



RESEARCH ARTICLE

The New Law of Digital Trade: Electronic Contracts, Data Flows and Cross-Border Commerce under Emerging International Legal Frameworks

Muhammad Jahanzaib Aslam¹

Muhammad Maaz Shakeel²

¹ LLM Scholar, University of Stirling, Stirling, Scotland, UK. Email: mjahanzaibaslam1122@gmail.com

² LLM Scholar, Postgraduate School of Legal Studies, University of Punjab, Pakistan. Email: maaz.shakeel35@gmail.com

ARTICLE HISTORY

Received 12-03-2026

Accepted 11-08-2026

Published 05-10-2026

KEYWORDS

digital trade; electronic contracts; electronic signatures; electronic transferable records; paperless trade; data flows; UNCITRAL; WTO Agreement on Electronic Commerce; platforms; private international law; consumer protection; Pakistan

CORRESPONDING AUTHOR

Muhammad Maaz Shakeel

maaz.shakeel35@gmail.com



<https://doi.org/10.68740/jjil22>

ABSTRACT

The article considers whether existing international legal regimes can sufficiently regulate data-driven cross-border commerce without the need for a single, overarching digital-trade code. Using a doctrinal and comparative method, it examines five jurisdictions – the United Kingdom, Australia, Canada, India and Pakistan – across four functional dimensions: electronic contracting and authentication; electronic transferable records; cross-border data governance; and platform, consumer and cross-border redress. The analysis distinguishes binding international obligations from model laws, domestic legislation, preferential trade agreements and new institutional work. It contends that the international legal framework has not developed in a uniform manner. The UNCITRAL Model Law on Electronic Commerce, the Model Law on Electronic Signatures and related domestic legislation provide for a relatively high degree of functional equivalence for electronic communications and signatures. Paperless trade has advanced with the Model Law on Electronic Transferable Records, but implementation is uneven and interoperability remains a network issue. Data-driven commerce presents a unique challenge. While trade agreements may discipline some constraints on cross-border data flows, privacy and sectoral regulation tend to be domestic and create legally salient interfaces with trade commitments. Platform liability, consumer jurisdiction and cheap cross-border redress are even less harmonised. The article concludes with an argument that the current framework is best understood as a layered and function-specific system. The main contribution is an analytical framework to evaluate legal capability by the function a rule performs and the legal layer from which that rule derives. The comparison also indicates that domestic implementation, interoperability and institutional capacity are as important for the practical governance of digital trade as the existence of international instruments.

1. INTRODUCTION

Digital trade is often discussed as if it were a single area of law. In practice, a cross-border digital transaction may comprise an electronically concluded contract, an electronic transferable record, personal data crossing borders, a platform intermediary, a payment system, intellectual property rights, and rules on which court or regulator has jurisdiction. These elements are legally linked but not governed by one instrument. The key question, therefore, is not whether law exists for digital trade, but to what extent existing international and domestic legal systems are able to perform the different functions required by data-driven commerce.

The research question is: How far can existing international legal systems govern data-driven cross-border commerce? For this purpose ‘existing’ refers to treaties in force, model laws, domestic legislation implementing international standards, preferential trade agreements and international instruments adopted but not yet in force. ‘Regulate’ is used in a functional sense. The article asks four questions: can the legal system (a) create and authenticate transactions; (b) give legal effect to transferable electronic trade documents; (c) govern cross-border data flows in a way that accommodates privacy and other public interests; and (d) provide rules for platform relationships, jurisdiction, consumer protection and redress.

The article makes two related points. First, the legal architecture is layered. UNCITRAL model laws require domestic enactment; treaties create obligations only for their parties; preferential trade agreements create more detailed commitments for their parties; and emerging instruments may have persuasive or prospective significance without yet constituting binding law. Second, capability is function specific. The international framework is fairly well developed for electronic contracting and developing for transferable records, but much less integrated for data as commercial subject matter, platform governance and low-value cross-border redress.

It compares the United Kingdom, Australia, Canada, India and Pakistan in particular. These jurisdictions are not statistically representative of world digital trade. They are chosen because they offer a useful legal comparison across systems with substantial common-law or common-law influenced commercial traditions, but differ significantly in their adoption of electronic-trade legislation, privacy frameworks, paperless-trade rules and digital-trade commitments. So the comparison is doctrinal, not empirical.

An example of the evolution of the field is the work of UNCITRAL. The Model Law on Electronic Commerce adopted the principles of non-discrimination, technological neutrality and functional equivalence as the fundamental values for electronic communications and transactions. The Model Law on Electronic Signatures contained provisions on reliability and recognition of signatures. The Model Law on Electronic Transferable Records provided functional equivalence of documents whose legal operation traditionally depended upon possession or exclusive control (UNCITRAL, 1996, 2001, 2017). UNCITRAL Working Group IV is currently engaged in developing model legislative provisions on contracts for the supply of data and is also considering the broader consolidation of its electronic-commerce texts (UNCITRAL, 2026).

The WTO track is something else. The Agreement on Electronic Commerce was concluded through the Joint Statement Initiative and, after MC14 in March 2026, 67 WTO members agreed to interim arrangements to facilitate the agreement’s entry into force among participating members while its incorporation into the WTO legal framework remains under discussion. Under the Agreement’s terms, its entry into force requires 45 instruments of acceptance (WTO, 2026a, 2026b). It should therefore not be described as a code binding on all members across the WTO.

The differences matter at the domestic level as well. The UK has passed the Electronic Trade Documents Act 2023. Australia is working toward uniform amendments in accordance with MLETR. Canada has a multi-tiered system of electronic transactions and privacy. India has long

recognised electronic records and signatures and the Digital Personal Data Protection Rules 2025 have now been notified with phased commencement. Pakistan has the Electronic Transactions Ordinance 2002, PECA as amended, sectoral regulation and an e-commerce policy framework, but no enacted comprehensive personal-data protection statute or MLETR-equivalent legislation (Pakistan Code, 2002; Ministry of IT & Telecommunication, 2023; Ministry of Commerce, 2025).

The contribution of the article is therefore analytical and not predictive. It proposes a framework of capabilities, layered by function, for assessing digital-trade regulation. The framework does not claim to be an established category of international law. It is an interpretive device to explain how apparently conflicting assessments of digital-trade governance can both be true: a legal system may be very capable of validating an electronic contract while being ill-equipped to govern data ownership, platform liability or cross-border consumer redress.

2. METHODOLOGY AND ANALYTICAL FRAMEWORK

This is a doctrinal study of comparative law. The doctrinal component defines the legal status, scope and interaction of international instruments, model laws, national statutes and selected trade commitments. Primary sources are preferred. In the comparative section, the same functional questions are asked for each jurisdiction: (1) electronic contracting and signatures; (2) transferable electronic trade documents; (3) personal and non-personal data governance; (4) platform and consumer regulation; and (5) international digital-trade commitments and cross-border dispute mechanisms.

The jurisdictions were purposively, rather than statistically, selected. The United Kingdom is an example of a mature common-law commercial system with a dedicated electronic trade-document statute. Australia has a federal system, is a key stakeholder in digital-trade negotiations and is also working on legislation in line with the MLETR. Canada is an example of the interaction of federal and provincial laws. India has long-standing electronic-transaction laws and a recently notified data-protection regime. Pakistan is an example of a system in which electronic transactions and e-commerce policy have developed in the absence of a comprehensive personal-data statute and a specific electronic-transferable-records statute.

The study does not measure enforcement frequency, trade volumes, business costs, judicial outcomes or compliance rates. Therefore it is not in a position to determine that one jurisdiction is economically more successful than another. The figures included in this article are heuristic illustrations only. Their numerical values are not reported as empirical results, as no replicable scoring methodology underlies them.

The analytical framework differentiates four legal layers. The first layer is binding international law—treaties and agreements that are in force for the relevant parties. The second layer is made up of model laws and legislative standards, which are not automatically binding because they have been adopted by UNCITRAL or another international body. The third layer is made up of domestic law enacted by individual jurisdictions. Layer four consists of emerging projects, draft texts and policy instruments that could influence future law, but do not yet have the legal status of enacted rules. The distinction is important so that one does not treat a model law, a draft working paper and a treaty as equivalent sources.

Within those layers, the article uses ‘capability’ in a narrow legal sense: whether the relevant rules are capable of performing a particular regulatory function. It does not mean that the rules are necessarily efficient, fair or economically useful. This distinction makes it possible to assess the international framework more accurately, without transforming the article into an empirical regulatory-impact study.

3. THE INTERNATIONAL LEGAL ARCHITECTURE OF DIGITAL TRADE

3.1 UNCITRAL Electronic Commerce Instruments

The UNCITRAL Model Law on Electronic Commerce 1996 is still a key instrument. Its principles of non-discrimination, technological neutrality and functional equivalence overcome the legal barriers that arise when legislation assumes paper, handwritten signatures or physical originals. It also contains rules concerning electronic contract formation, attribution, acknowledgements of receipt, and the time and place of dispatch and receipt (UNCITRAL, 1996). UNCITRAL reports that a large number of jurisdictions have adopted legislation based on or inspired by the Model Law, although the extent of national implementation varies.

That framework is supplemented by the Model Law on Electronic Signatures 2001, which deals with issues of technical reliability, conduct of signatories and relying parties, and recognition of foreign certificates and signatures (UNCITRAL, 2001). What makes these instruments legally significant is their function: They provide legislative techniques by which domestic law can remove formal obstacles to electronic transactions. They do not, as such, unify substantive contract law, evidence law or consumer protection.

The 2005 United Nations Convention on the Use of Electronic Communications in International Contracts puts similar principles into treaty form for its States Parties. As of the date of the present article, UNCITRAL has 21 States Parties. The Convention is therefore significant but cannot be regarded as a universal treaty framework for the five jurisdictions studied here (UNCITRAL, 2005). But the difference between a treaty and a model law is important: UNCITRAL's legislative texts can influence a State without the Convention binding it.

3.2 Electronic Transferable Records and Paperless Trade

The 2017 Model Law on Electronic Transferable Records deals with a more complicated problem than ordinary electronic contracting. Transferable instruments, such as a bill of lading or a bill of exchange, may require possession, uniqueness, and transferability of control as a matter of law. Therefore, the MLETR is based on functional equivalence based on identification, control and integrity rather than stating that a digital copy is the equivalent of paper (UNCITRAL, 2017).

Domestic enactment is uneven. The current status list of UNCITRAL identifies legislation based on or influenced by MLETR in 13 States or jurisdictions including the United Kingdom, France, Singapore, China, the United Arab Emirates and others (UNCITRAL, 2026a). The Electronic Trade Documents Act 2023 (United Kingdom) is particularly important because it grants the legal effects of paper documents to qualifying electronic trade documents when the conditions of the reliable-system statute are met (Electronic Trade Documents Act 2023, 2023).

Australia illustrates the networked nature of paperless trade. The Attorney-General's Department said the Commonwealth, states and territories agreed in November 2025 to develop national model amendments consistent with the MLETR. As of September 2026, this is still in the legislative preparation stage rather than passed national MLETR legislation (Attorney-General's Department, 2026).

Thus, one domestic enactment does not solve the legal problem. A transferable electronic document is only useful if the relevant carrier, financing party, registry and destination jurisdiction recognise the legal concept of control. So the international framework has an interoperability problem as well as a legislative problem. MLETR has also been considered in recent scholarship as a useful harmonising device whose success depends on adoption and compatibility across trading corridors (Anyamele, 2024).

3.3 Data as Commercial Subject Matter

Data creates another legal problem because, unlike a physical object, data can be copied without the transfer of a unique physical object. A contract might be about access to a data set, continuous data feeds, machine generated data, data quality, permitted uses or restrictions on onwards transfer. The UNCITRAL Working Group IV has been working on model legislative provisions on contracts for the provision of data and, in 2026, on the passive provision of data and the consolidation of electronic-commerce texts (UNCITRAL, 2026b).

The current project is not yet law binding everywhere. Its importance is forward-looking and legislative: it aims to identify default contractual rules which can reduce uncertainty when parties trade data. Recent scholarship has explored the connection between UNCITRAL's proposed rules on data provision and existing regimes that govern digital content, noting that the project is one of many in a broader discussion on contractual classification and regulatory overlap (Šafranko, 2024).

The data also show the limitations of functional equivalence. An electronic signature can be used to perform the function of a signature in writing and a controlled electronic record can be used to perform the function of possession. Neither technique allows us to determine who owns a dataset, whether a data subject has privacy rights, whether an algorithm is allowed to use the dataset, or whether a regulator is allowed to restrict its transfer. Those questions require a lot of private and public law.

3.4 WTO Agreement on Electronic Commerce and the Post-MC14 Position

Another layer of the architecture is the WTO Agreement on Electronic Commerce. The WTO materials talk about it as a baseline set of global digital-trade rules, but the legal position in September 2026 has to be carefully stated. Negotiations were concluded in 2024; 67 members adopted a pathway through interim arrangements at MC14 in March 2026; and participating members continue to seek incorporation of the Agreement into the WTO legal framework. The Agreement itself enters into force upon the deposit of 45 instruments of acceptance, subject to its terms (WTO, 2026a, 2026c).

Thus, the Agreement cannot be seen as binding WTO law for all members. Its practical significance depends on acceptance and operation of the interim arrangements. The distinction is especially pertinent to India and Pakistan who questioned the institutional arrangements for the E-Commerce Agreement in the WTO General Council in July 2026 (WTO, 2026d).

The issue of customs duties must also be dissociated from the Agreement. A long-standing WTO moratorium on customs duties on electronic transmissions expired on 30 March 2026 when members failed to agree a multilateral consensus to renew it. Conversely, the E-Commerce Agreement contains a customs duty commitment offer by the participating parties. The two developments are related but not legally the same (WTO, 2026e).

3.5 Preferential Agreements, Data Flows and Regulatory Autonomy

More detailed digital-trade disciplines than the multilateral system have evolved in several areas within preferential trade agreements, such as electronic authentication, paperless trading, cross-border data flows, location of computing facilities and online consumer protection. For example, Australia's digital-trade strategy describes the country's aim to facilitate data flows while preserving policy space for privacy and other public interests (Department of Foreign Affairs and Trade, 2026).

The resultant legal tension is not simply 'free trade versus privacy'. Modern digital trade agreements often contain exceptions, carve-outs, non-conforming measures or other mechanisms

to retain regulatory autonomy. The legal question is how these mechanisms relate to the substantive commitment. Recent scholarship has placed regulatory autonomy at the center of digital-trade agreements, rather than treating data-flow liberalisation as an unconditional rule (Burri & Kugler, 2024).

The parties to preferential commitments are still bound by their treaty obligations. They should not be called customary international law or rules of universal application. Their relevance for the comparative analysis is that they are examples of how States have sought to balance the openness of digital markets with privacy, consumer protection and other public policy objectives.

4. ELECTRONIC CONTRACTS, AUTHENTICATION AND TRANSFERABLE RECORDS

The legal recognition of the electronic contracts is now relatively mature in the jurisdictions studied. But maturity should not be confused with uniformity. UNCITRAL's functional-equivalence framework eliminates the fundamental formal objection to electronic records. Excluded transactions, evidentiary requirements, consumer safeguards, signature technologies and consequences of authentication failures continue to be determined by national law (UNCITRAL, 1996, 2001).

India's Information Technology Act 2000 provides for recognition of electronic records and electronic signatures and contracts through electronic means. Australia's Electronic Transactions Act 1999 provides a federal framework under which transactions are not invalid simply because electronic communications were used and permits specified legal requirements concerning writing, signatures, documents and retention to be satisfied electronically (Information Technology Act 2000, 2000; Electronic Transactions Act 1999, 1999).

Pakistan's position needs to be handled with care. Electronic documents, records, communications and transactions are given legal recognition under the Electronic Transactions Ordinance 2002. The Ordinance also deals with writing, originals, retention and electronic signatures (Electronic Transactions Ordinance 2002, 2002). PECA has a clear role to play, particularly in relation to cyber offences and related regulatory powers. Treating PECA as Pakistan's principal electronic-commerce statute therefore obscures the more relevant commercial legislation.

The UK's Electronic Trade Documents Act 2023 is more important for paperless trade than for ordinary contract formation. Electronic trade documents are defined by reference to a reliable system that can identify, protect against unauthorised alteration and exclusively control. Qualifying electronic trade documents are given effects equivalent to paper documents (Electronic Trade Documents Act 2023, 2023).

Evidence is still a significant boundary. Recognition of an electronic record does not, in itself, harmonise evidentiary procedure, authentication of foreign records, discovery, or admissibility standards. The international framework is therefore stronger at removing formal invalidity than at ensuring uniform litigation outcomes.

5. CROSS-BORDER DATA FLOWS AND THE TRADE-PRIVACY INTERFACE

Cross-border data flows demonstrate why digital trade cannot be reduced to electronic contracting. Trade agreements may protect certain cross-border data transfers or limit unjustified localisation; domestic privacy law may impose conditions on transfers of personal information. The legal issue is thus one of coordination: the same transaction can be subject both to a trade obligation and a privacy obligation, without either instrument automatically displacing the other.

The United Kingdom is a case in point. International transfers of personal information under the UK GDPR are subject to the transfer rules, which include adequacy regulations, appropriate safeguards and specified derogations. The current guidance of the Information Commissioner's Office confirms that restricted transfers must meet one of those legal routes (Information Commissioner's Office, 2026). Where digital-trade commitments exist, such domestic privacy requirements still remain.

Australia also pairs privacy regulation with digital trade commitments. Under APP 8 of the Australian Privacy Principles, there is a framework for cross-border disclosure where an APP entity must, generally, take reasonable steps in relation to an overseas recipient and can remain accountable for certain acts or practices of that overseas recipient (Office of the Australian Information Commissioner, 2025).

Canada's privacy architecture is more federal-provincial than is often assumed. PIPEDA applies to organisations that engage in commercial activities within its scope, and substantially similar provincial laws apply in British Columbia, Alberta and Quebec and other sectoral regimes apply in specific contexts (Office of the Privacy Commissioner of Canada, 2026). Where provincial legislation is otherwise relevant, federal privacy requirements may continue to engage cross-border transactions.

India's Digital Personal Data Protection Act 2023 and Rules 2025 introduce a phased regime. The Rules were notified in November 2025, with some provisions effective immediately, consent-manager provisions after one year and most substantive obligations after 18 months. The principal cross-border transfer regime is therefore not accurately described as fully operational in September 2026; the relevant substantive phase is scheduled for 13 May 2027 (Ministry of Electronics and Information Technology, 2025).

Pakistan does not have a comprehensive personal data protection law. The Ministry of IT and Telecommunication continues to refer to the Personal Data Protection Bill as a draft legislative instrument. That is not to say that Pakistan has no regulation at all related to data: different aspects of the digital economy are covered by sectoral rules, telecom regulation, electronic-transaction law, cybercrime law and e-commerce policy. The legal lacuna is the absence of a comprehensive horizontal personal-data statute similar to the newer regimes discussed above (Ministry of IT & Telecommunication, 2026).

A key finding is the fragmentation that arises. International trade rules may impact the legality of localisation measures and create commitments regarding data flows, but they do not themselves create a complete private law of data. At the same time, the same data may be a contractual subject matter, personal information, confidential information, intellectual property, evidence and a regulated cross-border transfer. There is not yet a single international instrument that resolves all of those classifications.

6. PLATFORM COMMERCE, CONSUMERS, JURISDICTION AND CROSS-BORDER REDRESS

Platforms make the traditional bilateral model of international commerce more complicated. A platform can provide marketplace services, payment features, advertising, ranking, logistics or customer support, where the actual sale occurs between a seller and a consumer. The legal implications of that role are generally governed by domestic consumer, contract, competition, privacy and intermediary rules, rather than by a single international digital trade instrument.

This is exemplified by consumer protection. The Australian Consumer Law applies across Australia and continues to apply to online businesses. The Consumer Protection (E-Commerce)

Rules 2020 is an extension of the Consumer Protection Act 2019 of India. United Kingdom consumer law exists side-by-side with contract and data-protection legislation. Canada has a mix of federal and provincial regimes. Pakistan's e-commerce policy framework does not create a consolidated digital-consumer code and focuses on consumer protection, payments and cross-border e-commerce as regulatory areas (Australian Consumer Law, 2026; Department of Consumer Affairs, 2026; Ministry of Commerce, 2019).

Substantive consumer protection is a different thing from jurisdiction and applicable law. A choice-of-law clause may specify the applicable contract law, but its effect may be circumscribed by mandatory consumer rules, jurisdictional rules and public policy. International instruments such as the Hague Choice of Court Convention and the Hague Judgments Convention can improve predictability for participant states, but they do not provide a universal low-cost mechanism for every consumer claim. This practical problem is most acute in the case of low-value transactions where the costs of litigation outweigh the value of the matter in dispute.

Payment systems partly compensate for the shortcomings of formal adjudication. Sometimes disputes can be settled outside a court, through chargebacks, payment-network rules, electronic-money regulation and instant-payment systems. For example, Pakistan has a regulated payment service provider and Raast, and the State Bank of Pakistan is building cross-border payment connectivity (State Bank of Pakistan, 2026). These mechanisms are commercially important, but they are not alternatives to substantive jurisdictional and consumer-law rules.

Platform governance also brings up issues other than the contract of sale. The market participation before a sale can be impacted by ranking, recommendation, advertising and access conditions. Competition law, consumer law and sectoral regulation therefore belong to the practical digital-trade environment even if they are not traditionally labelled 'digital trade law'. That is another reason why the international framework is best understood as layered rather than singular.

7. COMPARATIVE NATIONAL FRAMEWORKS

7.1 United Kingdom

The United Kingdom has mature electronic-transactions law, a dedicated electronic trade documents statute, and a developed privacy and consumer protection framework. The Electronic Trade Documents Act 2023 is especially significant as it converts the functional logic of MLETR into domestic law, conferring the same legal effects of paper to qualifying electronic trade documents (Electronic Trade Documents Act 2023, 2023).

But the UK example does not solve the international problem. Recognition and interoperability still matter under UK law for an electronic trade document when the transaction is crossed-border. Also, UK GDPR transfer rules continue to apply to personal information going abroad. The lesson therefore is not that a jurisdiction has moved on from digital trade but that domestic implementation can make one layer of the international architecture work.

7.2 Australia

Australia has well-established electronic-transactions legislation and a comprehensive digital-trade treaty practice. The Commonwealth Electronic Transactions Act 1999 remains in force and the electronic-transactions legislation functions at the state and territory level (Electronic Transactions Act 1999, 1999). Australia is also an active player in international digital-trade negotiations and agreements.

Paperless trade remains a live legislative project. The Australian Attorney-General's Department records the November 2025 SCAG decision to develop national model amendments aligned with

MLETR. The correct description as of September 2026 is ‘implementation in preparation’ rather than ‘MLETR legislation already enacted’ (Attorney-General’s Department, 2026).

7.3 Canada

Canada shows how hard it is to treat a federal State as a single jurisdiction for digital law. UNCITRAL’s status information identifies the provincial law that is influenced by the Model Law on Electronic Commerce. Privacy regulation also works through PIPEDA and largely equivalent provincial regimes including in British Columbia, Alberta and Quebec (UNCITRAL, 2026c; Office of the Privacy Commissioner of Canada, 2026).

Bill C-36, introduced in the House of Commons on 19 August 2026, proposes further privacy reform, but it is a bill rather than an enacted statute as of the date of this article (Department of Justice Canada, 2026). References to the Bill C-36 track should accordingly be read as describing legislative development, not present law.

7.4 India

India’s e-commerce regime is built on the Information Technology Act 2000, consumer laws and the newer Digital Personal Data Protection regime. The IT Act provides statutory recognition to electronic records and signatures. The Consumer Protection (E-Commerce) Rules 2020 cover platform-facing consumer obligations (Department of Consumer Affairs, 2026; Information Technology Act 2000, 2000).

The DPDP Rules 2025 should be explained with phased rollout dates. The Data Protection Board and other initial provisions took effect earlier, consent-manager provisions are expected to take effect in one year, and most substantive obligations – including the main cross-border transfer framework – take effect after 18 months. So the article takes May 2027 as a future date of implementation, not law today.

India, too, shows the limits of using trade deals as a substitute for domestic regulation. Domestic privacy, sectoral and consumer requirements continue to shape the way businesses operate in the Indian market, even where a trade instrument disciplines localisation or promotes data flows.

7.5 Pakistan

Pakistan’s legal position in electronic transactions is more developed than is often assumed but less developed in the area of comprehensive data protection and paperless transferable records. The Electronic Transactions Ordinance 2002 gives legal recognition to electronic records, writing, originals, retention and electronic signatures. PECA, as amended, deals with cyber offences and related regulatory institutions; it is not to be regarded as the main commercial-law statute for electronic contracting (Electronic Transactions Ordinance 2002, 2002; Prevention of Electronic Crimes Act 2016, 2016).

Pakistan, too, has a national e-commerce policy framework. The 2019 policy of the Ministry of Commerce covers digital payments, consumer protection, cross-border e-commerce, logistics, taxation and legal/regulatory issues. The draft E-Commerce Policy 2.0 has been prepared for the period 2025–2030 (Ministry of Commerce, 2019, 2025). These policy instruments show active regulatory development, but they do not have the same legal footing as a comprehensive digital-trade code that has been enacted.

Pakistan’s payments infrastructure is a key practical element of digital commerce. The State Bank of Pakistan supervises payment systems, payment service providers and electronic-money institutions, and Raast provides an instant-payment infrastructure. These systems prove that

digital commerce can be made to work through sectoral regulation, even in the absence of a single digital-trade statute (State Bank of Pakistan, 2026).

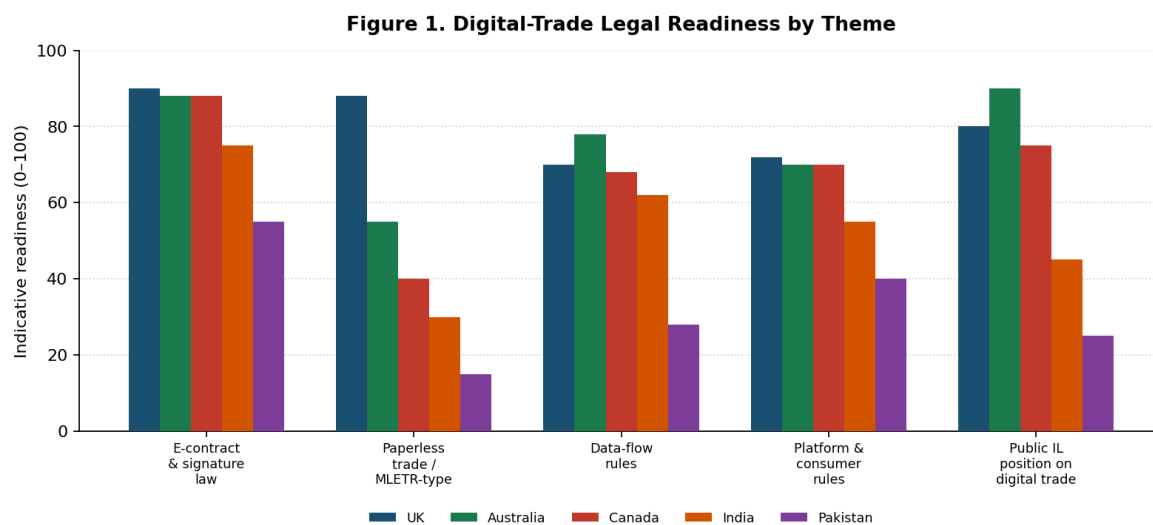
The main comparative gaps are the lack of an enacted comprehensive personal-data protection statute and the lack of MLETR-equivalent legislation. These gaps should not be described as an absence of digital law altogether. Pakistan instead illustrates a fragmented architecture, where electronic transactions, cybercrime, payments, telecom regulation, consumer issues and trade policy are undertaken by different instruments.

Table 1

Comparative legal stacks (Pakistan is discussed in the text: PECA-centred, no enacted PDP or MLETR statute).

Theme	United Kingdom	Australia	Canada	India
E-contracts / signatures	ECA 2000; functional equivalence well settled	ETAs (Cth and States); MLEC family	UECA / provincial ETAs; Quebec distinct	IT Act 2000; e-sign and contracts recognised
Paperless trade documents	Electronic Trade Documents Act 2023 (MLETR-aligned)	MLETR amendments in preparation (SCAG 2025)	MLEC adopted; MLETR not yet	Limited functional equivalence for negotiable docs
Data flows	UK GDPR + adequacy politics; PTA chapters	Open digital-trade chapters; JSI co-convenor	PIPEDA / Bill C-36 track; PTA chapters	DPDP negative-list model; Rule 15 from May 2027
Platforms / consumers	UK consumer law + Online Safety overlap	ACL + privacy reforms	Federal/provincial consumer statutes	Consumer Protection Act 2019 e-commerce rules
WTO ECA / JSI	Participant in JSI architecture	Co-convenor; MC14 interim arrangements	JSI participant	More cautious multilateral digital-trade posture

Note. Pakistan is analysed separately in section 7.5. Table entries are compressed descriptions; the surrounding text states the relevant legal propositions with the necessary qualifications.



Note. Heuristic composite of statute, treaty practice and implementation. Not an official index.

Figure 1. Indicative digital-trade legal readiness by theme.

Note. The 0–100 values are an authorial heuristic and are not an empirical index. The figure should be read as a conceptual illustration only.

8. DISCUSSION: THE LAYERED-CAPABILITY FRAMEWORK

The comparison supports a layered-capability account. The first layer—electronic formation and authentication—is relatively mature because functional-equivalence rules have been widely enacted and supplemented by treaty and domestic law. The legal question is no longer whether an electronic message can ever form a contract; it is whether particular transactions, signatures and records satisfy the relevant jurisdiction's formal and evidentiary requirements.

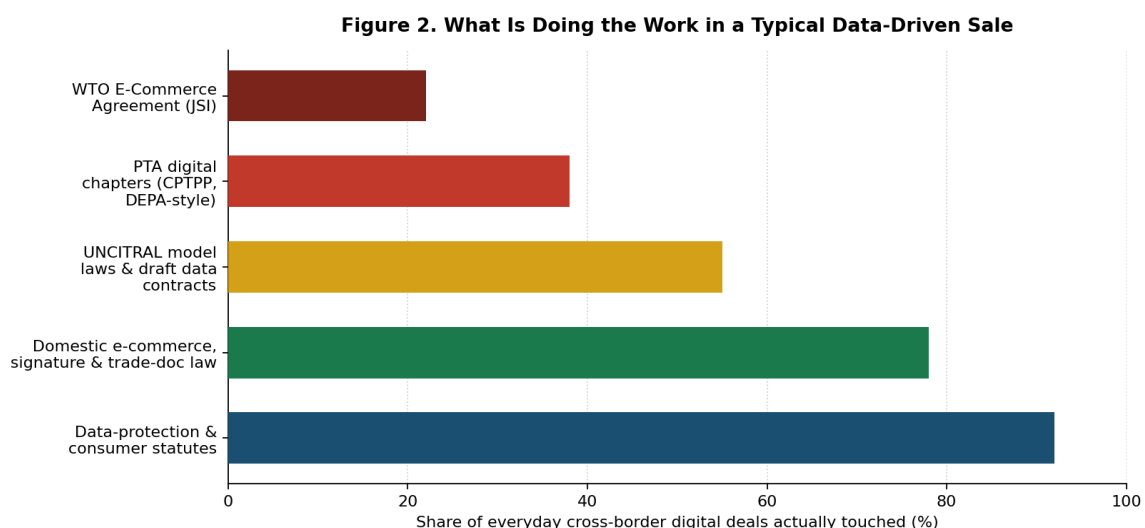
The second layer—transferable electronic records—is less mature because it requires a functional substitute for possession and exclusivity. MLETR provides a coherent legal technique, and the UK has enacted a detailed example, but UNCITRAL's status information shows that adoption remains limited compared with the first-generation Model Law on Electronic Commerce. The legal bottleneck is consequently interoperability across jurisdictions and commercial networks rather than the absence of a conceptual model.

The third layer concerns data as commercial subject matter and cross-border data governance. Here the legal framework is fragmented because the same data may be subject to contract, privacy, confidentiality, intellectual property, competition, cybersecurity and sector-specific rules. UNCITRAL's data-provision project may reduce contractual uncertainty, but it cannot by itself reconcile all of those regimes. Trade agreements can influence the treatment of cross-border data restrictions, but privacy law remains a major source of domestic regulatory autonomy.

The fourth layer concerns platforms, consumers, jurisdiction and redress. International instruments provide some building blocks, but much of the operative law remains domestic. The absence of inexpensive, broadly interoperable consumer redress means that a transaction can be legally valid yet practically difficult to enforce. Payment systems can reduce that gap for some transactions, but private payment mechanisms do not replace rules on jurisdiction, applicable law and mandatory consumer protection.

The framework also reveals why implementation capacity matters without converting capacity into a legal rule. A model law has little practical effect until a legislature enacts it, courts interpret it and commercial actors build systems around it. This is especially visible in paperless trade, where legal recognition of control must be accompanied by interoperable registries, carrier systems, financing arrangements and port procedures.

Figure 2 captures this conceptual point: domestic e-commerce and data-protection rules often do much of the day-to-day work, while international and preferential instruments operate selectively. Its percentages, however, should not be treated as measured shares of legal influence. The figure is best understood as a conceptual representation of the layered architecture.



Note. Illustrative. A consumer platform sale is still mostly domestic statute plus contract terms.

Figure 2. What is doing the work in a typical data-driven sale.

Note. The percentage shares are illustrative rather than empirical and should not be read as measured shares of legal influence.

Table 2

Where the international framework is thin.

Gap	What exists	What data-driven commerce still lacks
Data as the contract's subject-matter	UNCITRAL draft default rules (aim 2027)	A finished, widely enacted instrument
Electronic transferable records	MLETR + UK ETDA 2023	Network effects: few counterparties on the same law
Cross-border personal data	GDPR-style, DPDP negative list, PIPEDA	A trade rule that does not collide with privacy law
Platform private law	UNCITRAL exploratory work 2026	Allocation of liability among platform, seller, payer
Jurisdiction and judgments	Hague instruments; platform terms	Cheap enforcement for small cross-border claims
Customs on e-transmissions	Long WTO moratorium	Moratorium lapsed at MC14 2026; fragmentation risk

The post-MC14 customs position illustrates the difference between a multilateral moratorium and a plurilateral agreement. The lapse of the WTO moratorium creates legal and commercial uncertainty because members may take different positions on customs duties on electronic transmissions. The E-Commerce Agreement may provide a discipline among its participants, but it should not be treated as a universal replacement for the lapsed moratorium.

Private international law remains a structural constraint. Contractual choice-of-law and jurisdiction clauses can improve predictability, but mandatory consumer rules and public policy can limit their operation. International judgments instruments can assist where their conditions are satisfied, yet low-value consumer disputes often remain dependent on platform processes, payment mechanisms or domestic remedies.

Intellectual property also constrains data commerce. A dataset can involve copyright, trade secrets, database rights in some jurisdictions, contractual restrictions or confidentiality even where privacy law is irrelevant. A legal framework that treats cross-border data flows as purely a trade-liberalisation question will therefore understate the substantive rights attached to the data.

These observations lead to a more precise answer to the research question. Existing international and domestic law is capable of regulating some forms of data-driven cross-border commerce, particularly formation and authentication. It is progressively capable of paperless trade where jurisdictions adopt compatible transferable-record rules. It remains fragmented for data as an asset, platform governance and low-cost cross-border redress. The central problem is therefore incomplete functional coverage and interaction among legal regimes, rather than the complete absence of international regulation.

9. LIMITATIONS AND FUTURE RESEARCH

This study is doctrinal and comparative. It does not establish causal relationships between legal reforms and trade outcomes, and it does not test how businesses actually comply with the rules in each jurisdiction. The comparative conclusions should therefore be understood as legal-structural observations.

Future research could test the layered-capability framework through case studies of specific trade corridors, electronic bills of lading, cross-border data-processing arrangements, platform disputes and small-value consumer claims. Empirical work could also test whether legal recognition of electronic transferable records correlates with actual adoption by carriers, banks, insurers and customs authorities.

10. CONCLUSION

The existing legal framework can regulate data-driven cross-border commerce, but its capacity is uneven and function-specific. Electronic contracting and authentication are supported by a mature family of UNCITRAL instruments and extensive domestic legislation. Electronic transferable records are supported by MLETR and a growing number of implementing jurisdictions, but interoperability remains incomplete. Data as commercial subject matter is the subject of emerging UNCITRAL work rather than settled international legislation. Cross-border personal-data governance remains a field in which trade commitments interact with domestic privacy and sectoral regulation. Platform liability, consumer jurisdiction and low-cost redress remain substantially more fragmented.

The five jurisdictions demonstrate different combinations of these layers. The United Kingdom shows the domestic effect of MLETR-aligned legislation through the Electronic Trade Documents Act 2023. Australia combines extensive electronic-transaction legislation and active digital-trade diplomacy with MLETR implementation still under development. Canada demonstrates the complexity of federal and provincial electronic-commerce and privacy law. India combines longstanding electronic-transaction rules with a newly notified, phased data-protection regime. Pakistan has a functioning legal basis for electronic transactions and an active e-commerce policy framework, but it still lacks a comprehensive enacted personal-data statute and MLETR-equivalent legislation.

The principal contribution of the article is therefore the layered-capability framework. It distinguishes what international law presently does from what model laws enable, what domestic law implements, and what emerging projects may accomplish in the future. This distinction prevents two opposite errors: treating digital trade as legally unregulated, and treating the existence of multiple instruments as evidence of a complete international code.

The next phase of digital-trade law is likely to be determined less by the creation of a single universal instrument than by interoperability among existing layers. Enactment of transferable-record legislation, completion and implementation of UNCITRAL's data-provision work, the operation of the WTO Agreement on Electronic Commerce among participating members, coordination between trade and privacy regimes, and practical mechanisms for platform and consumer redress are therefore central to the development of a more coherent system. These are not conclusions that international law has already settled; they are the legal and institutional areas in which the present framework remains incomplete.

REFERENCES

- Anyamele, U. (2024). Promoting digitalization of electronic trade documents in Nigeria through the Model Law on Electronic Transferable Records. *Journal of African Law*, 69(1), 53–72. <https://doi.org/10.1017/S0021855324000202>
- Attorney-General's Department. (2026). Model Law on Electronic Transferable Records (MLETR). Australian Government. <https://www.ag.gov.au/international-relations/model-law-electronic-transferable-records-mletr>
- Australian Consumer Law. (2026). Australian Consumer Law. Australian Government. <https://consumerlaw.gov.au/>
- Commonwealth Secretariat. (2025). The Commonwealth Model Law on Digital Trade and Guide to Enactment. <https://thecommonwealth.org/model-law-digital-trade>
- Department of Consumer Affairs. (2026). Consumer Protection (E-Commerce) Rules, 2020. Government of India. <https://consumeraffairs.gov.in/pages/consumer-protection-acts>
- Department of Foreign Affairs and Trade. (2026). Digital trade and the digital economy. Australian Government. <https://www.dfat.gov.au/trade/services-and-digital-trade/e-commerce-and-digital-trade>
- Department of Justice Canada. (2026). Bill C-36: An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts. Government of Canada. https://www.justice.gc.ca/eng/csj-sjc/pl/charte-charte/c36_1.html
- Electronic Trade Documents Act 2023, c. 38 (UK). (2023). <https://www.legislation.gov.uk/ukpga/2023/38>
- Electronic Transactions Act 1999, No. 162 (Cth) (Australia). (1999). Federal Register of Legislation. <https://www.legislation.gov.au/C2004A00553/latest>
- Electronic Transactions Ordinance 2002 (Pakistan). (2002). Pakistan Code. <https://pakistancode.gov.pk/>
- Information Technology Act 2000 (India). (2000). India Code. <https://www.indiacode.nic.in/>
- Information Commissioner's Office. (2026). International transfers and adequacy regulations. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/>
- Ministry of Commerce. (2019). E-Commerce Policy of Pakistan. Government of Pakistan. <https://www.commerce.gov.pk/ecommerce-policy-2019/>
- Ministry of Commerce. (2025). Draft E-Commerce Policy 2.0 (2025–2030). Government of Pakistan. <https://www.commerce.gov.pk/>
- Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025. Government of India. <https://www.meity.gov.in/>
- Ministry of IT & Telecommunication. (2026). Legislations: Personal Data Protection Bill. Government of Pakistan. <https://www.moitt.gov.pk/Legislations>
- Office of the Australian Information Commissioner. (2025). Chapter 8: APP 8 cross-border disclosure of personal information. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>
- Office of the Privacy Commissioner of Canada. (2026). PIPEDA requirements in brief and provincial privacy laws. <https://www.priv.gc.ca/>
- Pakistan Code. (2016). Prevention of Electronic Crimes Act 2016, as amended. Government of Pakistan. <https://pakistancode.gov.pk/>
- Burri, M., & Kugler, K. (2024). Regulatory autonomy in digital trade agreements. *Journal of International Economic Law*, 27(3), 397–423. <https://doi.org/10.1093/jiel/jgae025>
- Šafranko, Z. (2024). Regulating data provision contracts—Filling the gaps or overlapping the EU rules on the contracts for the supply of digital content? *InterEULawEast*, 11(1), 119–137. <https://doi.org/10.22598/iele.2024.11.1.6>
- State Bank of Pakistan. (2026). Payment systems and Raast. <https://www.sbp.org.pk/>
- UNCITRAL. (1996). Model Law on Electronic Commerce with additional article 5 bis. United Nations Commission on International Trade Law. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
- UNCITRAL. (2001). Model Law on Electronic Signatures. United Nations Commission on International Trade Law. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

- UNCITRAL. (2005). United Nations Convention on the Use of Electronic Communications in International Contracts. United Nations Commission on International Trade Law.
https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications
- UNCITRAL. (2017). Model Law on Electronic Transferable Records. United Nations Commission on International Trade Law.
https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
- UNCITRAL. (2026a). Status: Model Law on Electronic Transferable Records.
https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status
- UNCITRAL. (2026b). Working Group IV: Electronic Commerce.
https://uncitral.un.org/en/working_groups/4/electronic_commerce
- UNCITRAL. (2026c). Status: Model Law on Electronic Commerce.
https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce/status
- WTO. (2026a). Agreement on Electronic Commerce. World Trade Organization.
https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm
- WTO. (2026b). How to accept the Agreement on Electronic Commerce. World Trade Organization.
https://www.wto.org/english/tratop_e/ecom_e/how_to_accept_agreement_e.htm
- WTO. (2026c). Members discuss preparations to bring E-Commerce Agreement into force by mid-2027. World Trade Organization. https://www.wto.org/english/news_e/news26_e/jsec_09jun26_414_e.htm
- WTO. (2026d). DG calls for simultaneous progress on WTO reform and outstanding negotiations. World Trade Organization. https://www.wto.org/english/news_e/news26_e/gc_14jul26_457_e.htm
- WTO. (2026e). Post-MC14 briefing note: E-commerce. World Trade Organization.
https://www.wto.org/english/thewto_e/minist_e/mc14_e/briefing_notes_e/ecommerce_e.htm
- Mitchell, A. D., & Mishra, N. (2019). Data at the docks: Modernizing international trade law for the digital economy. *Vanderbilt Journal of Entertainment & Technology Law*, 20(4), 1073–1120.
<https://scholarship.law.vanderbilt.edu/jetlaw/vol20/iss4/3/>

Source-status note: The article is current to 27 September 2026. References to draft or future instruments are expressly described as such. The article does not treat model laws, draft working papers or WTO interim arrangements as universally binding international law.

◆ Funding

This research received no external funding

◆ Conflict of Interest

The authors declare that they have no known financial or personal conflicts of interest that could have influenced the work reported in this paper.

◆ Data Availability Statement

All data used in this study are derived from publicly available legal sources, including statutes, judicial decisions, treaties and published academic literature cited in the references. No new datasets were generated or analysed.

◆ Ethical Statement

Ethical approval was not required because this study is based exclusively on publicly available legal documents, judicial decisions, treaties and published literature, and did not involve human participants, animals or confidential data.

◆ AI Use Disclosure

Generative artificial intelligence tools were used in a limited and assistive capacity during the preparation of this manuscript, primarily for idea development, language refinement, and grammatical correction. The authors retain full responsibility for the originality, accuracy, analysis, interpretation, and final content of the manuscript.

JOURNAL POLICIES JuriSocial Journal of International Law

OPEN ACCESS & LICENCE

All articles are freely available on publication under CC BY-NC 4.0. Readers may share and adapt the work for non-commercial purposes with proper attribution.

COPYRIGHT

Authors retain copyright and grant JJIL the right of first publication.

PEER REVIEW

Every research article undergoes double-blind peer review by at least two independent reviewers.

PUBLICATION ETHICS

JJIL follows the Committee on Publication Ethics (COPE) Core Practices and guidelines.

PLAGIARISM POLICY

All submissions are screened with similarity-detection software; plagiarism in any form leads to rejection.

GENERATIVE AI POLICY

AI tools cannot be listed as authors. Any substantive use must be disclosed; authors remain fully responsible for the content.

CORRECTIONS & RETRACTIONS

Errors are corrected through published corrigenda; retractions follow COPE guidelines.

ARCHIVING & INDEXING

Content is preserved through [PKP Preservation Network / LOCKSS]. DOIs are registered with Crossref.

PUBLICATION CHARGES

No article publishing fee charged

DISCLAIMER

The views expressed are those of the authors and do not necessarily reflect the views of the editors or the publisher.

Submissions & enquiries editor@jjil.jurisocial.org