, Law No. 242-FZ (2014); Vietnam, Decree 53/2022/ND-CP	GATS market access and national treatment; FTA computing-facility provisions (CPTPP art. 14.13; RCEP art. 12.14; USMCA art. 19.12)

Claim type	Content	Representative instruments	Principal commercial-law touchpoint
Regulatory jurisdiction (extraterritoriality)	Processing rules attach to data or actors regardless of where processing occurs	GDPR arts. 3(2), 44–50; PIPL art. 3(3); US CLOUD Act (2018)	Private international law (Rome I art. 9; overriding mandatory rules); blocking statutes; comity analysis
Protective exclusion	Foreign access to defined data categories is prohibited or heavily conditioned	EO 14117 and 28 C.F.R. pt. 202 (2025); Protecting Americans from Foreign Adversary Controlled Applications Act (2024); PIPL art. 41; DSL art. 36	Investment protection (fair and equitable treatment, expropriation); national-security exceptions in FTAs and GATS art. XIV bis
Developmental resource control	Data generated in the territory is a strategic economic asset whose value must be captured domestically	China's data-element policies; data-center local content requirements; EU Data Act access and switching rules	Industrial-policy disciplines; government procurement; EU state aid law

The taxonomy cuts across the conventional "three models" mapping developed in Section 3: every major regulator makes claims of more than one type. The European Union disclaims localization yet asserts sweeping extraterritorial jurisdiction; the United States champions free flows in trade negotiations while operating the most aggressive protective-exclusion program among democratic states; China pairs strict territorial controls with an active bid to accede to the very agreements (DEPA, CPTPP) that constrain such controls.

2.3. Why data sovereignty cannot be dominion over data

As a matter of legal structure, sovereignty claims over data fail the tests that make resource sovereignty coherent. Data is non-rivalrous: one state's "consumption" of data does not preclude another's. Data is delocalized by design: a dataset in a cloud environment exists simultaneously as compute instances, replicas, backups, and derived caches in multiple jurisdictions, and the "location" of any copy says little about where the data can be accessed. Data moves at negligible cost and near-instantaneously, so border controls must operate on persons and infrastructure—controllers, processors, carriers, cloud consoles, authentication systems—rather than on the data itself. Daskal (2015) demonstrated the resulting "un-territoriality of data": the geographic markers that anchor regulatory jurisdiction (where the server is, where the user is, where the controller is established) come apart, and each marker generates a different, overlapping jurisdictional claim. Kuner (2013) showed that transborder data flow law has, since the 1970s, always been a proxy war: states regulate transfers not because data crossing a border is intrinsically dangerous, but because the transfer is an administrable moment at which domestic regulatory projects—privacy, security, industrial policy—can be enforced.

The consequence, which frames everything that follows, is that "data sovereignty" in operation is never sovereignty over data. It is jurisdiction over the actors and facilities of data commerce: over the enterprise that decides to export, the cloud provider whose infrastructure carries the export, the certification body that validates the export, and the contract that authorizes it. That is precisely why international commercial law—with its doctrines on jurisdiction, necessity, recognition, and contractual obligation—is not one lens among many but the law of the battlefield itself.

3. Three Regulatory Models and the Fragmentation of Data Governance

3.1. The European Union: rights-based unilateralism and the adequacy system

The EU model rests on a single organizing idea: personal data may leave the European Economic Area only if the destination ensures a level of protection "essentially equivalent" to that of the GDPR—a formula the Court of Justice entrenched in *Schrems* (Case C-362/14, 2015) and *Schrems II* (Case C-311/18, 2020). Chapter V operationalizes the idea through three doors: adequacy decisions under Article 45 (currently covering Andorra, Argentina, Canada (commercial), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom, Uruguay, and—for certified entities—the United States); appropriate safeguards under Article 46, in practice the 2021 standard contractual clauses (Commission Implementing Decision (EU) 2021/914) and binding corporate rules; and narrow derogations under Article 49.

Three features of the model matter for commercial law. First, the Court has converted private contract documents into carriers of constitutional review. In *Schrems II*, the Court invalidated the EU–US Privacy Shield, upheld the clauses while subjecting them to a case-by-case "essentially equivalent" audit, and imposed on exporters a duty to verify, suspend, or terminate transfers when the destination's surveillance law undermines the clauses (paras 121, 135, 143). The Irish Data Protection Commission's decision of 22 May 2023 applied that duty at scale: a record €1.2 billion fine on Meta and an order to suspend EU–US transfers. The European Data Protection Board's Recommendations 01/2020 then obliged every exporter to perform transfer impact assessments—documentary diligence that functions as a private-law replica of the Court's adequacy analysis.

Second, adequacy has become a geopolitical instrument. The current EU–US Data Privacy Framework (Commission Implementing Decision (EU) 2023/1795) survived its first annulment challenge when the General Court dismissed *Latombe v Commission* (Case T-553/23, 2025) on 3 September 2025, but the framework rests on US executive commitments and FISA Section 702, whose April 2024 reauthorization (RISAA) expired on paper in April 2026 without successor legislation; collection under existing orders continues into 2027 under the statute's tail provision while reauthorization talks proceed (Brennan Center, 2026). The durability of adequacy is thus hostage to another state's domestic intelligence politics—an instability the model exports to every commercial relationship structured around it. The renewal of the UK adequacy decisions on 19 December 2025 until December 2031, following the UK's Data (Use and Access) Act 2025, shows the system functioning as intended: extraterritorial regulatory discipline delivered through market-access conditionality.

Third, the Union is differentiating rather than retreating. The Data Act (Regulation (EU) 2023/2854), whose substantive obligations became applicable on 12 September 2025, regulates third-country government access to non-personal industrial data held in the Union (Article 33) and thereby extends the adequacy logic beyond personal data. The Digital Omnibus proposal of 19 November 2025 (COM(2025) 837)—still before the Council and Parliament as of this writing—would streamline international transfer mechanisms, narrow the GDPR's material scope, and recalibrate enforcement, in response to concerns about European competitiveness (Latham & Watkins, 2025; ICLE, 2026). Whatever its final shape, the direction is procedural simplification of transfers, not abandonment of the essentially-equivalent standard.

3.2. The United States: market default, security edges

The US model has no comprehensive federal data-privacy statute; sectoral statutes (HIPAA, GLBA), the state-law patchwork led by the California Consumer Privacy Act, and the First Amendment's constraints on regulation define the domestic baseline. For cross-border flows the operative architecture is inverted: the default is freedom of movement, policed at the edges by national-security law. Four instruments define the edges. The CLOUD Act (2018) resolves *Microsoft Corp. v. United States* (829 F.3d 197 (2d Cir. 2016)) by

compelling US providers to disclose data in their control regardless of location while authorizing executive agreements for partner-state direct requests—agreements concluded with the United Kingdom and Australia. Executive Order 13873 (2019) and its implementing ICTS rules screen information-and-communications-technology transactions involving "foreign adversaries." Executive Order 14117 (2024) and the Data Security Program (28 C.F.R. Part 202, effective 8 April 2025) prohibit or restrict transactions giving China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, or Venezuela access to bulk US sensitive personal data—genomic, biometric, health, geolocation, financial data, and specified personal identifiers above volume thresholds—with due-diligence, audit, and reporting obligations phasing in through October 2025 (US Department of Justice, 2025). And the Protecting Americans from Foreign Adversary Controlled Applications Act (2024), upheld in *TikTok Inc. v. Garland* (2025), mandates divestiture of foreign-adversary-controlled applications; enforcement was repeatedly deferred by executive order during 2025 while divestiture negotiations continued.

The commercial-law significance of the American turn is profound: the state that wrote the free-data-flow provisions of CPTPP, USMCA, and the US–Japan and US–Korea digital agreements no longer supports them. In October 2023 the US Trade Representative withdrew support for the data-flow, localization, and source-code disciplines it had itself tabled in the WTO e-commerce negotiations (USTR, 2023), and the United States subsequently stood apart from the interim arrangements adopting the Agreement on Electronic Commerce (Section 4.2). The direction of American policy—free flow for allies' data, exclusion for adversaries' access—converges, from the opposite ideological direction, on the same selective model China operates.

3.3. China: security-development dualism and its recalibration

China's framework is statutory, comprehensive, and organized around two lists: the inventory of protected categories (personal information; "important data"; state secrets and core data) and the inventory of permitted export channels. The Cybersecurity Law (2017), Article 37, requires critical information infrastructure operators to store personal information and important data collected in China within China and to pass a CAC security assessment for export. The Data Security Law (2021) extends the architecture to all data handlers by Article 36's approval requirement for provision to foreign judicial or law-enforcement authorities, and Article 21's classification system. The PIPL (2021) supplies three export channels for personal information—CAC security assessment, certification, and the CAC standard contract (Articles 38–40)—alongside extraterritorial reach over offshore processing of Chinese residents' data where connected to offering goods and services to them (Article 3(3)) and a mirror of the blocking rule (Article 41).

Since March 2024 the system has been materially recalibrated toward facilitation. The CAC's Provisions on Promoting and Regulating the Cross-Border Flow of Data (22 March 2024) exempted transfers below defined volumes (broadly, non-sensitive personal information of fewer than 100,000 individuals per year, outside the critical-infrastructure class), created a presumption that data not officially notified as "important data" need not be exported as such, and authorized free-trade zones to adopt negative lists—data outside the list transfers freely with post-hoc filing. Tianjin published the first full-range negative list in May 2024; Beijing and Shanghai relaxed their lists in 2026 (Reed Smith, 2026). The State Council's Regulations on Network Data Security Management (Decree No. 790, effective 1 January 2025) consolidated the facilitation while tightening operational obligations. In parallel, China applied in 2021 to join CPTPP and DEPA; its DEPA accession working group has met since August 2022, with the tenth chief-negotiators round in April 2026 described by participants as entering a critical stage (MOFCOM, 2026). The recalibration is best read not as liberalization for its own sake but as a bid to make the Chinese regime interoperable with—while remaining distinct from—the disciplines of the agreements it seeks to join; Chander and Lê (2015) identified the underlying dynamic a decade ago as "data nationalism" managing its own costs.

3.4. Secondary movers

Russia pairs the oldest localization mandate—Law No. 242-FZ (2014), requiring the initial recording of Russians' personal data on domestic servers—with the 2019 Sovereign Internet Law's deep-packet-inspection infrastructure. India's Digital Personal Data Protection Act 2023 replaced the older sectoral approval regime with Section 16's negative-list model: transfers are permitted except to countries the Central Government notifies; the final Rules of 13 November 2025, adopted with phased commencement, leave the list empty for now, while sectoral localization (payments, banking) persists (Legal 500, 2026; Scrut.io, 2025). Vietnam's Decree 53/2022/ND-CP mandates localization on the request of the cybersecurity authority; Brazil's LGPD follows the EU's channel logic, with the ANPD's Resolution No. 19/2024 approving standard contractual clauses. The aggregate picture is fragmentation with a convergent grammar: virtually every major jurisdiction now operates a licensing system for data exports, differing in scope, thresholds, and institutional design (OECD, 2022; Ezell and Cory, 2021).

3.5. The collision matrix

Table 2 constructs the principal direct conflicts. Each row is a configuration in which compliance with one regime is, in the ordinary case, incompatible with compliance with another; each has produced or will produce concrete commercial disputes.

Table 2. Principal regulatory conflicts in cross-border data governance

Conflict pair	Governing norms	Nature of the conflict	Existing resolution channel
US compelled disclosure vs. EU transfer discipline	CLOUD Act, 18 U.S.C. § 2713; GDPR arts. 44–48	Prohibition (EU) vs. compulsion (US) over the same data movement	CLOUD Act executive agreements (UK, Australia); comity analysis; data-segmentation architecture
US compelled disclosure vs. Chinese blocking	CLOUD Act; DSL art. 36; PIPL art. 41	Compulsion vs. criminal prohibition of compliance	None operative; waiver practice; exit from one market
EU adequacy system vs. US exclusion program	GDPR ch. V; 28 C.F.R. pt. 202	EU conditions export on destination-state protection; US conditions transactions on data categories and counterparties	Parallel compliance; neither regime recognizes the other
Chinese export review vs. FTA disciplines	PIPL arts. 38–40; CPTPP arts. 14.11, 14.13; RCEP art. 12.15	Domestic approval regimes vs. treaty commitments not to restrict transfers	Not yet litigated; prospective CPTPP accession discipline
State surveillance access vs. private contract	FISA § 702; SCCs 2021/914, clauses 15–16 (notice, suspension)	State practice can render contractual undertakings impossible, triggering suspension duties	Transfer impact assessment; suspension; forum re-routing

The matrix demonstrates the point on which Section 6 builds: the conflicts are not between a sovereign and a state of nature, but between two regulatory jurisdictions each asserting competence over the same transaction through different legal instruments. That is the classic configuration international commercial law exists to manage.

Tracing the introductory ERP scenario through the matrix shows how the conflicts are actually worked out in practice—and at what cost. The German subsidiary's employee data cannot be pooled with the American

database under standard contractual clauses alone if the US provider is an "electronic communication service provider" within FISA Section 702: the clauses require a transfer impact assessment, and *Schrems II* litigation plus the Data Privacy Framework's contested durability mean the assessment's conclusion depends on US surveillance law that changed twice between 2024 and 2026. The Chinese telemetry cannot be synchronized at all without CAC assessment or free-trade-zone negative-list coverage, and once stored in China it cannot be produced in response to a US grand jury subpoena without exposing the enterprise to liability under Article 36 of the Data Security Law. The customer records, if they include bulk precise geolocation or health data of US persons, cannot be processed by any Chinese subsidiary of the group without a prohibited covered transaction under the Data Security Program. Each edge of the matrix is thus resolved not by a rule of priority but by an engineering decision: segment the data, regionalize the architecture, and license the residual. Data sovereignty has thereby already restructured the physical topology of global commerce—independent analyses count at least 144 localization measures in force across the world's economies as early as 2021, a number that has grown since (Ezell and Cory, 2021; OECD, 2022)—and commercial law's task is to make that restructuring disciplined rather than escalatory.

4. The Trade-Law Channel: Disciplining the Form of Data Sovereignty

4.1. The WTO baseline and the end of the moratorium

Within the WTO architecture, data flows are disciplined as trade in services. The supply of a data-processing, cloud-computing, or software-as-a-service offering from one territory to another is a mode 1 (cross-border supply) service falling within scheduled commitments on computer and related services and value-added telecommunications; measures restricting data export or conditioning it on local infrastructure engage market access (GATS Article XVI), national treatment (Article XVII), and domestic regulation (Article VI) to the extent of the schedule. The 1998 Work Programme on Electronic Commerce established that framework's application to digital supply, and members have maintained since 1998 a moratorium on customs duties on electronic transmissions. That moratorium lapsed at MC14 in March 2026 when members declined to extend it—the first interruption since the regime's creation, freeing members in principle to impose duties on electronic transmissions while leaving the practical incidence of any such duties uncertain (ORF, 2026).

The deeper question is the exception architecture. A localization or export-approval measure will typically be defended under GATS Article XIV(a) (public morals, which panels have accepted can embrace data privacy) and increasingly under Article XIV bis (essential security interests). The necessity analysis in *China—Electronic Payment Services* (WT/DS413/R, Panel Report, adopted 2012) supplies the template: China failed to demonstrate that its measures favouring UnionPay were necessary, given reasonably available less trade-restrictive alternatives. The necessity test thus disciplines the *fit* between a data-sovereignty measure and its declared objective, not the objective itself. Article XIV bis, rendered more salient by the post-2022 security environment and by the Appellate Body's paralysis, introduces a self-judging dimension that could swallow much of the discipline if read expansively; the digital-trade cases that would test the boundary have not yet been brought.

4.2. The Agreement on Electronic Commerce: plurilateral law after the American exit

The Joint Statement Initiative on Electronic Commerce, launched in 2017 by a coalition of WTO members, produced a stabilized text on 26 July 2024 (INF/ECOM/87): the first multilateral instrument addressing, among other matters, cross-border data flows, computing-facility location, source code, electronic authentication, and consumer protection. Its data-flow article follows the CPTPP formula: parties may maintain restrictions pursued for a legitimate public policy objective, provided the restrictions are not applied in an arbitrary or unjustifiable manner and do not restrict trade more than necessary. After the October 2023

US withdrawal from the data-flow, localization, and source-code provisions and its subsequent disengagement from the JSI, a revised text was sponsored on 24 November 2025, and on 28 March 2026 some 66–67 members—representing roughly 70% of world trade—adopted a Declaration on Interim Arrangements (WT/MIN(26)/42) under which the Agreement on Electronic Commerce will operate among accepting parties, entering into force thirty days after certification of sufficient acceptances, pending its contested incorporation into the WTO legal framework (Hinrich Foundation, 2026; Global Data Alliance, 2026; WTO, 2026).

The Agreement's legal character is precisely the interesting part. It is open plurilateralism as necessity: institutionalized cooperation outside the consensus multilateral track, in the institutional form (a declaration on interim arrangements) that trade law historically reserves for precisely such moments. For data sovereignty, the Agreement is a floor, not a ceiling: it disciplines arbitrary discrimination and unnecessary restrictiveness while expressly preserving public-policy space broad enough to cover the GDPR, the PIPL, and the Data Security Program alike. Its longer-run force will depend on whether the European Union participates (its adequacy system creates a standing objection to treating free flow as the default) and on whether the disciplines harden into dispute settlement with teeth.

4.3. Preferential agreements: from CPTPP's high-water mark to the unsettled USMCA

The operative disciplines today are preferential. CPTPP Articles 14.11 and 14.13 prohibit, respectively, restrictions on cross-border transfers of information by electronic means, including personal information, and requirements to use or locate computing facilities in the territory as a condition of market access—subject to exceptions for legitimate public policy objectives and, for computing facilities, financial regulatory measures. The United Kingdom's accession, in force on 15 December 2024 and between the UK and all other parties by 1 September 2026, extended the discipline and, for the first time, subjected a G7 economy's data-governance regime to it. USMCA Articles 19.11 and 19.12 tighten the CPTPP text marginally while carving out a broader financial-regulatory exception, and Article 19.13 narrows source-code protection relative to CPTPP. RCEP Articles 12.14 and 12.15 reproduce the structure with materially more flex: transition periods for developing parties, an explicit financial-regulatory exception, and a public-policy exception that has been read against the backdrop of ASEAN's regulatory diversity. The DEPA (2020), now extending beyond its Chile–New Zealand–Singapore founders (the Republic of Korea has acceded; eight aspirants including China and Canada are in the queue), modularizes the enterprise: data flows, digital identities, artificial-intelligence governance, and data innovation are separate modules parties can adopt at different depths (Burri and Polanco, 2020).

Two structural observations follow. First, the strongest texts sit in the most fragile containers. At the USMCA joint review on 1 July 2026, the United States declined to confirm the sixteen-year extension; the agreement now proceeds through annual reviews toward its 2036 sunset unless renewed, with renegotiation rounds continuing into September 2026 (White & Case, 2026; USTR, 2026). The lesson commercial actors have drawn—that data-flow commitments are reversible political facts rather than settled law—is itself a governance cost. Second, the European Union has deliberately stayed outside this architecture: the EU's FTAs contain no data-flow chapters, because the Union treats the adequacy system, not market access, as the governing frame. The result is a world in which the trade-law discipline of data sovereignty is regional and variable, with CPTPP, DEPA, RCEP, and the EU's adequacy network each policing a different perimeter (Aaronson, 2019).

4.4. What trade law actually disciplines

Across all four instruments, the pattern is consistent. Trade law does not, and will not in any foreseeable text, prohibit data-sovereignty regulation as such. What it disciplines is form: measures must be transparent, non-discriminatory in application, not arbitrary or unjustifiable, and not more trade-restrictive than necessary, with least-restrictive-alternative reasoning supplied by panels' necessity jurisprudence. The essential contest in

every future dispute—over a localization mandate, an export-approval regime, or a bulk-data prohibition—will be whether the general exceptions clause absorbs the measure. That contest is winnable on both sides, which is precisely why the plurilateral floor matters: it converts data-sovereignty conflict from an unreviewable assertion into a justiciable claim.

Two structural gaps in the trade-law channel deserve emphasis. The first is the absence of any challenge practice. No localization measure has been tested before a WTO panel or an FTA tribunal, despite the breadth of scheduled commitments on computer and related services. The explanation is economic, not doctrinal: the claimant must be a government willing to spend political capital against a regulatory fashion most members share; the defendant's most likely defense—Article XIV bis security—now travels through an appellate machinery that has been paralyzed since 2019, so even a favorable panel report risks cycling unadopted into the void; and exporters damaged by localization are usually the same firms that fear retaliation in the defendant's procurement and licensing decisions. The consequence is that the discipline exists on paper while the practice of data sovereignty develops in a litigation vacuum—an unstable equilibrium that the interim Agreement on Electronic Commerce may eventually disturb, provided its participants resolve the dispute-settlement question its stabilized text left open.

The second gap is the adequacy system's status in trade law. The GDPR conditions market access for data services on a unilateral, discretionary finding of essential equivalence that no FTA disciplines and no WTO schedule constrains; from a trade-law standpoint, the adequacy decision functions as a recognition regime—which trade law has always treated as tolerable in principle yet reviewable when applied arbitrarily. Were the European Union ever to become a party to a data-flow instrument, the negotiated question would be precisely this: whether adequacy findings become subject to necessity-style review, or whether the Union's recognition system remains a law-free zone inside the trading system. The Union's refusal, to date, to accept data-flow commitments in its own FTAs—the EU–Japan and EU–Korea agreements are silent on data flows precisely because adequacy is the Union's preferred instrument—signals that it understands the stakes exactly (Aaronson, 2019; Burri and Polanco, 2020).

5. The Private-Law Channel: Contract, Choice of Law, and Dispute Resolution

5.1. Standard contractual clauses as regulatory infrastructure

The most consequential commercial-law development in this field is doctrinally unglamorous: the migration of public regulatory law into standard-form contract. The EU's 2021 standard contractual clauses (Decision 2021/914) do not merely allocate private risk; they embed the entire *Schrems II* constitutional analysis in contractual obligations—the exporter's transfer impact assessment, the parties' warranties about government-access laws, the importer's notice and challenge duties, and—most striking—the obligation to suspend or terminate transfers when effective protection cannot be ensured (clauses 14–16). After *Schrems II* and the EDPB's Recommendations 01/2020, signing the clauses without a documented assessment is itself an infringement. The United Kingdom's International Data Transfer Addendum, China's CAC standard contract (with mandatory filing), and Brazil's ANPD-approved clauses (Resolution 19/2024) replicate the technique. A single multinational data-processing arrangement may thus require the EU clauses for European personal data, CAC filing for Chinese personal information, and Data-Security-Program due diligence for US bulk sensitive data—three public-law regimes, each carried into operation by a private contract instrument.

The doctrinal significance is that contract has become the interface layer of the data-sovereignty system: the moment at which abstract regulatory conflict is converted into allocable private obligations, warranties, indemnities, and suspension rights. Practice has internalized the point—data-processing agreements now routinely include government-access notification covenants, flow-down clauses, audit rights over

subprocessors, and re-transfer conditions that track the clauses' architecture. The scholarly label for the phenomenon—transnational private ordering—is accurate but understates the direction of travel: it is public law that is doing the ordering, through private forms (Kuner, 2013; Schwartz, 2019).

5.2. Choice of law and the limits of party autonomy

Private international law manages, without resolving, the clash of public policies. Parties to a cross-border data transaction enjoy broad choice-of-law freedom under the Rome I Regulation (Article 3) and the Hague Principles on Choice of Law in International Commercial Contracts (2015). But that freedom is bounded by overriding mandatory provisions (Rome I, Article 9(1)): provisions whose observance a forum regards as crucial—into which category data-protection regimes are routinely placed, with the GDPR's own Article 3 asserting territorial and targeting jurisdiction regardless of the chosen law. The practical consequence is a characteristic asymmetry: for non-personal industrial and commercial data, party autonomy is close to complete, and governing-law, jurisdiction, and transfer-annex clauses function predictably; for personal data, the chosen law governs the commercial shell while the mandatory regime of every affected jurisdiction governs the data itself. The Data Act's Article 33 extends the mandatory-clipper technique to non-personal data, conditioning third-country government access on treaty basis and proportionality. Choice of law thus allocates which forum's coercive law applies to which limb of the transaction—an incidence rule, not a conflict rule in the classic sense (Svantesson, 2023).

5.3. Jurisdiction, judgments, and the enforcement mesh

Forum fragmentation compounds the problem. Brussels Ia governs EU-side jurisdiction over controllers and processors; US courts assert personal jurisdiction over US-directed processing businesses; Chinese courts over China-collected data. Judgments circulate badly: the 2019 Hague Judgments Convention, in force since 1 September 2023 (for the UK from 1 July 2025; Albania and Montenegro from 1 March 2026; Andorra from 1 June 2026), excludes from its scope matters relating to privacy, including defamation (Article 5(2)(b))—the drafters' concession to speech-protective jurisdictions that has the incidental effect of leaving the growing volume of data-protection judgments outside the only general enforcement instrument. The United States signed the Convention in 2022 but has not ratified it. Recognition of foreign data-regulatory orders therefore proceeds through the older, thinner channels—comity analysis, MLATs under the Hague Evidence Convention (with its Article 23 reservations), and the CLOUD Act's executive-agreement track—alongside the EU's European Production Order Regulation (2023/1543), applicable from August 2026, which authorizes direct orders to providers regardless of location and will itself collide, on its face, with blocking statutes.

5.4. Arbitration and investment protection

Commercial arbitration is emerging as the quiet workhorse of data-commerce disputes: cloud supply agreements, data-processing arrangements, and platform partnerships are arbitrable in the ordinary way, and their disputes—breach of transfer conditions, subprocessor failures, regulatory suspension—turn on contract law carrying embedded public norms. Arbitration's virtues here are practical: neutrality, confidentiality (itself a data-protection asset), and enforceability under the New York Convention in 170-plus states. Its structural limit is that an award binds the parties, not the regulator; an arbitration cannot set aside a CAC assessment order or a Data Security Program prohibition.

Investment law reaches the regulator, and data infrastructure is squarely covered investment: data centers, cable landing stations, and platform operations are assets in which foreign investors hold protected interests. Localization mandates adopted without transition, abrupt divestiture orders of the PAFACA type, and denial-of-access measures are all candidate fair-and-equitable-treatment and indirect-expropriation claims, subject to the essential-security carve-outs most treaties contain and to the policy legitimate expectations doctrine will

accord regulatory sovereignty. No data-localization ISDS award has yet been published; the likelihood that one will, as enforcement of the newer exclusion programs bites foreign investors, is a disciplining consideration in itself.

The arbitration channel also has a doctrinal soft spot worth naming: the public-policy exception to enforcement. An award compelling a party to execute a data transfer that a mandatory regime prohibits will meet resistance at the recognition stage under Article V(2)(b) of the New York Convention, since enforcement contrary to the forum's data-protection or blocking rules is now routinely characterized as contrary to public policy. The prudent structuring consequence is familiar to commercial lawyers: data-transfer obligations belong in the contract's substance—conditions, alternatives, suspension rights—rather than in bare performance orders an arbitrator will eventually be asked to compel, because compulsion is the point at which the private-law channel breaks against the public-law wall.

6. Reconciling Sovereignty and Flows: A Commercial-Law Framework

6.1. Reframe the object: allocation, not dominion

The framing deadlock—sovereignty versus free flow—dissolves once Section 2's structural point is taken seriously. Data sovereignty is not a claim over a resource but an assertion of regulatory competence over persons and infrastructure, and the question international commercial law answers in every other domain of contest (financial services, telecommunications, competition) is not *whether* states regulate across borders but how competences are allocated and reciprocal overreach is disciplined. The analogy to the general exceptions architecture of the GATT and GATS is exact: the trading system never required deregulation; it required regulation of a certain form—non-discriminatory, transparent, necessary. A defensible settlement for data follows the same logic.

6.2. Differentiate by data type and risk

Every significant regulatory movement of 2024–2026 is, in substance, a differentiation move: China's volume thresholds and important-data presumption; India's empty negative list; the US program's category-specific bulk thresholds; the Data Act's separate, lighter track for non-personal data; the Digital Omnibus's attempt to rationalize transfer mechanisms. The commercial insight these systems are converging on is that most cross-border business data is either non-personal or low-risk personal data, for which licensing is pure friction, while a narrow band—biometric, genomic, geolocation, government-linked, bulk aggregated—carries the security and dignity risks that justify control. A framework that codifies this convergence—free flow for non-personal and sub-threshold personal data by default, tiered authorization for the sensitive band, mutual recognition of each other's tiering—would capture most of the gains both camps claim, and would be administrable through the contract infrastructure of Section 5.1 already in place (OECD, 2022; Global Data Alliance, 2023).

6.3. Institutionalize interoperability

Differentiation needs institutions. Four building blocks exist and require only connection. The plurilateral floor—the interim arrangements for the Agreement on Electronic Commerce—supplies the necessity-and-non-arbitrariness baseline among its parties. The recognition layer can bridge the EU adequacy system and the Global CBPR Forum (established 2022) into interoperable certification rather than competing exclusions; the EU–Japan mutual adequacy and the UK's dual-hatted status (adequacy plus CBPR participation) prove the bridge is buildable. The due-regard layer is the OECD's 2022 Declaration on Trusted Government Access, which specifies legality-necessity-proportionality ground rules for cross-border government access—precisely the *Schrems II* variable—and could be incorporated by reference into MLATs, CLOUD Act agreements, and

the e-evidence order regime. And the deconfliction layer—modernized mutual legal assistance replacing the Article 48 GDPR / CLOUD Act / Article 36 DSL triangle with designated-authority channels—is the single highest-value technical fix available, because it addresses the conflicts in Table 2 that private ordering cannot reach.

6.4. Rebuild the private-law infrastructure deliberately

The final component is to treat the private-law channel as infrastructure to be designed rather than residue to be tolerated. UNCITRAL's instruments—the Model Law on Electronic Commerce (1996), the Convention on the Use of Electronic Communications in International Contracts (2005), and the Model Law on Electronic Transferable Records (2017)—keep trade documents functional across jurisdictions and should extend to data-transaction default rules. Model data clauses for supply, processing, and joint-venture agreements—building on the 2021 clauses' architecture but generalized beyond personal data—would lower transaction costs that currently function as a tax on cross-border commerce. And dispute-resolution design—arbitration for the contractual layer, the 2019 Judgments Convention for the enforcement mesh (notwithstanding its privacy exclusion), investment discipline for the regulatory layer—completes the allocation. None of this requires a new global treaty; all of it requires treating data commerce as what it is: the ordinary business of international commercial law.

6.5. Objections and limits

Three objections to the framework deserve direct answers. The first is the fragmentation-realist objection: the world is consolidating into rival data blocs, each internally integrated and externally guarded, and no reconciliation framework survives that geopolitics (Mueller, 2017). The objection correctly describes the direction of the American and Chinese programs but mistakes bloc formation for the absence of law. Blocs trade with each other; the very instruments that divide them—the adequacy list, the Data Security Program's exemptions, the negative lists—are recognition rules, and recognition rules are the raw material of interoperability regimes, not their negation. The nineteenth-century gold standard, the mid-century Bretton Woods arrangements, and today's equivalence regimes in financial regulation all emerged from exactly this configuration of guarded blocs seeking transactional efficiency.

The second objection is the security-exception objection: any necessity-and-non-arbitrariness discipline can be swallowed by essential-security clauses, which recent FTA practice and the post-2022 WTO disputes suggest states increasingly treat as self-judging. The objection has force, but it proves less than it claims. Security exceptions protect security measures, and most of the measures documented in Section 3—volume thresholds, certification schemes, contractual filing, adequacy review—are administration, not security, measures; states defend them as privacy or regulatory measures because that is what they are. The genuine security core—bulk exclusion of adversary access—is narrower, and even there, the framework's demand is modest: designated-authority channels and proportionality review, not free flow.

The third objection comes from the opposite camp: any risk-tiered system entrenches surveillance categories and legitimizes controls once presented as exceptional. The concern is real, but the alternative is not the absence of controls—it is the current unreviewable licensing sprawl, whose chief casualties are the smallest commercial actors, who cannot segment architectures or maintain three parallel compliance programs. A tiered system with necessity review at least subjects each control to a justification burden, which is the most any exceptions architecture in trade law has ever achieved.

7. Conclusion

The data-sovereignty debate has been misdescribed as a collision between states and a borderless technology. It is better understood as a classic conflict of regulatory competences over a new class of transactions, conducted through the oldest instruments commercial law possesses: conditions on market access, exceptions clauses, mandatory rules, standard contracts, and forums for dispute. The developments of 2024–2026—the lapsed WTO moratorium, the interim Agreement on Electronic Commerce, the unsettled USMCA review, the American turn to selective exclusion, the European attempt at internal recalibration, and the Chinese and Indian moves toward differentiated transfer regimes—do not add up to fragmentation alone. They add up to a system groping, unevenly and without coordination, toward exactly the settlement commercial law has offered every previous generation of contested cross-border flows: sovereignty exercised in allocable form, disciplined by necessity and non-arbitrariness, differentiated by risk, and operationalized through contract. The task for international commercial lawyers is not to lament the absence of a global data regime but to assemble one from the instruments already at hand.

Author Contributions

Withheld for double-anonymous review; to be completed by the corresponding author before publication.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable: this article is doctrinal legal research and involved no human subjects.

Informed Consent Statement

Not applicable: this article is doctrinal legal research and involved no human participants.

Data Availability Statement

No new datasets were generated. All sources relied upon are publicly available legal instruments, case law, and publications cited in the References.

Conflicts of Interest

The author declares no conflict of interest.

References

- Aaronson, S.A. 2019. What are we talking about when we talk about digital protectionism? *World Trade Review*, 18(4), 583–607.
- Agreement on Electronic Commerce (stabilized text, WTO Doc. INF/ECOM/87, 26 July 2024); Declaration on Interim Arrangements for the Agreement on Electronic Commerce, WTO Doc. WT/MIN(26)/42 2026.
- Bradford, A.U. 2020. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press.
- Brennan Center for Justice 2026. Section 702 surveillance authority will not lapse if reauthorized by March 2027. New York: Brennan Center for Justice.
- Burri, M., & Polanco, R. 2020. Digital trade provisions in preferential trade agreements: Introducing a new dataset. *Journal of International Economic Law*, 23(1), 187–220.

Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Schrems (Schrems II)*, ECLI:EU:C:2020:559 (16 July 2020).

Case C-362/14, *Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650 (6 October 2015).

Case T-553/23, *Latombe v Commission*, General Court of the European Union (3 September 2025).

Chander, A., & Lê, U.P. 2015. Data nationalism. *Emory Law Journal*, 64, 677.

China—Certain Measures Affecting Electronic Payment Services, WT/DS413/R and WT/DS413/AB/R (adopted 31 August 2012).

Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 348 (2018) (codified 18 U.S.C. §§ 2713, 2523).

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries.

Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 (EU–US Data Privacy Framework adequacy).

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018), arts. 14.11, 14.13, 29.1.

Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, art. 5(2).

Convention on the Use of Electronic Communications in International Contracts (New York, 2005).

Cybersecurity Law of the People's Republic of China (2017), art. 37; Data Security Law (2021), arts. 21, 36; Personal Information Protection Law (2021), arts. 3, 38–43.

Cyberspace Administration of China (CAC) 2024. *Provisions on Promoting and Regulating the Cross-Border Flow of Data* (promulgated 22 March 2024). Beijing: CAC.

Cyberspace Administration of China, *Provisions on Promoting and Regulating the Cross-Border Flow of Data* (22 March 2024); *Regulations on Network Data Security Management* (State Council Decree No. 790, effective 1 January 2025).

Daskal, J. 2015. The un-territoriality of data. *Yale Law Journal*, 125(2), 326–398.

Digital Personal Data Protection Act 2023 (India), s. 16; Digital Personal Data Protection Rules 2025 (notified 13 November 2025).

European Commission 2025. Proposal for a Digital Omnibus Regulation, COM(2025) 837 final (19 November 2025).

European Data Protection Board 2021. *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (version 2.0, adopted 18 June 2021).

Executive Order 14117 of 28 February 2024; US Department of Justice, Data Security Program, 28 C.F.R. Part 202 (effective 8 April 2025).

Ezell, S., & Cory, N. 2021. *A Global View of Barriers to Cross-Border Data Flows*. Washington, DC: Information Technology and Innovation Foundation.

General Agreement on Trade in Services, arts. III, VI, XVI, XVII, XIV, XIV bis.

General Data Protection Regulation (EU) 2016/679, arts. 3, 44–50.

Global Data Alliance 2023. *Cross-Border Data Policy Index*. Washington, DC: Global Data Alliance.

Global Data Alliance 2026. 67 WTO members advance plurilateral Agreement on Electronic Commerce. Washington, DC: Global Data Alliance.

- Goldsmith, J.L., & Wu, T. 2006. *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.
- Hinrich Foundation 2026. How 66 (or is it 67?) WTO members are trying to unblock the e-commerce deal. Singapore: Hinrich Foundation.
- International Center for Law & Economics (ICLE) 2026. Analysis of the Digital Omnibus proposal's progress in the Council. Portland, OR: ICLE.
- Irish Data Protection Commission 2023. Decision in inquiry concerning data transfers from the EU/EEA to the USA by Meta Platforms Ireland (22 May 2023).
- Kukutai, T., & Taylor, J. (eds.) 2016. *Indigenous Data Sovereignty: Toward an Agenda*. Canberra: Australian National University Press.
- Kuner, C. 2013. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press.
- Latham & Watkins 2025. Digital Omnibus: EU Commission proposes to streamline digital regulation. Client Alert (27 November 2025).
- Legal 500 2026. Cross-border data transfers under India's DPDP Act.
- Microsoft Corp. v United States*, 829 F.3d 197 (2d Cir. 2016); *United States v Microsoft Corp.*, 584 U.S. ____ (2018) (vacated as moot).
- Ministry of Commerce of the People's Republic of China (MOFCOM) 2026. Coverage of the chief negotiators' meetings on China's accession to the DEPA. Beijing: MOFCOM.
- Mueller, M. 2017. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge: Polity Press.
- Observer Research Foundation (ORF) 2026. Duties on data: WTO MC14 and the digital dilemma. New Delhi: ORF.
- Organisation for Economic Co-operation and Development (OECD) 2022. *A Preliminary Mapping of Data Localisation Measures*. Paris: OECD.
- Organisation for Economic Co-operation and Development 2022. *Declaration on Government Access to Personal Data Held by Private Sector Entities* (adopted 14 December 2022). Paris: OECD.
- Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H 2024.
- Reed Smith 2026. Beijing and Shanghai update negative list regimes for cross-border data transfers. Client Alert (May 2026).
- Regional Comprehensive Economic Partnership Agreement (2020), arts. 12.14–12.15.
- Regulation (EC) No. 593/2008 on the Law Applicable to Contractual Obligations (Rome I), arts. 3, 9.
- Regulation (EU) 2022/868 (Data Governance Act); Regulation (EU) 2023/2854 (Data Act), art. 33; Regulation (EU) 2023/1543 (European Production Orders).
- Schwartz, P.M. 2019. Global data privacy: The EU way. *New York University Law Review*, 94, 771.
- Scrut.io 2025. India's DPDP Rules 2025: Cross-border transfer under Rule 15.
- Svantesson, D.J.B. 2023. *Extraterritoriality and Targeting in Data Privacy Law*. Oxford: Oxford University Press.
- TikTok Inc. v. Garland*, 604 U.S. ____ (17 January 2025).
- US Trade Representative (USTR) 2023. Statement on e-commerce negotiations at the World Trade Organization (24 October 2023).

US Trade Representative (USTR) 2026. Joint statement following the USMCA joint review meeting (1 July 2026).

US–Mexico–Canada Agreement (2018), arts. 19.11–19.13.

White & Case 2026. USMCA 2026 joint review: United States declines to confirm extension. Trade Alert (2 July 2026).

World Trade Organization (WTO) 2024. Joint Statement Initiative on Electronic Commerce: Stabilized text, INF/ECOM/87 (26 July 2024). Geneva: WTO.

World Trade Organization (WTO) 2026. Members discuss preparations to bring the E-Commerce agreement forward (9 June 2026). Geneva: WTO.

WTO, Work Programme on Electronic Commerce, WT/L/274 (1998); Ministerial decisions on the moratorium on customs duties on electronic transmissions (1998–2024); Thirteenth Ministerial Conference outcome 2024.