

Research Article

Laws Governing E-Commerce in The Era of Industry 5.0

Abdul Sakib Majid¹ and Shazia Kousar²

¹Ph.D. Scholar, Department of Law, Gurugram University, Haryana

²Lecturer, Dogra Law College, Jammu

*Corresponding Author

Abdul Sakib Majid

(sakibmajid25@gmail.com)

Article History

Received: 28.02.2026

Accepted: 23.03.2026

Published: 09.04.2026

Abstract:

The quick development of digital technologies and the start of Industry 5.0 have caused major changes in the commercial world, resulting in difficulties with regulations and legal issues in e-commerce. The paper explores the different laws that oversee online sales, with special focus on how technology and human needs affect commerce. It explores how laws at the national and global levels, including those for consumer protection, data privacy, handling digital contracts and intellectual property rights, are responding to current digital advances. Industry 5.0 which blends human insight with advanced technology, has raised the importance of fast and adaptive legal measures. New technologies such as AI, blockchain and IoT, are now changing the way e-commerce operates, so laws and obligations in digital commerce have to be reviewed. The contribution examines the role of novel approaches in modernising legislation and points out that regulatory sandboxes and flexible laws improve the safety and reliability of digital markets. The research uses a comparison of laws and case studies to find important areas where regulations are not strong enough and then offers strategic changes to strengthen and update the laws. In the end, this paper helps advance the discussion about forming a reliable legal framework that encourages the sustainable growth of e-commerce, following Industry 5.0 standards.

Keywords: E-commerce, Industry 5.0, Innovation, Digital Regulation, Legal Frameworks.

Copyright @ 2026: This is an open-access article distributed under the terms of the Creative Commons Attribution license which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use (NonCommercial, or CC-BY-NC) provided the original author and source are credited.

INTRODUCTION

Blending leading digital technologies and human priorities which is known as Industry 5.0, is bringing a revolution to global business. Industry 5.0 puts a strong focus on being more sustainable, meeting human needs and being flexible. In this view, e-Commerce tries to make things easier for people, protect the environment and promote trust among society. As stated by the European Commission, Industry 5.0 is about using research and innovation to achieve a sustainable, human centric and resilient industry because of this shift, new legal issues emerge. Indian people and companies now conduct transactions using AI in online markets, blockchain for supply chains and devices that order products independently. Laws that were put in place during previous ages of industry should respond quickly to changes caused by Industry 5.0.

In this paper, the Indian legal framework for e-Commerce is studied against the background of Industry 5.0 and some global strategies are explored briefly as a contrast. It considers four fundamental areas: keeping consumers safe, protecting their privacy and safety online, handling contracts by digital means and ensuring the rights of creators with intellectual property. The report also discusses the ways AI, blockchain and IoT are affecting e-Commerce and leading to new legal problems. We will analyse whether laws including the Information Technology Act, 2000 and the Consumer Protection Act, 2019 (particularly its e-Commerce rules), are sufficient for this new way of doing business.

Using landmark court cases, both inside India and abroad, we will highlight where principles are at work and where they should be re-examined. In addition, we analyse new regulatory tools (such as sandboxes) and suggest steps to help India develop a modern and aligned digital commerce industry.

INDUSTRY 5.0 AND THE DIGITAL COMMERCE LANDSCAPE

Industry 5.0 is a blend of human centric and sustainable practices with automation, which is impacting the fast expansion of the Indian e-commerce industry. Nevertheless, conventional laws find it difficult to deal with cross border trade, automated trading and sustainability issues.

Regions such as the EU, USA among other nations globally have revised laws governing digital commerce to control the platform, data security and online commerce. By comparison, India has regulations that have been undergoing change, and there is a need to review and reinforce laws to meet Industry 5.0 challenges.

INDIAN E-COMMERCE REGULATORY FRAMEWORK

Important e-Commerce laws in India are the Information Technology Act, 2000 (as amended) which sets rules for online activities and transactions; the Consumer Protection Act, 2019 which introduced new sections on e-Commerce; laws made for each sector (payments, telecom, etc.); and also particular rules (including the e-Commerce Rules 2020 and the Intermediary Guidelines and Digital Media Etiquette Rules 2021).

Information Technology Act, 2000 (IT Act)-The digital legal landscape in India started with the IT Act, which acknowledges digital signatures, electronic contracts and intermediary liability and punishes cybercrimes. Although it is not a direct e-commerce law, it helps in the online trade by verifying the electronic contracts and electronic evidence. Nevertheless, even with the amendments, it primarily revolves around cybercrime and might not be effective in emerging issues in Industry 5.0 like AI and privacy.

Consumer Protection Act, 2019 (CPA 2019)- Old consumer law from the 1986 Act was replaced with the modern CPA 2019. A major point is that it teaches us what e-Commerce is and what's owed by online retailers. Chapter VII, specifically Sections 94 through 96, is designated to E-Commerce, the first rule gives the government powers to establish guidelines for online markets. As a result of this authority, the Consumer Protection (e-Commerce) Rules were published on 23 July 2020. All e-Commerce players must follow many Rules that require them to be open, fair and responsive to complaints. By law, all platforms have to make the seller's contact details, return policies and fee structure visible to buyers. They have to choose a grievance officer who will address any customer's complaint within 48 hours and settle it within a month. Notably, the Rules work outside India as well: those e-Commerce businesses based abroad that sell to Indian customers must follow them. In essence, the Consumer Protection Act and its e-Commerce Rules make online sales more about the consumer.

Intermediary Guidelines (IT Rules 2021)-The Intermediary Guidelines 2021 stipulates that digital platforms, such as e-commerce marketplaces, should employ compliance officers, sort out complaints and take down illegal content within established deadlines. Although they are primarily referenced towards digital intermediaries, they can also be applied to marketplaces by demanding due diligence and revealing the sources of illegal content. Nevertheless, the intellectual property infringements are not covered under safe harbour protection provided under Section 79 and platforms should take action against counterfeit listings on receiving notification.

The Digital Personal Data Protection Act, 2023- In August 2023, India passed its first complete data protection law. It will be implemented in October 2024. Under the Act, e-Commerce platforms must obtain user agreement, restrict how data is used, ensure safety measures, name a data protection officer and form mechanisms to deal with concerns. With GDPR, data subjects have the right to request their data, change it, delete it and move it. Compared with earlier ideas, the DPDP Act limits its authority even as it greatly increases the rights of internet users and makes companies more accountable online. For the first time, e-Commerce companies have to follow clear privacy rules identical to those in the EU's GDPR. For those who read it: the DPDP Act gives permission to handle data without consent in officially approved exceptional cases (state functions, emergencies). In brief, there is now a general privacy law in India that will include all e-Commerce players.

Other Relevant Laws-There are other laws that also influence e-commerce in India. Online payment is governed by the Payment and Settlement Systems Act, cross border transactions governed by FEMA and the old IP laws still govern online trade. The legal system is consequently a combination of more senior laws and the more recent ones such as the CPA 2019, the DPDP Act 2023 and the IT Rules 2021. Nevertheless, the swift advances in AI, automated contracts and decentralized finance are causing a necessity to implement additional changes in the law.

CONSUMER PROTECTION IN DIGITAL COMMERCE

The e-commerce regulation in India is focused on consumer protection. Consumer Protection Act 2019 and E-Commerce Rules mandate platforms to publish their identity, seller and customer service and service details, have a grievance officer and provide solutions to complaints within stipulated deadlines. The marketplace and inventory models should provide the

transparency of prices, products information and advertising with the exclusion of fabricated reviews and fake products. Breaking the law is penalized and even to foreign e-commerce websites that sell in India, the law takes effect.

Dark Patterns and Misleading Practices- Many e-commerce businesses now use design flaws like feeling a false rush to purchase or hiding costs from customers to encourage people to spend more. Indian law now considers these types of discrimination to be unfair. What the CPA considers an unfair trade practice (Sec. 2(47)) is quite broad and in late 2023 the Central Consumer Protection Authority (CCPA) issued guidelines to stop 13 types of dark patterns in online buying. This means using techniques like drip pricing (charging fees at the last minute), confirm shaming, bait and switch and subscription traps. This decision by the law to name such tricks as “unfair practices” is consistent with global action: EU law prohibits secret fees and urgent prompts and agencies like the UK’s CMA are scrutinising these practices. Advertisements that use false time limits (countdowns that reset themselves) are specifically not allowed in India. They prove that India cares about providing careful protection for digital users.

Case Law Example- Reclaiming Your Rights When Shopping Online. Since CPA 2019 is fresh, Indian courts are just getting started when it comes to deciding e-Commerce matters. Even so, judgments from the past are still relevant. In *IRCTC v CBI* (2022), the Supreme Court looked at online ticket transactions and decided that clicking to purchase was as binding as signing a contract. In addition, the *Satish Chand Gupta v. Jindal Stainless* considered that telephone calls between the parties count as verbal agreements in a contract. Likewise, courts would recognize click to buy as an acceptable transaction form. It was decided in *Specht v Netscape* in the U.S. that online terms must be brought to users' attention before their agreement is considered binding. All the aspects of making and accepting an offer for a contract and the actual payment can be carried out through electronic tools. Just like in *Trimex International FZE v Vedanta Aluminium*, the Supreme Court approved an online contract without a stamp since it recognized the freedom of online contracting. All of these show that consumer agreements made online are protected by the law, requiring the same laws to protect them as other agreements.

DATA PRIVACY AND SECURITY IN E-COMMERCE

At the centre of e-Commerce is the gathering and processing of personal information such as names, addresses, payment details and what users do online. As a result, privacy and security laws are extremely important. In 2023, the Supreme Court recognised privacy as a main right for Indians *K.S. Puttaswamy (Retd.) v Union of India*, but until then, no law protected individual data. There were very few provisions in the IT Act 2000: Section 43A applied liability for breach of “sensitive personal data” to corporates who did not implement reasonable security and Section 72A penalised anyone who exposed another’s personal information in violation of a lawful contract. However, most of the time these sections were unused (since they only covered breaches of contract in a fiduciary role and the penalties were low).

The Digital Personal Data Protection Act, 2023 will provide explicit user consent to process their personal data, force companies to have statements on privacy, and will also enable users to access, revise or delete their personal data. Data fiduciaries should also apply security measures and disclose data breaches to the Data Protection Board. In the case of e-commerce, user consent is needed to gather data to do marketing or profiling, but there are government exceptions on the need to do this to enhance security or due to emergency.

DPDP Act gives the consumers more control over their personal data, adjudicating the right to access, delete, and withdraw consent over their data and imposes penalties up to Rs. 250 crores in case of violation. It is consistent with the international privacy standards like the GDPR but allows more legitimate use of data.

With the increasing cyber threats against e-commerce, agencies such as CERT In and police involve themselves in investigations, and payment security regulations and standards such as tokenization and PCI DSS improve this security. Some of the proposed laws such as Digital India Act are meant to enhance additional digital security and regulatory measures.

Case Law-Even though there are no Indian cases of e-Commerce privacy, *K.S. Puttaswamy v Union of India* ruled that informational privacy should be included under Article 21. It was made clear by the Court that technology can weaken autonomy when it is abused in surveillance or through the misusing of data. Therefore, when an online retailer immigrates anonymous data, applies AI that unintentionally discriminates, those actions may subject them to restrictions of privacy. Across the globe, *Google Spain v AEPD* granted people the right to have their personal data removed from Google search results. Though the DPDP Act doesn’t cover much, user control is now being discussed more openly. Privacy actions happening in other countries such as class actions in California’s CCPA and proceedings under GDPR, will guide how India’s courts interpret online information practices.

ELECTRONIC CONTRACTS AND DIGITAL TRANSACTIONS

Online transactions are made possible because electronic contracts can be enforced in the law. Indian law has modified its

contract rules to fit the needs of digital trade, just like many other countries. The IT Act, 2000 expressly permits the use of electronic contracts. Section 10A clarifies that electronic formation of a contract does not make it automatically unenforceable. Considering Section 4 and 5 about digital signatures, messages sent via email or e sign are considered valid agreements. This point was stated by the Supreme Court in *Trimex Int'l FZE v Vedanta Aluminium Ltd.*, an email contract was considered enforceable since autonomy for parties was valued more than meeting specific technical standards for a contract.

The security related to Digital Signatures and their Validity. The law explains what an electronic signature is and allows them to be just as valid as traditional “wet ink” signatures (but excluding a few documents). The SC declared in *National Insurance Co. Ltd. v Pranay Sethi* that an electronically signed insurance contract is valid. It stated that a continuous certification process within asymmetric encryption (government issued ID system) makes an e signature both trustworthy and legit. Therefore, when an e signature is used, clauses for written and signed agreement are met too. Still, when the section was created, it did not cover contracts for the sale of land or other real estate. The reason for this was addressed in 2022 through an amendment realising that contracts for selling properties can now be carried out digitally. Because of this, most contracts can now be made, completed and finalised online.

One problem that keeps occurring is the Indian Stamp Act, 1899 is in order for an instrument with stamp duty to be chargeable, current law requires that it be executed (signed). A central question related to e contracts is if giving an electronic consent is enough to count as agreement. The *Trimex* case showed that it might be inefficient to insist on stamps for transactions made online. Limiting e agreements to require stamping, as called for in the *Great Offshore v Iranian Offshore* case, would put digital transactions at risk, according to Justice Bhandari. Yet, in *N.N. Global Mercantile v Indo Unique Flame*, a majority of 3:2 decided that even unstamped digital arbitration agreements cannot be submitted for consideration until all fees are paid. The case put into question if e contracts signed without e stamping could actually be enforced. For the moment, many prefer to use e stamps or print and stamp a digital document just to stay safe. Because stamp laws do not fit with Industry 5.0’s goal to minimise friction, they are in need of change.

Courts have long addressed the validity of electronic contracts. In *Specht v Netscape Communications Corp.*, the court stated that online terms should be prominently displayed to the users and should not be concealed under browse wrap agreements. Electronic contracts are accepted in India whereby there is a clear offer and acceptance like use of emails or clicking acceptance buttons. Section 10A of the Information Technology Act and principles of the UNCITRAL Model Law on Electronic Commerce validate such contracts. Blockchain smart contract is not regulated specifically in India, however, when the key elements of a contract are present, they can be enforced under the general contract law, yet problems such as inaccuracy in code can create legal challenges.

Click wrap agreements are mostly used in online platforms that allow users to accept the general terms with clicking consent. Indian courts tend to uphold such contracts provided that they are normally presented in a clear and non-unconscionable manner. Supreme Court in *TrimexInternational FZE Ltd. v Vedanta Aluminium Ltd.* acknowledged that, the formation of a binding contract is possible where there exist clear offer and acceptance despite the electronic communications. Therefore, the contracts reached due to the use of online consent processes are accepted as valid contracts under the Indian law in case the conditions are communicated reasonably to the user.

INTELLECTUAL PROPERTY RIGHTS (IPR) INE-COMMERCE

Intellectual property (IP) protection problems have become more challenging due to E-Commerce. Pirated media, fake goods and unauthorised brand ideas can all be posted on these marketplaces online. Both Indian patent and copyright law and new e-commerce regulations govern this issue.

If something is done online that infringes on copyright, the Copyright Act, 1957 (as amended) allows you to ask for injunctions and compensation. Intermediaries now enjoy certain protection: if a website or platform has a proper system and responds to takedown notices, it cannot be sued. The law follows the same approach as the “notice and takedown” rule in the U.S. Digital Millennium Copyright Act (DMCA). Just as for patents, the Trade Marks Act, 1999 also prohibits “ambush commerce”, in addition to other provisions. Introducing goods as real when they are fake using a trademark leads to both criminal charges and lawsuits. Earlier this year, amendments included Section 135 which prevents the use of software or devices designed for illegal trademark use online. Generally, it is brand owners who take action by issuing notices to stop online infringement in India under the IT Act. According to the Rules, intermediaries must show record of IP violations by third parties and take action on directions issued by courts or the police.

The Consumer e-Commerce Rules touch on issues related to IP in a different way. A record needs to be kept of sellers who have offered IP infringing goods before. For now, sellers stay on the platforms unless the company decides to ban them. In this way, platforms are expected to keep information accessible, but courts, police or the platform’s own rules decide when to act. When a company learns that its trademark is being used on a counterfeit listing, it can send a notice under Section 69 of the IT Act and the platform should block the listing within 36 hours. If the procedure is not followed, the company

could lose the protection under Section 79.

Case Law-It has been proven that Indian courts are actively protecting IP on the internet. For example, in *Yahoo! Inc. v Akash Arora* the Delhi High Court concluded that displaying a “Yahoo” advertisement in response to the search “Yahoo” was likely to confuse consumers and break trademark rules. Just recently in *CPI Securitas v BCSBI (2022)*, the Supreme Court stated that it is a crime, both in-store and online, to sell duplicates with genuine trademarks. According to *Indian Performing Right Society v Sanjay Dalia*, playing music under copyright on public sites without getting a licence is considered an infringement. These cases, made before CPA 2019, show that courts have been flexible in applying IP law to new ways of doing business. Many cases related to e-Commerce intellectual property are seen worldwide, as platforms such as eBay and Amazon regularly have conflicts with fake items appearing on their sites. WIPO calls on countries to implement steps to improve the enforcement of online IP rights such as by selecting locations where notifications about court orders will be held. The Trade Marks Rules from 2022 by India shows that the country is paying closer attention to online problems.

Both existing and new rules are used by Indian law to protect intellectual property in online transactions. Yet, platforms have to keep up with a million listings, meaning they rely on advanced tools like image recognition for monitoring. The Safety Pledge from the CCPA is part of the government’s plan to improve the safety of online shopping. It covers confirming that goods are genuine and that IP is respected which brings industry actions into line with IPR laws. Even so, it is important to reinforce procedures for getting infringing content removed and to supply those with rights with greater resources to do it.

EMERGING TECHNOLOGIES TRANSFORMING E-COMMERCE

Artificial Intelligence (AI)

AI is revolutionizing e-commerce by using recommendation systems, chatbots and dynamic pricing but it also causes concern over misinformation, discrimination and black box decision making. India does not have an explicit AI law yet, but policymakers are beginning to think of a risk-based framework akin to the one in the EU, with more stringent rules of high-risk systems.

The AI in e-commerce is partially governed by existing consumer protection and cyber and privacy laws, with such policies as dark pattern in place to combat manipulatory actions. In the future, regulation might encompass transparency, algorithm audit and explainability to warrant fair and responsible use of AI.

Blockchain and Digital Payments

Blockchain has the potential to support e-commerce through making the supply chains more transparent, facilitating automated smart contracts and cross border payments. In India, the e Rupee is being promoted by RBI to enable digital transactions; however, the cryptocurrencies provided by the private sector are regulated.

Nonetheless, there is still legal ambiguity in terms of jurisdiction, smart contracts recognition and enforcement. To overcome these challenges, clarification of the legal status of blockchain evidence and smart contracts and revision of the law like the stamp act might help.

Internet of Things (IoT) and e-Commerce

The IoT devices to be able to make purchases automatically include smart fridges or voice assistants, which in turn evoke legal concerns regarding consent, responsibility and unauthorized use. There are liability issues such as security risks like hacking that allow fraudulent orders. In the Consumer Protection Act 2019, manufacturers or platforms might be liable to faulty or unsafe IoT products resulting in consumer loss.

At present, conflicts can be resolved by referring to the existing legislation such as the CPA, IT Act and product liability regulations, but in the future, India might want to think over the specific IoT laws with compulsory security provisions.

Regulatory Innovations: Sandboxes And Adaptive Laws

India is promoting e-commerce innovation in the form of regulatory sandboxes and relaxed regulation where companies can experiment with technologies such as AI, blockchain and new payment systems with oversight. Programs like RBI sandbox and the suggested Digital Commerce Sandbox allow experimentation, and risks are also identified early.

One way to achieve the goal of responsible innovation as well as consumer protection is the suggested Digital India Act that would allow developing a flexible legal framework that can be updated on a regular basis, and principle-based guidelines and industry cooperation, including the Safety Pledge.

GLOBAL CONTEXT AND COMPARATIVE INSIGHTS

European Union-EU regulations like the Digital Services Act demand large online platforms to be transparent and risk-assessed and offer minor protection to smaller online platforms in terms of limited liability. EU consumer regulations also enable purchase cancellation in 14 days on the Internet and demand the publication of prices and guarantees. India might be in line with these trends by offering the same cooling off return right like 7 days no questions asked refund policy on the purchases made at e commerce.

United States-The Federal Trade Commission and state legislation, such as the California Consumer Privacy Act that provides users with information rights over their data, regulate unfair practices in the U.S. The DPDP Act in India also regulates personal data, but it may be enhanced to rights, e.g., data portability. Such U.S. actions on copyright and platform liability and heightened focus on large e commerce platforms represent a global shift of greater protection of consumer and competition, seen in India by Competition Commission inquiries into large e commerce platforms such as Amazon and Flipkart.

Other Jurisdictions-Countries such as Singapore, the UK and Australia have revised e-commerce laws to guarantee digital goods refunds and anti-unfair subscription practices. India has also embraced comparable consumer safeguards including transparent pricing and disallowing of fake reviews as it shifts towards the equal treatment of online and offline sales. With the world organizations such as the OECD and the WTO coming up with cross border e commerce regulations, India needs to bring its laws up to date with international practices including Industry 5.0 issues such as environmental claims.

POLICY RECOMMENDATIONS FOR INDIA

For a green, strong e-Commerce environment that fits Industry 5.0, the following policies should be considered:

Strengthen Privacy Enforcement- Complete enforcement of the DPDP Act by ensuring that there is a robust oversight body to check compliance and bring punitive action against misuse of data. Enforce user rights (e.g. data portability) and easy withdrawal of consent and encourage awareness campaigns to the general public to facilitate improved protection of their digital privacy.

Modernize Contract and Stamp Laws-Support digital transactions by removing or simplifying stamp duty on electronic contracts by amendments or easy e stamping systems. Identify electronic signatures and impose transparent regulations on click wrap agreements under section 10A, as well as allow certification of smart contracts. These provisions can be consolidated in a specific Digital Signature Act that falls under Digital India Act.

Expand Consumer Protections-Implement a cooling off period of 7 days to e-commerce purchases, increase the effectiveness of resolving cross-border complaints by introducing collaboration with CCPA and international regulators, and improving the National Consumer Helpline using AI chatbots and multilingual support. Make sure that there are convenient, easy-to-use platforms based on the WCAG standards and update the e-commerce regulations on a regular basis to tackle the new challenges and threats like subscription traps.

Enhance IPR Enforcement-Establish a central registry of infringement notices that should be respected by all platforms, which would make the enforcement less burdensome. Offer legal safeguarding to platforms that take down infringement listings and create a single system of complaint, potentially under the CCPA, for cross border infringement. Incentivize anti-counterfeit measures such as the use of a blockchain tag where legal protections are provided and the laws are in tandem with the international customs against misrepresenting online trademarks.

Regulate Emerging Tech-Establish special guidelines concerning new technologies in e-commerce. Make AI generated pricing or offers be labeled and ban discriminatory algorithms and make AI applied to payments and credit be high risk. Admit controlled innovation in blockchain and crypto, accept lawful smart contracts as legitimate contracts and impose security principles and disclosure necessities on IoT apparatus, and treat anomaly in buying with hacked equipment as an unfair trade practice.

Promote Sustainability-In e commerce by enhancing the Greenwash Guidelines 2024 to stipulate transparency on use of carbon and recyclability of products and promoting recyclable packaging and buy back incentive programs by tax exemptions. Sellers must also be mandated by law to dispose of packaging waste and facilitate circular models such as product as a service and make e commerce consistent with Industry 5.0 values.

Facilitate Innovation via Sandboxes-Create an e-commerce sandbox under an appropriate ministry where startups can test technologies such as drone delivery, warehouse robots and blockchain supply chains. Temporary regulatory softening would permit controlled testing over a period of one year, which would assist the authorities in testing their effects on consumers before making official regulations.

Adaptive and Principled Regulation-The regulation must be open to changing technologies. Rather than providing a list of

forbidden strategies, legislation must compel online advertising to be transparent, truthful, and reasonable yet leave the companies to revise the principles. Programs such as the Safety Pledge promote responsible platform use and a periodic review or sunset clause can be put in place to ensure that laws are not obsolete to Industry 5.0.

International Cooperation-India must encourage global e-commerce systems and frameworks using WTO regulations that safeguard consumer and data rights, embrace privacy adequacy arrangements in bilateral business, and collaborate with regulators in the EU, US and others to devise shared standards in digital products, AI and interoperable payments.

Skilling and Awareness-An effective e-commerce architecture necessitates the creation of community consciousness about online rights, trained officials to manage the digital evidence and prudent business ethics to assist the regulators. These measures would assist India to develop a safer and more resilient digital marketplace that fits the principles of industry 5.0 in terms of sustainability, human centric growth and great data security.

CONCLUSION

India is in its critical phase of digital commerce. Such technological advancements as AI, blockchain and IoT are efficiency-saving and personalized, but they pose a threat to the established legal provisions. Although laws like the Consumer Protection Act, 2019 and the IT Act have enhanced consumer protection and data regulation, loopholes still exist in areas like contract enforcement, privacy and technology specific regulation.

Comparisons with other jurisdictions such as the EU and USA indicate that India can embrace the best practice on privacy and platform governance and ensure laws remain flexible to technological change using tools such as regulatory sandboxes and revised laws such as the Digital India Act.

All in all, innovative and secure e-commerce involves collaboration between regulators, consumers, and business. India can develop a robust digital marketplace by means of clear laws, social corporate citizenship, and knowledgeable citizens in line with the human centric ideals Industry 5.0.

REFERENCES

1. https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en. (Last visited on May 25, 2025).
2. Ibid.
3. Supra note 1.
4. <https://www.upguard.com/blog/digital-india-act>. (Last visited on May 25, 2025).
5. <https://www.indialaw.in/blog/civil/consumer-protection-e-commerce-rules/>. (Last visited on May 25, 2025).
6. Ibid.
7. <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en#:~:text=Entities%20responsible%20for%20collecting%2C%20storing%2C,have%20a%20detrimental%20effect%20on>. (Last visited on May 25, 2025).
8. Ibid.
9. Supra note 5.
10. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2114829>. (Last visited on May 25, 2025).
11. Ibid.
12. AIR 2003 SC 36.
13. 11 ILED 832.
14. (2017) ibclaw.in 415 SC.
15. (2017) 10 SCC 1.
16. <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en>. (Last visited on May 25, 2025).
17. Ibid.
18. Supra note 16.
19. ILEC 060 (CJEU 2014).
20. Supra note 14.
21. 2017 (16) SCC 680.
22. 2008 (14) SCC 240.
23. 2023 INSC 1066.
24. 306 F.3d 17 (2d Cir. 2002).
25. 78(1999) DLT 285.
26. AIR 2015 SC 3479.
27. <https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?center=india&lang=en>. (Last visited on May 25, 2025).

28. <https://thepayers.com/payments-general/rbi-supports-fintech-innovation-with-on-tap-regulatory-sandbox--1273165#:~:text=RBI,credit%20scoring%2C%20and%20many%20more>. (Last visited on May 25, 2025).
29. <https://www.upguard.com/blog/digital-india-act#:~:text=The%20upcoming%20Digital%20India%20Act,day%20technological%20issues>. (Last visited on May 25, 2025).
30. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2114829#:~:text=Further%20to%20strengthen%20consumer%20protection%2C,addressing%20false%20claims>. (Last visited on May 25, 2025).