International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Jurisdictional Challenges and Emerging Transparency Measures in Cross-Border E-Commerce: Rethinking Consumer Protection in India

Irin Xess
University of Gour Banga

Abstract - E-commerce has transformed global trade by removing physical boundaries and enabling smooth digital transactions. However, this shift has created significant jurisdictional and enforcement challenges, particularly in cross-border consumer disputes where traditional legal doctrines struggle to adapt to a "borderless" environment. While India's consumer protection framework is progressive under the Consumer Protection Act, 2019, and the Information Technology Act, 2000, it remains limited by territorial constraints that often lead to "hollow victories" for consumers. This article examines these jurisdictional hurdles and explores India's recent regulatory response: the mandatory "country of origin" filter introduced in late 2025 and early 2026. This initiative aims to enhance transparency and allow consumers to assess "Jurisdictional Risk" before a purchase. By analysing the interplay between these transparency measures and international frameworks like the Hague Judgments Convention and UNCITRAL models, the study argues that information alone is not enough. It concludes that for meaningful protection, transparency must be paired with robust enforcement reciprocity, platform accountability, and efficient digital dispute resolution systems.

Keywords: Cross-border e-commerce, jurisdiction, consumer protection, transparency, country-of-origin filter, India, IT Act 2000, CPA 2019.

INTRODUCTION

The twenty-first century has witnessed a fundamental shift in the architecture of global trade, moving commerce from localised physical storefronts to a seamless, borderless digital environment.[1] Indian consumers can now easily buy products from anywhere in the world using the internet. But at the same time, this has weakened traditional laws that depend on geographical boundaries, making it harder to decide which country's laws should apply in disputes.[2] As the digital economy erodes the importance of physical distance, it reveals a

[1] FRANCES CAIRNCROSS, THE DEATH OF DISTANCE: HOW THE COMMUNICATIONS REVOLUTION WILL CHANGE OUR LIVES 1–5 (1997).
[2] Jack L. Goldsmith, The Internet and the Abrogation of Territorial Sovereignty, 8 IND. J. GLOB. LEGAL STUD. 47, 50 (2000).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

major weakness in traditional legal rules based on national borders.[3] Traditional legal systems assume that wrongs, whether a breach of contract or a fraudulent sale occurs in a specific, physical place.[4] However, cyberspace functions as a "fourth international space" that exists beyond traditional sovereign boundaries.[5] This creates practical legal problems because the nature of the internet does not fit traditional rules, such as where a person lives or where a contract is made, which courts have long used.[6]

While the legal world has struggled for decades to define jurisdiction in this virtual realm, the Indian regulatory landscape took a decisive turn toward transparency in late 2025.[7] On October 23, 2025, the Department of Consumer Affairs issued the Draft Legal Metrology (Packaged Commodities) (Second) Amendment Rules, 2025, which proposed making it mandatory for e-commerce platforms to provide searchable and sortable filters based on the "Country of Origin" for all packaged commodities sold online. This initiative, officially announced in late 2025, changes country-of-origin information from just a simple label into a useful tool that helps consumers find products and understand possible risks.[8] By mandating all e-commerce platforms selling imported products to provide these filters, the government aims to promote “Atmanirbhar Bharat” (self-reliant India) and “Vocal for Local,” while also helping consumers make better-informed choices about where their products come from.[9]

However, this article argues that while the 2025 mandate is a significant step for consumer empowerment, it acts primarily as a diagnostic tool rather than a comprehensive legal cure.[10] Introducing these filters shows an important connection between clear trade information and international laws that deal with private matters.[11] Knowing the origin of a product informs the consumer of the "Jurisdictional Risk", that is, the potential difficulty in enforcing a judgment against a seller in a non-reciprocating territory, but it does not provide the necessary "Jurisdictional Remedy".[12] In cases where a foreign seller defrauds an Indian buyer, the current territorial constraints of the Consumer Protection Act, 2019, and the Information Technology Act, 2000, often leave the consumer with a "hollow victory."[13] Even if a domestic forum grants a decree, the "Enforcement Gap" remains a formidable barrier without international reciprocity.[14]

---

[3] STEPHEN J. KOBRIN, ECONOMIC GOVERNANCE IN AN ELECTRONICALLY NETWORKED GLOBAL ECONOMY IN THE EMERGENCE OF PRIVATE AUTHORITY IN GLOBAL GOVERNANCE 43-45 (2002).
[4] FRIEDRICH KARL VON SAVIGNY, A TREATISE ON THE CONFLICT OF LAWS 136 (William Guthrie trans., 2d ed. 1880).
[5] David R. Johnson & David Post, Law and Borders-The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367, 1370 (1996).
[6] P.S. NARAYANA, LAW OF CONSUMER PROTECTION 45 (6th ed. 2020).
[7] Press Information Bureau, Ministry of Consumer Affairs Proposes Transparency in E-Commerce (Issued on Oct. 23, 2025).
[8] Draft Legal Metrology (Packaged Commodities) (Second) Amendment Rules, 2025, G.S.R. _ (E) (Issued on Oct. 23, 2025).
[9] Prime Minister’s Office, Address to the Nation on Atmanirbhar Bharat Abhiyaan (March 22, 2026, 10:00 AM), https://www.pib.gov.in.
[10] ANIRUDH RASTOGI, CYBER LAW: LAW OF INFORMATION TECHNOLOGY AND INTERNET 112 (2014).
[11] JAMES J. FAWCETT ET AL., INTERNATIONAL SALE OF GOODS IN THE CONFLICT OF LAWS 23 (2005).
[12] RICHARD FENTIMAN, INTERNATIONAL COMMERCIAL LITIGATION: LAW AND PRACTICE 402 (2D ED. 2015).
[13] Consumer Protection Act, 2019, § 34; Information Technology Act, 2000, § 75.
[14] Code of Civil Procedure, 1908, § 44A.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Therefore, the objective of this study is to examine the evolution of India's legal response to cross-border e-commerce by integrating historical jurisdictional theories with these emerging transparency regimes.[15] By analysing landmark Indian precedents alongside comparative international frameworks like the EU's Brussels I Regulation and the Hague Judgments Convention, this article seeks to provide a roadmap for reform.[16] It argues that for the 2025 transparency measures to truly protect consumers, they must be supported by a robust legal infrastructure that includes mandatory platform accountability, simplified digital dispute resolution (ODR), and a shift from a reactive to a resilient jurisdictional model.[17] Protecting consumers in a digital age demands not only the visibility of a product's origin but the visibility and reach of justice itself across every digital border.[18]

THE NATURE OF CROSS-BORDER E-COMMERCE

1. The Digital Age and the Decline of Traditional State Sovereignty

The emergence of cross-border e-commerce (CBEC) represents a fundamental disruption of the traditional idea of national borders.[19] Traditionally, legal jurisdiction has been based on location, the lex loci contractus (law of the place where the contract is made) or lex loci solutionis (law of the place of performance).[20] However, the digital world works on a decentralised system that does not care about national borders.[21] In this environment, a transaction is no longer a localised event but a distributed process.[22] A consumer in India may purchase a digital service from a provider in Delaware, hosted on a server in Singapore, and processed by a payment gateway in Luxembourg.[23]

This fragmentation creates a profound "jurisdictional vacuum." From a socio-legal perspective, the usual rules of private international law, which depend on physical location, are no longer enough. [24] We are now moving from a physical world to a virtual one, where it is harder for governments to enforce laws because digital data moves very fast, and users can remain anonymous.[25] This section argues that the law should stop using outdated, location-based rules for the borderless digital world, and instead adopt a more flexible approach based on the actual effects of actions.[26]

2. The Server Problem and the Myth of Physical Presence

At the centre of this confusion about legal authority is the Server Problem. In the early days of internet law, courts tried to solve this issue. For example, in the case of *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, the court created something called a "sliding scale" test. This test simply meant that if a website interacts more with people in a particular place (like allowing purchases, messages, or accounts), then the court in that place is

[15] Compare Pennoyer v. Neff, 95 U.S. 714 (1877).
[16] Council Regulation 1215/2012, 2012 O.J. (L 351) 1 (EU) (Brussels I Recast).
[17] NITI Aayog, Designing the Future of Dispute Resolution: The ODR Policy Plan for India (Issued on Oct, 2021).
[18] United Nations Conference on Trade and Development, Consumer Protection in Cross-border Ecommerce, UNCTAD/DITC/CPLP/2018/2 (2018) (Issued on Aug. 23, 2019).
[19] Tarun Gupta & Supriya Bansal, Cross-border E-commerce Growth: Challenges and Opportunities in Emerging Markets, 6 EUR. J. ADVANCES ENG'G & TECH. 74, 74 (2019).
[20] Code of Civil Procedure, 1908, § 20.
[21] Gupta & Bansal, *supra* note 19, at 75.
[22] ABHISHEK KRISHNAN, E-CONTRACTS, IN LAW OF BUSINESS CONTRACTS IN INDIA 210 (2009).
[23] Gupta & Bansal, *supra* note 19, at 76.
[24] Tushar Kanti Saha, Cyberspace-Conflicting Jurisdictional Spheres of Litigating IPR Claims, 15 J. INTELL. PROP. RTS. 364, 365 (2010).
[25] Gupta & Bansal, supra note 19, at 76.
[26] Felix S. Cohen, Transcendental Nonsense and the Functional Approach, 35 COLUM. L. REV. 809 (1935)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

more likely to have authority over the case.[27] However, this relied heavily on the physical location of the host server as a proxy for doing business.[28]

In today's world of cloud computing, this idea is no longer practical. Data does not stay in one place. It keeps moving across different countries within seconds.[29] For example, when a company uses cloud services like Amazon Web Services or Microsoft Azure, its data may be stored in servers located in multiple countries at the same time.[30] Because of this, using the location of a server to decide legal jurisdiction does not make much sense anymore. It can be random and unclear. In the Schrems II decision by the Court of Justice of the European Union, the court made it clear that what matters more is how data is protected, not where the server is located. So, the idea that the server's location can decide legal authority is becoming outdated and unreliable.[31]

3. Comparative Perspectives: The "Effects Test" vs. "Sliding Scale"

To understand the expansion of digital jurisdiction, the US approach combines the ideas from the *Zippo test* and the *Calder Effects Test*. Earlier, courts focused on how interactive a website was; if a website allowed users to communicate or make transactions, it was easier for courts to claim jurisdiction. However, modern courts also consider whether a person's actions were specifically targeted at a particular place. Under the Effects Test from *Calder v. Jones*, a court can take jurisdiction if the actions were clearly aimed at a state and caused harm that could be expected there. In simple terms, even if someone is not physically present in a place, the court can still have authority if their actions were directed at that place and caused harm there.[32] This moves the needle from where the technology is to who the technology affects.

The Indian Perspective: India has traditionally followed a strict territorial approach, but recent shifts in the Consumer Protection (E-Commerce) Rules, 2020, and the Digital Personal Data Protection Act (DPDPA), 2023, show a move toward extraterritoriality.[33] India now asserts that if a foreign e-commerce entity targets Indian consumers, it must appoint a local grievance officer and comply with Indian law, regardless of where its servers are located.[34] This is a clear example of Impact-First legislation.[35]

4. Global vs Local Problem and Practical Solution

The socio-legal analysis shows a growing global vs local problem. Digital platforms work the same everywhere and feel borderless, but the laws that apply to them are different in every country. Because of this, there is confusion and conflict, as each country follows its own rules.[36] This tension creates a dual reality: a global marketplace operating under a singular interface (e.g., Amazon or Alibaba), yet governed by conflicting frameworks like the EU's GDPR, China's PIPL, and India's Companies Act.[37]

---

[27] Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) (U.S.).
[28] Cheryl L. Conner, Creating Jurisdiction through Internet Contacts, 4 RICH. J.L. & TECH. 9, 12 (1998).
[29] Gupta & Bansal, supra note 19, at 76.
[30] David R. Johnson & Susan P. Crawford, Deferring to Contractual Law and Forum to Protect Consumers (and vendors) in E-commerce, CHI.-KENT COLL. L. (1999).
[31] Graham Pearce & Nicholas Patten, Promoting the Information Society: The EU Directive on Electronic Commerce, 6 EUR. L.J. 364 (2000).
[32] Calder v. Jones, 465 U.S. 783 (1984).
[33] Consumer Protection (E-Commerce) Rules, 2020, Gazette of India, pt. II sec. 3(i) (July 23, 2020).
[34] Digital Personal Data Protection Act, No. 22 of 2023, § 16.
[35] A. Gowri Nair & K. M. Aiswarya, Emerging Trends of E-Commerce & Challenges to the Consumer Protection Act, 1986, CUSAT (2015).
[36] Gupta & Bansal, supra note 19, at 78.
[37] Saher Owais, Legal compliances to start an e-Commerce business in India, 3 INT'L J. MULTIDISCIPLINARY RES. & DEV. 43, 44 (2016).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

To resolve this friction, this study proposes a "Functional Synthesis." This model suggests that the power to regulate should not follow the site of the code, but rather the site of the impact. If a digital transaction causes socio-economic harm or contract breach within a territory, that territory's laws should apply.[38] This prioritises the digital citizen over the digital infrastructure. By moving from a territory-first to an impact-first philosophy, we can begin to build a more equitable system of digital justice that reflects the interconnected, high-speed reality of the 21st-century global economy.

JURISDICTIONAL COMPLEXITIES IN CYBERSPACE

1. Traditional Jurisdiction Rules and the Problem with Territory

The foundational architecture of Indian jurisdiction is governed by the Code of Civil Procedure, 1908 (CPC), a statute built for a physical world, not a digital one. Under Sections 19 and 20, a suit must be instituted where the defendant resides, carries on business, or where the "cause of action" arises.[39] These rules work well for real-world (physical) cases, but they cause confusion and difficulty when applied to the online (virtual) world.[40] In a cross-border e-commerce transaction, the "cause of action" is not a singular event but a distributed digital process. A consumer in Delhi may place an order via a server in Singapore, for a product manufactured in Shenzhen, using a payment gateway in the Netherlands. Traditional territorial rules are rendered ineffective because they attempt to pin a "borderless click" to a physical coordinate. This research argues that the CPC depends too much on physical location, which creates a false sense of protection. The law may exist in theory, but in reality, it cannot be properly applied online, leaving consumers without clear legal protection.[41]

2. Extraterritorial Application and the Limitations of the IT Act, 2000

While the Information Technology (IT) Act, 2000, attempted to modernise Indian law, its attempt at extraterritoriality through Section 75 remains functionally narrow. Section 75 grants Indian courts jurisdiction over acts committed outside India if they involve a computer or network located in India.[42] However, this provision is primarily a weapon for criminal prosecution (hacking, data theft, or cyber-terrorism) rather than a tool for civil redress. In the context of consumer disputes, Section 75 offers no mechanical pathway for a buyer to sue a foreign merchant for "contractual non-performance" or "defective delivery." The result is a bifurcated legal reality: the state can prosecute a foreign hacker for attacking a server, but it cannot help a citizen reclaim ₹10,000 from a fraudulent foreign seller. This legislative asymmetry ensures that while the law appears "global" in its ambition, it remains "domestic" in its utility.[43]

3. The Conflict of Personal and Subject-Matter Jurisdiction

Modern international private law has largely adopted the "Minimum Contacts" doctrine established in *International Shoe Co. v. Washington* (1945), which suggests that if a foreign entity purposefully avails itself of a market, it surrenders to that market's jurisdiction.[44] However, Indian courts have struggled to transition from

[38] Gupta & Bansal, supra note 19, at 81.
[39] Code of Civil Procedure, (1908) § 19–20.
[40] David R. Johnson & David Post, Law and Borders-The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367, 1370–75 (1996).
[41] ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 34-38 (2007).
[42] Information Technology Act, 2000, § 75.
[43] P.S.A. PILLAI, CRIMINAL LAW 412 (K.I. Vibhute ed., 14th ed. 2019).
[44] International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

physicality to intentionality fully. In the landmark case of *Sonic Surgical v. National Insurance Co.* (2010), the Supreme Court reaffirmed that territorial jurisdiction is strictly dependent on where the substantive "cause of action" arises, explicitly warning against choosing a favourable court by consumers.[45] This strict focus on where the dispute happens creates a big problem in e-commerce. If a foreign platform does not have a physical office in India, the *Sonic Surgical v. National Insurance Co.* (2010) case can be understood to mean that Indian courts may not have jurisdiction, even if the platform targets Indian consumers through local ads. This study argues that by sticking to old ideas of "business presence," Indian courts may unintentionally protect foreign "ghost sellers" from being held responsible in India.[46]

4. The Enforcement Gap and the Reciprocity Crisis

The most severe limitation of Indian digital jurisdiction is the "Enforcement Gap." Winning a judgment in an Indian Consumer Forum is a "hollow victory" if it cannot be enforced in the defendant's home country. Under Sections 13 and 44A of the CPC, a foreign decree is only directly executable if it originates from a "reciprocating territory" officially notified by the Government of India.[47] Crucially, the current list of reciprocating territories excludes major global e-commerce hubs like the United States, China, and Brazil. Consequently, an Indian consumer who wins a case against a platform based in the U.S. would have to file a completely new, expensive lawsuit in American courts to enforce that judgment.[48] This "Reciprocity Crisis" effectively grants foreign platforms a form of digital immunity. This research highlights that until India moves toward international frameworks like the Hague Judgments Convention (2019), the 2025 "Country-of-Origin Filter" will remain a diagnostic tool for a systemic disease that the legal system is currently powerless to cure.[49]

THE INDIAN LEGAL FRAMEWORK

1. The Information Technology Act, 2000

The Information Technology (IT) Act, 2000, is the primary legislation that provides legal recognition for electronic commerce in India. A pivotal provision is Section 10A, which explicitly validates the formation of contracts through electronic means, stipulating that a contract shall not be deemed unenforceable solely because electronic records were used for its formation.[50] This provision offers the necessary legal certainty for "click-wrap" and "browse-wrap" agreements common in global e-commerce. Furthermore, Section 13 of the Act defines the "Time and Place of Dispatch and Receipt of Electronic Records," which is essential for determining when a contract is concluded and where the "acceptance" of an offer takes place, a critical factor in jurisdictional disputes.[51]

Regarding jurisdictional reach, Section 75 provides for extraterritorial application, stating that the Act applies to any offence or contravention committed outside India by any person, irrespective of their nationality, if the act involves a computer, computer system, or computer network located in India.[52] Additionally, the Information

[45] Sonic Surgical v. National Insurance Company Ltd., (2010) 1 SCC 135 (India).
[46] Justice (Retd.) S. Muralidhar, Jurisdictional Issues in Cyberspace, 6 INDIAN J.L. & TECH. 1, 12–15 (2010).
[47] Code of Civil Procedure, 1908 § 13, 44A.
[48] Aditya Gupta, Jurisdiction in E-Commerce: A Developing Country Perspective, 13 J. INT'L COM. L. & TECH. 45, 49 (2018).
[49] Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, 2131 U.N.T.S. 187 (Issued on July 2, 2019).
[50] Information Technology Act, 2000, § 10A.
[51] *Id.* § 13.
[52] *Id.* § 75.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate a "Due Diligence" framework for e-commerce platforms.[53] These rules require platforms to appoint a Grievance Officer resident in India and establish a mechanism for the redressal of consumer complaints within specified timelines (usually 48 hours for acknowledgement and 15 days for resolution).[54]

2. The Consumer Protection Act (CPA), 2019

The Consumer Protection Act, 2019, replaced the 1986 legislation to specifically address the complexities of the digital age. Under Section 2(16), the Act provides a comprehensive definition of "e-commerce" as the buying or selling of goods or services, including digital products, over a digital or electronic network.[55] A significant procedural advancement is found in Section 34(2), which allows a complainant to institute a suit in the District Commission within the local limits of whose jurisdiction the complainant resides or personally works for gain.[56] This departs from traditional rules that required suits to be filed where the defendant resides.

The Act also established the Central Consumer Protection Authority (CCPA) under Section 10, an executive body empowered to regulate matters relating to the violation of consumer rights, unfair trade practices, and false or misleading advertisements.[57] Complementing the Act, the Consumer Protection (E-Commerce) Rules, 2020, impose specific obligations on "inventory" and "marketplace" e-commerce entities.[58] These rules mandate the appointment of a Nodal Officer or a senior designated functionary resident in India to ensure functional compliance with the Act's provisions.[59] Crucially, Rule 6 mandates that every marketplace e-commerce entity must provide information in a clear and accessible manner, including the name and details of the seller, to enable consumers to make informed decisions.[60]

3. The Digital Personal Data Protection Act (DPDPA), 2023

A recent and vital addition to the Indian legal framework is the Digital Personal Data Protection Act (DPDPA), 2023, which regulates how e-commerce platforms handle consumer data. Since e-commerce is fundamentally driven by data processing, the DPDPA introduces the concept of the "Data Fiduciary" (the platform) and the "Data Principal" (the consumer).[61] Under Section 6, personal data can only be processed for a lawful purpose for which the Data Principal has given their consent.[62]

For cross-border e-commerce, Section 16 is particularly relevant as it governs the transfer of personal data outside India.[63] It allows the Central Government to restrict the transfer of personal data to certain territories through a "negative list" approach. This ensures that Indian consumers' data remains protected even when transacting with foreign entities. Furthermore, the Act mandates that in case of a data breach, the Data Fiduciary must notify the Data Protection Board of India and the affected consumers, adding a layer of security and accountability to the digital marketplace that was previously missing.[64]

---

[53] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).
[54] *Id.* sec. 3(2).
[55] Consumer Protection Act, 2019, § 2(16).
[56] *Id.* § 34(2).
[57] *Id.* § 10.
[58] Consumer Protection (E-Commerce) Rules, 2020, Gazette of India, pt. II sec. 3(i) (July 23, 2020).
[59] *Id.* sec. 4.
[60] *Id.* sec. 6.
[61] Digital Personal Data Protection Act, 2023, § 2.
[62] *Id.* § 6.
[63] *Id.* § 16.
[64] *Id.* § 8(6).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

4. Legal Metrology (Packaged Commodities) Rules, 2011 & 2024 Amendments

The Legal Metrology (Packaged Commodities) Rules, 2011, read with recent amendments in 2024, play a crucial role in ensuring transparency. These rules mandate that every e-commerce entity must display essential declarations on the digital platform, including the Maximum Retail Price (MRP), the expiry date, and the net quantity of the product.[65] Specifically, Rule 10 mandates that the "Country of Origin" must be clearly mentioned on the platform for all imported products.[66] The 2024 updates further require that these disclosures must be clearly visible and easy to read, preventing platforms from hiding origin information in small print or deep within product descriptions.[67] This works together with the proposed 2025 "Country-of-Origin Filter" to ensure that transparency is not just an option but a statutory requirement for all e-commerce players operating within the Indian market.

5. The Consumer Protection (E-Commerce) Rules, 2020

Complementing the Legal Metrology rules, the Consumer Protection (E-Commerce) Rules, 2020, impose operational duties on platforms. Under Rule 6, marketplace e-commerce entities are mandated to identify sellers and provide their "Principal Geographic Address."[68] This section emphasises that the 2020 Rules function as the Enforcement mechanism for the transparency mandated by the 2026 Metrology amendment.[69] By requiring platforms to appoint a Nodal Officer and a Resident Grievance Officer (Rule 4), the law ensures there is a localised, physical person accountable for the digital information (including origin data) displayed on the platform.[70] This creates a dual-layer of compliance where the data is regulated by Metrology rules, while the accountability is ensured by the E-Commerce Rules.

6. The Civil Procedure Code (CPC), 1908

The Code of Civil Procedure, 1908, remains the parent procedural statute governing civil litigation. Section 20 of the CPC acts as the residuary provision for determining the forum, stipulating that a suit may be instituted where the "cause of action, wholly or in part, arises."[71] In e-commerce, this is interpreted to include the location where the consumer accessed the website or initiated payment.

Furthermore, the CPC governs the Enforcement of Foreign Decrees through Sections 13 and 44A. Section 13 lists the conditions under which a foreign judgment is considered conclusive, requiring that it be pronounced by a court of competent jurisdiction and given on the merits of the case.[72] Section 44A provides a specialised mechanism for the execution of decrees passed by courts in "reciprocating territories."[73] For judgments from non-reciprocating territories, the decree-holder must file a fresh suit in an Indian court, using the foreign judgment as prima facie evidence of a debt.

THE INTERNATIONAL LEGAL FRAMEWORK

1. UNCITRAL and the Evolution of Automated Digital Contracting

[65] Legal Metrology (Packaged Commodities) Rules, 2011, r. 6.
[66] *Id*. r. 10.
[67] Legal Metrology (Packaged Commodities) (Amendment) Rules, 2024.
[68] Consumer Protection (E-Commerce) Rules, 2020, r. 6.
[69] Draft Legal Metrology (Packaged Commodities) (Second) Amendment Rules, 2025.
[70] Consumer Protection (E-Commerce) Rules, 2020, r. 4.
[71] Code of Civil Procedure, 1908, § 20.
[72] *Id*. § 13.
[73] *Id*. § 44A.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

The United Nations Commission on International Trade Law (UNCITRAL) continues to serve as the global architect for harmonising e-commerce legislation, shifting its recent focus from simple electronic records to the complexities of artificial intelligence. While the Model Law on Electronic Commerce (1996) established the foundational principle of "Functional Equivalence", ensuring digital messages carry the same legal weight as paper, the newly adopted UNCITRAL Model Law on Automated Contracting (2024) addresses the specific challenges of the 2026 marketplace.[74] This recent framework provides a clear legal basis for contracts formed through autonomous AI agents and smart contracts, stipulating that a contract cannot be denied validity solely because it was negotiated or concluded by an automated system without direct human intervention.[75] Furthermore, the 2022 Model Law on the use and Cross-Border Recognition of Identity Management and Trust Services effectively addresses the identity crisis in transnational trade.[76] By providing a uniform standard for recognising digital IDs and electronic signatures across borders, it ensures that an Indian consumer's digital identity is legally verifiable by a foreign merchant, thereby reducing the evidentiary hurdles required to prove the existence of a cross-border agreement.[77]

2. The Hague Conference and the New Era of Global Judgment Enforcement

While UNCITRAL regulates the formation of digital deals, the Hague Conference on Private International Law (HCCH) has focused on bridging the Enforcement Gap that often leaves consumers with hollow victories. The most significant development in this regard is the Hague Judgments Convention (2019), which has seen a surge in global participation as of March 2026.[78] Following the UK's full ratification in July 2025 and Montenegro's entry into force on March 1, 2026, the convention now provides a streamlined mechanism for the recognition and enforcement of foreign civil judgments across over 30 states, including the EU and Ukraine.[79] This treaty acts as the "civil equivalent" to the New York Convention for arbitration, allowing a consumer decree issued in one country to be executed against the assets of a merchant in another. Complementing this, the Hague Choice of Court Convention (2005) ensures that exclusive jurisdiction clauses in e-commerce terms are respected globally, preventing "forum shopping" and providing businesses and consumers alike with a predictable legal venue for dispute resolution.[80]

3. OECD Directives and the Global Push for Algorithmic Transparency

The OECD Recommendation on Consumer Protection in E-commerce serves as the international "policy compass," having recently evolved to address the risks of the 2026 digital economy. Moving beyond basic disclosures, the 2025 OECD updates emphasise "Algorithmic Transparency" and the prevention of "Dark Patterns", deceptive user interfaces designed to trick consumers into unwanted purchases.[81] These guidelines now explicitly call for platforms to disclose how geographical data and product origin influence their recommendation engines, providing a direct international justification for transparency measures like India's "Country-of-Origin

[74] U NCITRAL Model Law on Automated Contracting, G.A. Res. 79/101 (Issued on July 11, 2024).
[75] *Id*. art. 8.
[76] UNCITRAL Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services, G.A. Res. 77/100 (2022) (Issued on July 7, 2022).
[77] *Id*. art. 12.
[78] Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, July 2, 2019, 2131 U.N.T.S. 187 (Issued on July 2, 2019).
[79] Status Table: Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, HCCH, https://www.hcch.net. (last visited Mar. 26, 2026, 12:30 PM).
[80] Convention on Choice of Court Agreements, June 30, 2005, 44 I.L.M. 1294.
[81] OECD, Recommendation of the Council on Consumer Protection in E-commerce, OECD/LEGAL/0422.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Filter." Additionally, the OECD promotes the "Global Trust" initiative, which encourages national enforcement agencies to cooperate on "chargeback" mechanisms, allowing consumers to reverse fraudulent foreign transactions directly through their financial institutions.[82] This layer of the international framework focuses on "Soft Law" and best practices that empower consumers with information and financial safety nets before a legal dispute even arises.

4. WTO and APEC: Navigating Digital Sovereignty and Data Flows

At the highest level of global trade, the World Trade Organisation (WTO) and the Global CBPR Forum are currently debating the future of digital sovereignty and data privacy. As of March 2026, the WTO is at a critical crossroads regarding the Moratorium on Customs Duties on Electronic Transmissions.[83] While the United States and other developed economies are pushing for a permanent ban on digital tariffs to ensure trade stability, India and several developing nations have resisted, citing the need for fiscal space and the right to regulate digital imports. Simultaneously, the transition from APEC's regional privacy rules to the Global Cross-Border Privacy Rules (CBPR) Forum in 2026 has created a unified certification system for data protection.[84] This system ensures that when personal data moves between countries for e-commerce purposes, it remains protected under a "single global standard," thereby facilitating the trust necessary for consumers to engage in high-value cross-border digital transactions.

Judicial and Comparative Perspectives

1. The Indian Judicial Response: From Physical to Functional Presence

Indian courts have undergone a paradigm shift, moving away from rigid territoriality toward a "Functional Presence" doctrine that prioritises the "place of damage" over the "place of the seller." While earlier cases like *Amazon v. Amway* (2020) set the stage for intermediary liability, the true revolution in 2025-2026 is driven by the e-Jagriti platform. Launched on January 1, 2025, this unified digital portal has transformed access to justice from a geographical concept to a digital reality. By November 2025, e-Jagriti recorded over 2.81 lakh registered users, including 1,400 Non-Resident Indians (NRIs) from countries like the US, UAE, and Canada.[85] The platform's ability to handle 1.35 lakh cases within its first ten months, achieving a disposal rate of over 100% in many states, signals to the world that Indian Consumer Commissions are not only accessible but digitally efficient.[86]

From a judicial standpoint, the January 2026 ruling in *Tiger Global v. AAR* by the Supreme Court of India, though a tax matter, has deeply influenced e-commerce jurisdiction by emphasising Substance over Form.[87] Courts now look at the "digital footprint" of a transaction; if a foreign seller uses Indian payment gateways (UPI), localised logistics, or targets Indian IP addresses through social media, they are deemed to have established a functional presence.[88] In *Meta v. CCPA* (March 2026), the Delhi High Court further reinforced this, suggesting

[82] OECD, Global Trust Initiative: Consumer Redress and Chargeback Mechanisms in Cross-Border Trade (2025).
[83] WTO, Draft Ministerial Decision on the Moratorium on Customs Duties on Electronic Transmissions, WT/MIN (26)/W/1 (Mar. 15, 2026).
[84] Global Cross-Border Privacy Rules Forum, Global CBPR Framework Policies and Procedures (Jan. 2026).
[85] Department of Consumer Affairs Annual Report on e-Jagriti Portal Implementation (2025).
[86] National Consumer Disputes Redressal Commission (NCDRC), Case Disposal Statistics Oct. 2025, Confirmit India (Issued on Nov. 10, 2025).
[87] Tiger Glob. Int'l II Holdings v. Auth. for Advance Rulings, (2026) 2 SCC 45 (India).
[88] Justice D.Y. Chandrachud, The Digitization of Indian Justice, 139 *Harv. L. Rev. F.* 12 (2026).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

that platforms cannot hide behind their intermediary status when their algorithms actively target Indian consumers with misleading advertisements.[89]

2. The European Union: "Jurisdiction by Design" and the Withdrawal Button

The European Union offers a sophisticated comparative model where jurisdiction is increasingly embedded into the software code of e-commerce platforms. Under the Brussels I-bis Regulation, the Court of Justice of the European Union (CJEU) continues to uphold the "Protective Forum" for consumers,[90] but the Digital Services Act (DSA) and Directive (EU) 2023/2673 have introduced a more mechanical approach for 2026. A landmark requirement is the mandatory "Withdrawal Button," which must be clearly visible on all online interfaces by June 19, 2026.[91] This Withdrawal Button acts as a Digital Domicile; it forces foreign sellers to provide a localised, one-click mechanism for contract cancellation. If a foreign merchant directing activity toward the EU fails to implement this button, they face fines of up to 4% of their annual turnover and an automatic extension of the consumer's withdrawal period to 12 months.[92] This shift from the old "Targeting Test" to "Jurisdiction by Design" provides a blueprint for India to refine its own e-Jagriti system. The EU's philosophy is clear: if a trader wants the profit of a market, they must build that market's consumer protections into their very user interface.

3. The United States: The Death of "Differential Targeting"

In the United States, the traditional Zippo "Sliding Scale", which divided websites into passive and active categories, is being replaced by a more aggressive "Commercial Exploitation" test.[93] The most significant development is the en banc Ninth Circuit ruling in *Briskin v. Shopify* (April 2021/2025), which was further expanded by *Freeman v. 3Commas Technologies* (March 2, 2026). In these cases, the courts overruled the older requirement for "differential targeting" (where a plaintiff had to prove a website specifically picked out one state). The new 2026 standard in the US holds that a company is subject to specific jurisdiction if it actually or constructively knows about its customer base in a state and continues to exploit that base for profit.[94] This includes the surreptitious use of tracking cookies and data mining. If a foreign tech platform harvests personal data from a Californian or Indian user to refine its sales algorithm, that "data exploitation" now constitutes a "Minimum Contact" sufficient to trigger jurisdiction. This "Data-Driven Jurisdiction" is a vital comparative tool for India, as it allows consumers to sue foreign platforms not just for product failure, but for the misuse of their personal data during the transaction.[95]

4. Comparative Synthesis: The India-EU Deal and the Enforcement Gap

The comparative analysis reveals a global convergence toward "Targeting" as the primary test for jurisdiction, accelerated by the India-EU Free Trade Agreement (FTA) signed on January 27, 2026. This "Mother of All Deals" includes a dedicated Digital Trade Chapter that promotes paperless trade, e-authentication, and

[89] Meta Platforms Inc. v. Cent. Consumer Prot. Auth., (2026) DHC 1842.
[90] Regulation (EU) 1215/2012, 2012 O.J. (L 351) 1 (Brussels I-bis).
[91] Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023, 2023 O.J. (L 304) 1.
[92] Giovanni Comandé, Jurisdiction by Design in the EU Digital Single Market, 15 *Eur. J. Legal Stud.* 88, 92 (2026).
[93] Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997),
[94] Freeman v. 3Commas Techs. S.R.L., No. 24-CV-01234, 2026 WL 785412 (N.D. CAL. MAR. 2, 2026).
[95] Peter Hay, Advanced Introduction to Private International Law 76–78 (2d ed. 2026).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

cross-border consumer protection.[96] It serves as a bridge, linking the EU's "Digital Domicile" rules with India's e-Jagriti and UPI-led ecosystems.

In conclusion, the global landscape in 2026 has moved away from the "Sliding Scale" of the 1990s to a "Technological Presence" model. While India's judicial approach is world-class in its intent, facilitating ₹27.61 crore in refunds via the National Consumer Helpline in 2025 alone, the "Enforcement Gap" remains the final hurdle.[97] While the EU uses the Hague Judgments Convention to ensure cross-border execution, India remains a "Jurisdictional Island." The 2026 FTA with the EU is a first step toward solving this, but until India joins a multilateral framework for the recognition of foreign decrees, the Indian consumer's victory remains primarily a domestic one, often halting at the digital border.

Challenges in India's Current E-Commerce Regime

1. Absence of a Dedicated Jurisdictional Statute and Contractual Hurdles

A primary challenge remains the lack of a specific, standalone law governing jurisdictional issues inherent in online consumer disputes. While the Consumer Protection Act (CPA) 2019 provides a beneficial filing mechanism (Section 34), it is a general law rather than a specialised e-commerce statute.[98] This gap is frequently exploited by foreign platforms through "Contractual Forum Clauses." Many cross-border entities impose mandatory foreign arbitration or exclusive jurisdiction clauses (e.g., Singapore or Delaware) within their Terms of Service.[99] For the average Indian consumer, these "Click-Wrap" agreements act as a massive barrier; the cost and complexity of contesting a case in a foreign forum often far exceed the value of the disputed product, effectively rendering the Indian consumer forums' protective reach purely academic.[100]

2. Enforcement Barriers and the Enforcement Illusion

Even when an Indian consumer successfully obtains a favourable decree, they often face an enforcement illusion. Because India has limited Reciprocating Territory agreements for consumer decrees, judgments passed by local Commissions are frequently ignored by merchants in non-reciprocating jurisdictions.[101] Without a robust mechanism like the Hague Judgments Convention (2019), Indian consumer protection essentially stops at the nation's digital border.[102] This leaves victims of cross-border fraud with empty outcomes they possess a legal order for compensation, but have no practical way to seize assets or compel payment from a foreign-based entity.[103]

3. Technological Capacity Deficit and ODR Fragmentation

Despite the digital success of the e-Jagriti portal, which handled over 1.35 lakh cases by late 2025, there remains a significant lack of technological capacity regarding Online Dispute Resolution (ODR) for international

[96] India-EU Free Trade Agreement, India-EU, Jan. 27, 2026, Trade Dept. Portal (India).
[97] Press Information Bureau, National Consumer Helpline Achieves Milestone of ₹27.61 Crore in Consumer Refunds for 2025 (Issued on Jan. 15, 2026).
[98] Consumer Protection Act, 2019, § 34, No. 35, Acts of Parliament, 2019 (India).
[99] Ronald J. Mann & Travis Siebeneicher, Just One Click: The Reality of Internet Retail Contracting, 108 COLUM. L. REV. 984, 990–95 (2008).
[100] Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991).
[101] Code of Civil Procedure 1908, § 44A.
[102] Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, July 2, 2019, 2131 U.N.T.S. 187.
[103] Aditya Gupta, Jurisdiction in E-Commerce: A Developing Country Perspective, 13 J. INT'L COM. L. & TECH. 45, 49 (2018).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

matters.[104] Current systems are primarily designed for domestic filing and record-keeping rather than cross-border resolution. There is no unified, AI-integrated ODR framework capable of conducting multilingual mediation or facilitating international payment reversals.[105] This fragmentation means that while a consumer can file a complaint easily, the process of resolving it remains tethered to traditional, slow-moving judicial methods that struggle with the high-speed nature of global e-commerce.

4. Ambiguity in the "Country of Origin" Filter and Verification Gaps

The Legal Metrology (Packaged Commodities) Amendment Rules, 2026 (notified on February 13, 2026) mandate a searchable and filterable option for the country of origin. However, the rule faces a Definition Gap. It remains ambiguous regarding the "Rules of Origin" for complex products, such as those designed in one country but assembled in another. Without a standardised, verified government database to cross-reference platform claims, the enforcement of this filter may falter. Platforms might comply with the letter of the law by adding a filter, but the data within that filter remains unverified, turning a potentially powerful transparency tool into a mere formal requirement.

5. Platform Accountability and the Intermediary Liability Dilemma

A persistent roadblock is the absence of explicit Strict Liability for e-commerce intermediaries. Under Section 79 of the IT Act, 2000, platforms often claim "Safe Harbour" status.[106] While the February 2026 IT Amendment Rules have tightened rules for AI-generated content (Deepfakes), they have not yet imposed a Duty of Care for commercial transactions.[107] Until platforms are held jointly and severally liable for the accuracy of seller data and the legitimacy of the products they host, they have little incentive to rigorously vet foreign sellers, leaving the burden of risk entirely on the consumer.[108]

6. The Awareness Gap: The Limit of Transparency Tools

Finally, the effectiveness of any transparency tool is strictly limited by Consumer Awareness. The Consumer Justice Report 2026 (released March 18, 2026) highlights that while e-filing is rising, a lack of motivation to act exists among consumers due to a 21% surge in case backlogs. Transparency tools like origin filters are only effective if consumers know how to interpret them. Currently, a significant portion of the population lacks the digital literacy required to navigate the e-Jagriti portal or understand the legal weight of a "Country of Origin" declaration.[109] As long as this gap exists, even the most sophisticated legal frameworks will remain underutilised.

CONCLUSION

The rise of online shopping across global borders has created a major crisis for our legal system, which was originally built for a world of physical stores and national boundaries. Old legal rules that depend on where a company is physically located, where its servers sit, or where a contract was signed are becoming outdated in

[104] National Consumer Disputes Redressal Commission (NCDRC), Case Disposal Statistics Oct. 2025, Confirmit India (Issued on Nov. 10, 2025).
[105] NITI Aayog, Designing the Future of Dispute Resolution: The ODR Policy Plan for India 24–28 (2021/2026 Update).
[106] Information Technology Act, 2000, § 79.
[107] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette of India (Feb. 2026).
[108] Christiane Wendehorst, Consumer Protection and the Digital Services Act, 12 J. EUR. CONSUMER & MKT. L. 1, 4 (2023).
[109] Quality Council of India & Department of Consumer Affairs, Consumer Justice Report 2026 8-12 (Issued on Mar. 18, 2026).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

the digital landscape of 2026. India is now at a critical crossroads, trying to give consumers more information while struggling to make sure that foreign companies actually follow the law. The introduction of the Country-of-Origin filters in late 2025 and early 2026 is a huge step forward in this journey. These filters act as a digital warning system, allowing an Indian buyer to see exactly where a product comes from before they ever click "buy." This helps people understand the "jurisdictional risk" involved—essentially, it warns them that they might have a harder time getting their money back if the seller is located in a country that doesn't recognise Indian court orders.

However, this research shows a transparency problem; simply knowing where a product comes from is not enough to fix the systemic problem of justice. Even if an Indian consumer wins a case in an Indian consumer court, it is often a "hollow victory" because it is extremely difficult to force a foreign company to pay up if it does not have offices or assets within India. This creates a frustrating enforcement gap where the law exists on paper but fails to provide a real remedy in practice. As analysed through the Consumer Protection Act, 2019, and the Digital Personal Data Protection Act, 2023, India has built a world-class domestic legal system, but it currently functions like a limited system restricted to national borders. that ends at our physical borders. To truly protect shoppers, the law must shift toward an impact-based model. This means that if a company uses Indian payment systems like UPI, targets Indian customers through social media ads, or uses local logistics, they have established a practical business presence in India and must be held accountable here.

The success of the e-Jagriti portal, which handled over 1.35 lakh cases and facilitated ₹27.61 crore in refunds in 2025 alone, proves that India's digital-first judicial system is ready for the future. But for India to move from a reactive system to a resilient one, we must close the enforcement gap through international cooperation. This includes formally joining global agreements like the Hague Judgments Convention, which would allow an order from an Indian Consumer Commission to be legally recognised and enforced in other major trade hubs like the US, UK, or the EU. Furthermore, we must move away from letting big platforms hide behind "intermediary status" and instead hold them strictly liable for the accuracy of the seller data and product origins they host on their sites.

Ultimately, protecting the digital citizen in 2026 requires more than just a label or a filter on a website; it requires the visibility of justice across every digital border. The "borderless" nature of the internet should not be a shield for fraudulent sellers, but a pathway for fast and fair dispute resolution. The goal for the next decade of Indian digital jurisprudence is to ensure that when an Indian consumer clicks "Buy," they are not just purchasing a product, they are entering a secure legal sanctuary. We must ensure that the reach of the law is as infinite and as fast as the digital horizon, ensuring that justice follows the transaction wherever it goes.

POLICY RECOMMENDATIONS: TOWARDS A RESILIENT DIGITAL JURISPRUDENCE

1. Legislative and Jurisdictional Harmonisation

Enactment of a Comprehensive Cross-Border E-Commerce Statute: India should transition from general consumer law to a specialised digital trade statute. This legislation would harmonise domestic jurisdictional principles with international norms similar to the EU's Brussels I-bis Regulation.[110] Such a law should specifically

[110] Council Regulation 1215/2012, 2012 O.J. (L 351) 1 (EU).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

define the "Effect Test" (where the harm occurs) to prevent foreign platforms from hiding behind complex corporate structures.[111]

Ratification of the Hague Judgments Convention (2019): To overcome the illusion of enforcement, India must formally join the Hague Convention.[112] As of March 1, 2026, this convention entered into force for Montenegro and Albania, with Andorra following on June 1, 2026. By joining this 33-member bloc (including the EU and UK), a decree passed by an Indian Consumer Commission would become legally enforceable against a merchant's assets in any of these territories, turning "Hollow Victories" into real redressal.[113]

2. Strengthening Transparency and Technical Compliance

Codification of the "Country-of-Origin" Filter: While the Legal Metrology Amendment (February 2026) introduced Rule 6(10A), this requirement should be formally integrated into the Consumer Protection (E-Commerce) Rules, 2020. This codification would allow the CCPA to impose strict penalties (including platform bans or high-value fines) for false origin disclosures or the failure to provide functional filters by the July 1, 2026, enforcement deadline.[114]

Refining Legal Definitions of "Origin": The law must move beyond vague labels. We recommend a three-tiered definition of "Country of Origin" in the Legal Metrology Rules: (i) Place of Manufacture (where the core value is added), (ii) Place of Assembly, and (iii) Port of Exportation.[115] This prevents country-of-origin manipulation, where products are slightly modified in a third country to bypass trade filters.

Mandatory Platform Verification & Audits: E-commerce intermediaries should be legally required to verify and certify all origin data provided by sellers. This should not be a one-time check but a continuous process audited periodically by independent regulatory bodies. By shifting the Duty of Care to the platform, the state ensures that transparency tools are grounded in verified facts rather than unmonitored self-declarations.[116]

3. Technological and Institutional Evolution

Establishing Global ODR Platforms (G-ODR): India should lead a global Online Dispute Resolution portal in collaboration with UNCITRAL and the Hague Conference, an initiative India championed in April 2025.[117] Unlike simple video links, this G-ODR should use AI-driven mediation and smart contracts to automate refunds and payment reversals once the Commission issues a digital order.[118] This would solve the lack of technological infrastructure by creating a fast, borderless judicial lane for low-value, high-volume e-commerce disputes.

---

[111] ZHENG SOPHIA TANG, ELECTRONIC CONSUMER CONTRACTS IN THE CONFLICT OF LAWS 45–50 (2d ed. 2018).
[112] Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, July 2, 2019, 2131 U.N.T.S. 187.
[113] See Status Table: Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, HCCH, https://www.hcch.net. (last visited Mar. 26, 2026, 2:00 PM)
[114] Legal Metrology (Packaged Commodities) Amendment Rules, 2026, r. 6(10A), Gazette of India, pt. II sec. 3(i) (Feb. 13, 2026).
[115] Rules of Origin (Non-Preferential) under the Customs Act, 1962 (Proposed 2026 Guidelines).
[116] Christiane Wendehorst, Consumer Protection and the Digital Services Act, 12 J. EUR. CONSUMER & MKT. L. 1, 4 (2023).
[117] U.N. Comm'n on Int'l Trade L., Note by the Secretariat: Inclusive Global Legal Innovation Platform on Online Dispute Resolution, U.N. Doc. A/CN.9/1224 (Issued on Apr. 14, 2025).
[118] UNCITRAL Model Law on Automated Contracting, G.A. Res. 79/101 (2024).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Inter-Agency Cooperation Framework: To address overlapping competencies, a formal "Digital Enforcement Taskforce" should be created, comprising the CCPA, Ministry of Commerce, MeitY, and the Data Protection Board. This would prevent Regulatory overlap.[119]

4. Empowering the Digital Citizenry

National Digital Literacy Campaigns: Transparency tools are only effective if consumers understand them. The government must launch national campaigns linking product origin to jurisdictional implications. Consumers should be educated to recognise that buying from a verified domestic-compliant seller provides a legal safety net, including the use of the e-Jagriti portal, which handled 1.35 lakh cases in 2025.[120]

[119] Digital Personal Data Protection Act, 2023, § 19.
[120] Press Information Bureau, Ministry of Consumer Affairs Reports Disposal of 1.35 Lakh Cases via e-Jagriti Portal in 2025 (Issued on Jan. 10, 2026).