INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"SAFEGUARDING INDIAN E-COMMERCE: LEGAL MECHANISMS, CYBERSECURITY CHALLENGES, AND REFORM IMPERATIVES"

AUTHOR – POOJA.S, STUDENT AT CHRIST UNIVERSITY, BANGALORE

BEST CITATION – POOJA.S, "SAFEGUARDING INDIAN E-COMMERCE: LEGAL MECHANISMS, CYBERSECURITY CHALLENGES, AND REFORM IMPERATIVES", INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (1) OF 2026, PG.1160-1176, APIS – 3920 – 0001 & ISSN – 2583-2344. DOI - https://doi.org/10.65393/NUBG8740

ABSTRACT

The steady growth in India's e-commerce sector is expected to reach above USD 363 billion by 2030. This development highlights the industry's substantial influence on the digital economy. However, this escalation has led to shortcomings, including cyber and security threats such as data breaches, payment fraud, and product liability. They undermine consumers' trust, reputation and financial status of the E-commerce platform.

This paper critically examines the prevalent cybersecurity threats targeting e-commerce platforms. It analyses the efficient working of current legal frameworks, compliance by platforms and legal accountability for the resulting harm utilising safe harbour principles.

The Research study employed is a qualitative doctrinal and case law-based analysis. Preliminary findings indicate weak enforcement due to fragmented regulation, inadequate penalties, vague definitions, and uncertain legal accountability resulting from the erosion of conditional immunity under Section 79. Geographically confined to the Indian Context, this paper seeks to make a practical contribution by proposing reform recommendations which aim to clarify liability, compliance mandates, enhance grievance redressal mechanisms, foster consumer trust, and improve cybersecurity resilience within the e-commerce ecosystem.

Keywords: Cyber Law, Cybersecurity Challenges, Data Privacy, Digital Consumer Rights, E-Commerce Regulation

I. INTRODUCTION

Our Nation's e-commerce industry is one of the fastest-growing digital markets in the world. It has a compound annual growth rate of 21.5%. This was achieved due to high internet usage, global connectivity, online payment mechanisms, consumer preferences, speedy and convenient nature, technological advancements, and government-led initiatives such as Digital India. It was further accelerated during the COVID-19 pandemic.

However, this growth has exposed the sector to the emerging risks, such as cybercrimes, which include identity theft, phishing, data breaches, payment fraud, and ransomware, and others. It lessens the platform's integrity and credibility, erodes consumer trust, and poses risks to our digital economy. Multiple legal frameworks like the IT Act 2000, the Consumer Protection Act 1986 and 2019, E-commerce directives of 2020 aid in addressing this issue.

Primarily, the IT Act of 2000 gives the foundation for governing cyber law. It provides legal recognition to electronic transactions, contracts and signatures. The Consumer Protection Act 2019 and the E-commerce Rules 2020 extend the definition to include online consumers. They offer grievance redressal and penalties for

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

offences such as product liability, deficiency of service, unfair trade practices and others. The Digital Data Protection Act of 2023 provide privacy safeguards and specific consent-based mechanisms for users. It states rights and duties for data fiduciaries and data controllers. The CERT-In Guidelines mandate cyber breach reporting and an incident response mechanism. Yet, the e-commerce industry faces challenges like jurisdictional ambiguity, lenient penalties and ineffective enforcement. Therefore, this paper aims to critically examine the efficacy of the present legislative safeguards, assessing their impact on platform compliance and consumer protection[2641].

The reports indicate that Cyber fraud caused losses of over $11,000 crore in the first nine months, with further escalation being expected. High-profile breaches are also noted in Online retail and fashion delivery services, illustrating systematic vulnerabilities, delayed reporting and lack of consumer redress. these persistent challenges indicate the gap between legislative intent and practical enforcement.

This study is limited to India's landscape and adopts a doctrinal qualitative legal methodology. It critically analyses judicial precedents that directly shape intermediary liability and consumer harm, including landmark rulings on privacy, such as the K.S. Puttaswamy case[2642] and safe harbour principles discussed in the Shreya Singhal case and Google vs Visaka[2643]. Specific e-commerce disputes like Flipkart Internet Pvt Ltd v State of NCT Delhi and Amazon Seller Services v Amway India Enterprises are also examined.

The paper argues that despite comprehensive legal statutes, the present cybersecurity regime remains more reactive than proactively preventive. To bridge this Governance and enforcement gap, the paper proposes an integrated reform package through strong governance measures, an accountability-based approach, strict compliance mechanisms, sectoral harmonisation and strong consumer protection to shape a secure and trusted e-commerce ecosystem.

The study is structured as follows: Part 2 identifies and categorises the major cybersecurity threats which affect Indian e-commerce platforms and their stakeholders. This includes phishing, identity theft and others. Part 3 examines the present legal framework which governs cybersecurity in Indian e-commerce. It aims to assess the compliance obligations and preventive mechanisms of platforms.

Part 4 evaluates the legal liability and accountability of e-commerce platforms in cases of cybersecurity breaches. Emphasis is given on safe harbour immunity, consumer reliefs, and judicial precedents. Part 5 identifies gaps and enforcement challenges in the current legislation and gives reform proposals and policy recommendations. The major objective is to enhance cybersecurity governance, platform accountability, and consumer trust in our nation's e-commerce sector. In conclusion, the crucial need to have a risk-based governance and accountable digital environment is highlighted to protect consumers of e-commerce sector.

II. MAJOR CYBERSECURITY THREATS BY INDIAN E-COMMERCE

The Digital era gave rise to the revolutionised Global commerce, which is now highly automated and has an interconnected internet economy. This paved the way for user-friendly e-commerce applications that collect vast amounts of data. Consumers trust that the services will protect their data properly and secure it from harmful threats. Nevertheless, since data, being the most valuable asset, is highly prone to being misused.

With increased dependency on digital information and online platforms, cybercrimes like data breaches, identity theft, phishing, etc, are becoming more frequent. This creates a heightened social and economic need for the

[2641] The Digital Personal Data Protection Act, 2023, No. 40, Acts of Parliament, 2023 (India).
[2642] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, 32 (India).
[2643] *Google India Pvt. Ltd. v. Visaka Industries*, (2020) 4 SCC 410 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

platforms to employ cybersecurity practices to protect data from such illegal practices. Cybersecurity essentially refers to the practice of protecting digital information, networks and systems from unauthorised access, corruption and misuse. Its core objective is to maintain the integrity, confidentiality, authenticity and availability for the authorised users for the intended purpose. However, a productive balance must be maintained between the crucial value of data and the inherent risk of exposure in this sector.

A. Identification of threats

E-commerce platforms face various cybersecurity threats, as follows:

- **Phishing Attacks:** The Sensitive data, like personal, financial information, etc, is being obtained from users by using fake websites or emails that imitate legitimate platforms.
- **Malware:** The System integrity gets compromised through malicious software such as viruses, worms, and ransomware
- **Data Breaches:** Unauthorised access to sensitive customer or business data is gained through technical or human vulnerabilities.[2644] It is most common in e-commerce platforms.
- **Distributed Denial of Service (DDoS) Attacks:** They overwhelm servers with excessive traffic to cause outages and disrupt the user experience.
- **Insider Threats:** Employees or contractors inside the entity having legitimate access to sensitive information can cause data theft or sabotage of sensitive information.
- **IoT Vulnerabilities:** It refers to the Exploitation of interconnected devices to gain unauthorised access to systems.

Cyber-attacks on e-commerce platforms are usually orchestrated by Cybercriminals, hacktivists/ state-sponsored Actors who exploit shortcomings for disruption and financial gain.[2645]

(i) Data Breaches

It occurs when there is unauthorised access to sensitive customer or business data, including personal and financial information, obtained by exploiting vulnerabilities in web applications. The process involves inserting malicious SQL code using SQL Injection into input fields, which leads to the manipulation of database queries to retrieve, modify, or delete stored information. This cybercrime follows economic losses, identity theft risks, reputational damage and consumer backlash to the affected entity[2646]

In 2018, one of the largest online retailers faced a data breach, which compromised millions of people's personal information. In the 2025 Data Breach Report, it reported an increase of 34% of attacks that exploit vulnerabilities to gain initial access compared to the 2024 [2647] This highlights the importance of strong data governance and safeguard protocols.

(ii) Phishing Attacks

This technique involves deceiving customers into revealing sensitive information like login credentials, payment details, or personal identifiers. Attackers usually create duplicates of well-reputed online services, fraudulent links, messages that appear to be from a genuine source or websites as a medium for users to log in. [2648] A notable instance was the Amazon phishing scam in which emails were sent to users claiming to have account problems. The mail redirected them to a fake login portal website. This scam caused financial losses, identity theft, and the erosion of consumer confidence. Section 67 of the IT Act deals with this offence -imprisonment up to 5 years and a fine which may extend to 10 lakhs or both.

[2644] George Caleb Oguta, *Securing the Virtual Marketplace: Navigating the Landscape of Security and Privacy Challenges in E-Commerce*, 18 GSC ADVANCED RESEARCH & REVIEWS 84 (2024).

[2645] H. Desamsetti, *Crime and Cybersecurity as Advanced Persistent Threat: A Constant E-Commerce Challenge*, 8 AM. J. TRADE & POL'Y 239 (2021).

[2646] Sukrit Garg et al., *Cyber Security's Influence on Digital Consumer Trust*, 12 INT'L J. CREATIVE RSCH. THOUGHTS 410 (2024).

[2647] Verizon, 2021 Data Breach Investigations Report (2021), https://www.verizon.com/business/resources/reports/dbir/.

[2648] *Understanding Social Engineering Attacks*, Nat'l Cyber Sec. Ctr. (2022), https://www.ncsc.gov.uk/.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

(iii) Identity Theft

Identity theft refers to the unauthorised use of personal information like names, date of birth, etc, to commit fraudulent acts and obtain financial or personal gain. Techniques such as phishing schemes using deception of users, data breaches where information is stolen, social engineering techniques, malware and spyware are used. Attackers commit acts on the stolen identity of a user, making it difficult to detect unless harm occurs. Section 66C of the IT Act prescribes a penalty for this offence- imprisonment up to 3 years and a fine of up to 1 lakh or both.

(iv) Malware and Ransomware

They are among the most critical threats in e-commerce as they lead to stealthily compromised systems. Malware is a programme or code designed to damage, disrupt, steal or gain unauthorised access to a computer, system or network. It tracks the digital activity of the affected system and misuses the stolen sensitive information of users and the platform. E.g., viruses, worms, Trojan Horses, Rootkits, Spyware.

Ransomware is a form of blackmail technique where they encrypt crucial data necessary for the organisation and demand ransom in exchange for the decryption key. These attacks made towards the affected entity, when revealed to the public, may demand closure.

(v) SQL Injection & Cross-Site Scripting (XSS)

In SQL Injection (SQLi), ALTER database queries are used to extract sensitive information by exploiting weaknesses in web-application databases. In Cross-Site Scripting (XSS), malicious scripts are injected into trusted websites to steal data or redirect users.[2649]

(vi) Denial of Service (DoS) & Distributed Denial of Service (DDoS) Attacks

In a DOS and DDOS attack, the servers are being flooded with excessive requests, thus generating enormous traffic leading to disruption of business and non-accessibility to legitimate users. [2650] Section 66F prescribes imprisonment which may extend to a life sentence.

(vii) Payment Fraud

Payment fraud includes fraudulent transactions via credit/debit cards or digital payment systems. Some of the common methods are the Manipulation of digital transactions to divert funds and Chargeback abuse.[2651] Major consequences are faced, such as Immediate financial losses, increased operating costs, scarce business resources wastage and reduction in merchant confidence.

B. Impact on E-Commerce and Trends in Cybersecurity Threats

E-Commerce platforms have far-reaching consequences across economic, reputational and legal dimensions.

The Financial losses faced include the theft of funds, ransom payment demands, costs of recovery, repair systems, security measures and legal expenses. Reputational Damage caused to the affected platform includes violation of consumer trust, reduction in sales, customer attrition and loss of long-term brand goodwill. The Legal Consequences for businesses are paying Regulatory fines, penalties for non-compliance, civil actions with respect to cybersecurity measures & data protection laws. These measures are needed to prevent risks and maintain safe e-commerce operations.

It is also necessary to know the modern patterns and evolving technological and regulatory dimensions that shape the above cybersecurity risks. Firstly, there are emerging threats which include the use of Artificial Intelligence, machine learning, and Quantum Computing. It is difficult for the platforms to detect and counter since they are

[2649] *SQL Injection: Prevention Guide*, OWASP (2021), https://owasp.org/www-community/attacks/SQL_Injection.

[2650] Shopify Security Team, *DDoS Protection Strategies for E-Commerce Businesses*, Shopify (2022), https://www.shopify.com/in/blog/ecommerce-security.

[2651] Fin. Action Task Force, Annual Report *2021-2022 (2022)*, https://www.fatf-gafi.org/en/publications/Fatfgeneral/Annual-Report-2021-2022.html.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

technologically advanced. It also has to be noted that IoT devices do not have robust security. Therefore, they are vulnerable and get exploited by unauthorised access.[2652]

Secondly, the cybercriminals employ advanced, sophisticated methods, such as Multi-Vector Attacks. They use Ransomware-as-a-service and exploit kits, which allow even non-technical actors to do complex cyber-attacks. Modern defence mechanisms, regular monitoring and standard security protocols are to be adhered to by platforms.

Thirdly, Evolving Regulations also shape cybersecurity obligations for e-commerce businesses. There is a need for Strict data protection, breach notifications, and consumer privacy protection mechanisms by the platforms. A substantial investment is to be made in cybersecurity infrastructure development and combat techniques. It is essential for compliance and to avoid penalties.[2653]

III. INDIAN LEGAL FRAMEWORKS THAT GOVERN CYBERSECURITY

A. Information Technology-related Acts

(i) Information Technology Act of 2000 and 2008

India's Cyber law regime is primarily regulated by the Information Technology Act 2000 and its subsequent amendments. It provides legal recognition across electronic transactions, signatures and records and prescribes reasonable cybersecurity practices. It empowers authorities to investigate, impose penalties, and prosecute cybercrimes.[2654]. The Act was enacted and enforced following the ratification of the "UNCITRAL Model Law on Electronic Commerce (1996)".[2655]

Relevant sections in the IT Act that promote cybersecurity are – Section 43 imposes a penalty and compensation for causing damage to a computer or a computer system. Section 66 prescribes a penalty of up to 5 lakhs and imprisonment for 3 years for an offence committed under section 43. Section 66 B–E consists of offences for hacking, stealing, cheating using a computer system, cyber terrorism and others. Section 66C states the punishment for fraudulent use of electronic signatures. Section 66E imposes a penalty for violation of privacy by capturing, publishing or transmitting private images without consent. Section 72 provides punishment for disclosure of confidential information without consent (Penalty for 3 years and a fine of 5 lakhs)[2656]

Information Technology (Amendment) Act, 2008 was put into effect from October 27th 2009, to address shortcomings of the 2000 Act. It included offences like emerging offences like phishing, identity theft and cyberstalking under the purview of the act. The definition of intermediaries was expanded, and new sections were introduced, which are as follows -

Section 43 A gives damages to the aggrieved person when the entity fails to take adequate security practices, leading to wrongful loss or compromise of sensitive information. Negligence is also considered a ground for this section. In case of Data breaches, it will be scrutinised as to whether e-commerce entities have taken reasonable security measures to prevent risks and protect consumers. It is a crucial aspect for determining their liability.

Section 69 of this act empowers the government to monitor, decrypt, block or erase data. Mandatory reporting of cybersecurity incidents by the affected intermediaries/corporations to CERT-In is included. Moreover, provisions for data storage, audits and cyber forensics are also added. The Imprisonment for cybercrimes and their related

[2652] F. Deligianni & S. Robbins, *Building a Robust Cyber Defence Strategy: Integrating AI-Driven Threat Mitigation and Blockchain Security in E-Commerce* (2024), https://doi.org/10.13140/RG.2.2.21587.80168.
[2653] R. Gupta, *Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies*, 1 J. ADVANCED MGMT. STUDS. 1 (2024).
[2654] Amit Kumar Kashyap & Mahima Chaudhary, *Cyber Security Laws and Safety in E-Commerce in India*, 2 Punjab B.J.L. & Safety 207 (2023).
[2655] G. Nikita Reddy, *A Study of Cybersecurity Challenges and Its Emerging Trends on Latest Technologies*, ResearchGate, https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies (last visited Oct. 6, 2025).
[2656] The Information Technology Act, 2000, §§ 43A, 66E, No. 21, Acts of Parliament, 2000 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

provisions is extended up to 10 years, along with deterrent penalties. [2657]

(ii) Rules and Guidelines in relation to Information Technology[2658]

(a) SPDI Rules, 2011:

It applies to "telecommunications, banking, financial institutions, and insurance". It applies to corporate entities handling sensitive personal data [2659] and identifies ISO/IEC 27001 norms as recognised international standards. Enterprises are strongly encouraged (but not legally required) to adopt them to comply with "reasonable security practices." These rules provide individuals the right to update personal information and impose restrictions on disclosure, transfer, and security measures.

(b) Electronic Service Delivery Rules, 2011: It enables government-designated services to be delivered electronically.

(c) IT Rules of 2013: It established the necessity of due diligence for intermediaries to claim safe harbour immunity under Section 79. Provisions for grievance redressal and incident reporting to CERT-In were brought. IT Rules, 2018, provide for a strict timeline of 72 Hours to remove prohibited content, deployment of technology-based automated tools, originator traceability and establishment of a grievance appellate committee.

(d) IT Guidelines, 2021 (Intermediaries and Digital Media Ethics Code): It replaced the IT rules of 2011. It contains provisions for a differentiation technique between large and small social media intermediaries based on user numbers, compliance requirements, mandatory terms of service, along with privacy policy, online gaming regulation and the need for transparency.

While the IT acts as a foundation, its cybersecurity provisions are outdated and largely reactive. It can be noted from sections 66, 66A-F,67 and 72 that it punishes cybercrime after its occurrence. Deterrence is prioritised over prevention. Section 43A has vaguely stated reasonable security practices, which allow for inconsistent interpretation. Section 69 is criticised as it raises serious concerns about government surveillance.[2660] Technological Neutral drafting increases uncertainty to address modern threats like AI-driven attacks, cross-border data trafficking, deepfakes and cryptocurrency. There is an absence of comprehensive data protection or privacy-related provisions in the act (Presently – DPDP ACT 2023). Other challenges are jurisdictional ambiguity, operational issues, the slow administrative nature of authorities, and the need for training personnel, infrastructure and skilled experts.

The SDPI rules also lack a proactive audit and a proper mechanism for certification. It excludes government entities, emerging data rights and grievance redressal mechanisms. These shortcomings have to be addressed swiftly.

(iii) Cybersecurity Institutions and Frameworks

(a) CERT-In (Computer Emergency Response Team – India)

It is the National nodal agency to report, respond, and mitigate cyber incidents. It also handles emergencies, awareness of cybercrimes and threat intelligence. [2661]

(b) CERT-In Directions, 2022

It is mandatory to report the cybersecurity incidents (data breaches, ransomware, phishing) within six hours. It requires the platforms to coordinate system clocks with NTP servers, maintain the logs for 180 days, and

[2657] The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

[2658] Avinash Patil, *Navigating the Digital Landscape: India's Evolving Legal Framework for E-commerce, Data Protection, and Cybersecurity* (May 29, 2024) (unpublished manuscript), https://dx.doi.org/10.2139/ssrn.4850285.

[2659] J.K. Malik & S. Choudhury, *Privacy and Surveillance: The Law Relating to Cyber Crimes in India*, 9 J. ENG'G COMPUTING & ARCHITECTURE 74 (2019).

[2660] Srinivasa Rao Dokku & Deenamma Kandula, *A Study on Issues and Challenges of Information Technology Act 2000 in India*, 1 ANNALS JUST. & HUMAN. 39 (2021).

[2661] Sanjeev Kumar, *Cyber Crimes in India: Trends and Prevention* (May 2021), https://www.researchgate.net/publication/351902133_CYBER_CRIMES_IN_INDIA_TRENDS_AND_PREVENTION (last visited Feb. 25, 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

retain known customers in certain services. Accountability and Compliance mechanisms are imposed on e-commerce entities for response and mitigation.[2662]

(c) Indian Cyber Crime Coordination Centre (I4C)

This Centre coordinates national-level responses to cybercrime and facilitates the exchange of intelligence amongst law enforcement agencies. Awareness and security mechanisms of Cybercrimes are promoted.

There is no single centralised authority to oversee the aspects of cybersecurity. Instead, the institutional functions overlap, leading to complexity and incoordination.

(d) Critical Information Infrastructure Protection (CIIP)

It is Managed by the "National Critical Information Infrastructure Protection Centre (NCIIPC)". The aim is to vital digital assets like banking, transport, etc and collaborate with regulators, industries, etc. This centre faces an acute shortage of trained professionals, funding irregular audits, and weak security maintenance, giving rise to vulnerabilities.

(e) National Cybersecurity Policies

National Cyber Security Policy, 2013, is a Comprehensive policy framework that applies to the government and private sector. The main aims are the protection of the cyber infrastructure, training professionals skilled in cybersecurity, preventing cyber incidents and developing mitigation mechanisms. However, it did not fully anticipate the rapid growth of technologies.

National Cyber Security Strategy, 2020 aims to enhance Cybersecurity resilience against cybercrimes and promote prevention mechanisms and audits. It has remained as a Draft and not been formally adopted. It lacks legal enforceability and specific time frames to achieve its goals.

B. Consumer Protection in Indian E-Commerce

The digital global revolution increased the number of online transactions, leading to new issues and concerns about consumer protection. The Indian Government has enacted legislation to safeguard the consumers. [2663]

(i) The Consumer Protection Act 1986 and 2019 Amendment

The Consumer Protection Act of 1986 forms the base for consumer protection and provides for establishing consumer forums and authorities to settle consumer disputes in a speedy, inexpensive manner. It had provisions for unfair trade practices, defective goods and consumer deficiency of consumers. Some Major rights of consumers include the right to safety, information, choice, grievance redressal, education, and the right to be heard. [2664]

Consumer Protection Act 2019 contains provisions which offer protection from fraudulent business practices, product liability, unfair contracts and misleading advertisements. It extended consumer protection to digital transactions and e-commerce services. Provisions like ADR, a central consumer protection authority, were created along with increasing the pecuniary jurisdiction of consumer forums.

(ii) Consumer Protection (E-Commerce) Rules, 2020

It was implemented on 23rd July 2020. It has been carefully designed to mitigate unfair trade practices and to safeguard the interests of consumers. The scope of the rules covers all goods and services under electronic mechanisms and all e-commerce enterprises under the inventory or marketplace model (Rule 3(1)(f) and Rule 3(1)(g)). It also covers e-commerce entities that offer goods and

[2662] V. Agarwal, *Privacy and Data Protection Laws in India,* 5 INT'L J. LIABILITY & SCI. ENQUIRY 205 (2012).

[2663] Ujwal Sharma & Gargi Bhadoria, *Legal Challenges and Regulations for E-Commerce Companies*, 7 INT'L J. L. MGMT. & HUMAN. 1314 (2024).

[2664] H.A. Aljifri et al., *Global E-Commerce: A Framework for Understanding and Overcoming the Trust Barrier,* 11 INFO. MGMT. & COMPUT. SEC. 130 (2003).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

services to Indian consumers, even if not physically present in India. [2665]

Responsibilities under the 2020 rules are: E-commerce entities must be registered and appoint a designated contact person (Rule 4). It also mandates the marketplace entities (sellers) to furnish accurate information about the listed products and information which is accurate regarding the characteristics. (Rule 5) They must also refrain from engaging in unfair trade practices and not refuse refund/return of goods which are defective or counterfeit. It must have a pre-existing written agreement with the entity before listing of products (Rule 6). Inventory-based entities have the same liability as marketplace entities. Some essential requirements are compulsory disclosure, data privacy and protection, clear refund and return policies and efficient grievance redressal, which is user-friendly in nature. [2666]

(iii) Challenges in consumer protection

The enforcement of the act and supervision by the authorities are inadequate. IPR issues, which involve the sale of spurious, counterfeit goods, are increasing. The 2020 rules prohibit refusing the return of these products. Another issue revolves around liability due to misleading descriptions of the products, which evolved into manipulative designs, known as dark patterns. (Hidden costs, subscription traps). In 2023, Guidelines for the prevention and enforcement of dark patterns were issued.

The influx of foreign e-commerce platforms further raises concerns about their compliance with Indian legislation, making it a jurisdictional issue. The central Consumer Protection Authority's scope cannot keep up with the number of digital transactions that occur, which may lead to a huge number of cases and backlogs. Further, there are Inconsistent provisions of product liability, uneven implementation of the act, regulatory overlaps and a lack of ADR Mechanisms.[2667]

In Consumer protection, efforts are consistently made to address new issues. Still, a few improvements in unnoticed concerns can strengthen consumer governance in the long run from cybersecurity threats.

C. The Digital Personal Data Protection Act, 2023 (DPDP)

The President signed the "Digital Personal Data Protection Act" on 11th August 2023. This act was signed, aiming at establishing India's dedicated legal framework for processing digital personal data. The Act recognises individuals' rights to safeguard personal information while allowing legitimate organisational processing. [2668]

It applies to the processing of digital personal data within India when data is collected online or collected offline and then digitised. This also applies to the processing of personal data outside India if it relates to offering goods or services within India. Any data about an individual who is identifiable by or in relation to such data. Processing includes collection, storage, use, and sharing wholly or partly automated operations on digital personal data.

Personal data may be processed by data fiduciaries for lawful purposes after obtaining consent from the concerned person to whom the data belongs. (section 6) A notice must be provided before seeking consent, detailing the data collected and the purpose. (Section 5) The person can withdraw consent at any time.

Exceptions for certain legitimate uses are allowed, including specified purposes voluntarily provided by the individual, provision of government benefits or services, medical emergency, and employment. For individuals below 18, consent must be provided by a parent or legal guardian.

[2665] Debika Mukherjee, *A Study of E-Commerce and Cyber Crime: Chances, Challenges and Prevention*, 6 INT'L J. MULTIDISCIPLINARY RSCH. 1 (2024).
[2666] PwC, Global Consumer Insights Survey 2020 (2020), https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey.html.
[2667] Kasina Naga Suryanarayana, *Consumer Protection in India: Laws, Challenges, and Effectiveness*, 5 INT'L J. RSCH. HUM. RES. MGMT. 94 (2023).
[2668] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Data access/ transfers are allowed across borders (outside India), except to countries restricted by a central government notification. The central government will establish the Data Protection Board of India to oversee compliance and grievances. Data localisation provision and storage issues pose a potential technological challenge for our nation.

The rights and duties of data principals are: The data principal has full rights to obtain information about processing, seek corrections and erasure of personal data if needed. He/she can also nominate another person to exercise rights on death/incapacity, and also access grievance redressal. Data principals must not register false or unmeritorious complaints. He/she is not entitled to furnish false particulars or impersonate another person. If any of the above rights are violated, they will be penalised up to ₹10,000.

Penalties [2669] apply under the following conditions:

Failure to prevent personal data breach (sec.5(8)): Up to INR 250 crore.

Failure to notify the Board and data principals (sec.5(6)): Up to INR 200 crore.

Non-fulfilment of obligations while processing children's data (sec.9): Up to INR 200 crore.

Non-fulfilment of obligations by a significant data fiduciary (sec.10): Up to INR 150 crore.

Breach of any voluntary undertaking given to the Board (sec.32): Penalty up to the extent applicable for the breach.

Miscellaneous non-compliance: Up to INR 50 crore.[2670]

Certain problems which are yet to be addressed in this act are: organisational challenges, high costs to entities, lack of independence of the data protection board, non-exclusion of individual rights such as data portability, vague provisions lacking specificity, excessive government exceptions and non-implementation till now. [2671] Some reforms may include adopting transparent data practices, Regular Data Protection Impact assessments, internal training and appointment of experts.

It is envisioned as an overhaul of the IT Act to tackle advanced challenges like deepfake technology, AI misuse, blockchain issues and emerging cyber frauds. Strong obligations are to be put on E-Commerce platforms with regard to cybersecurity standards, proper privacy policies, security controls and platform accountability. It aims to establish risk-based cybersecurity standards by focusing on the security and integrity of security systems.

D. Preventive Mechanisms

Compliance with the legal frameworks, along with prevention measures with respect to an e-commerce platform, must be fulfilled to reduce its vulnerability to risks.[2672]

(i) Data Security Controls

Platforms must implement encryption, authentication techniques, multi-factor controls, access controls, and digital signatures in order to protect the personal and sensitive information of the customers, like Name, Email and payment information. Precautionary steps such as Regular updates, firewall security, patching up, anti-virus software, and intrusion Detection systems must be undertaken to limit their vulnerability from cybercrimes.

(ii) Incident Response Plan and Breach Notification

It states the requirement to follow procedural protocols like detection, investigation, containment, and recovery. Prompt Incident Reporting is mandated by CERT In. Notification must be given immediately to the regulators

[2669] Torsha Sarkar, *The Legal Challenges to India's Proposed Surveillance Regime*, CTR. FOR INTERNET & SOC'Y (2019), https://cis-india.org/internet-governance/blog/india-digital-freedoms-4-platform-governance

[2670] S. Kethineni, *Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms*, in THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE 305 (T.J. Holt & A.M. Bossler eds., 2020).

[2671] Yatin Pandit, *Compliance Challenges before Indian Businesses under the Digital Personal Data Protection Act, 2023*, 11 INT'L J. RSCH. & ANALYTICAL REVS. 15 (2024).

[2672] KnowBe4, Security Awareness Training (2021), https://www.knowbe4.com/security-awareness-training/ (last visited Feb. 25, 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

and the affected customers, which is also given under the DPDP Act. An incident response team must be formed, who must be trained with Mock drills and forensic preparedness.[2673]

(iii) Logging, Monitoring, and Audit

Platforms must maintain system logs for 180 days as mandated by CERT In. Continuous monitoring must be done to detect anomalies, unusual spikes in the traffic and payment activity. This helps to prevent fraud and identify attacks like DDoS in an early stage. E e-commerce platform must also equip itself with security protocols, penetration testing and vulnerability assessments.[2674]

(iv) Organisational Measures

Employees must be trained and made aware of phishing, the prevention of insider threats, and proper data handling. Sites must hire compliance officers (as per IT Act/Intermediary Rules) and Data Protection Officers (as per DPDP Act) in necessary conditions. There must be oversight of the proper Implementation of role-based access controls, backup policies, and disaster recovery plans.[2675]

(v) Transparency with Consumer Awareness

Transparency is an important principle in e-commerce rules and the DPDP Act. Sites should show their privacy notices, get specific, express consent, and address the grievances of the person from whom data was collected. Education initiatives must be taken, where consumers are informed about phishing links and bogus deals. It also works as a deterrent mechanism against social engineering attacks.

(vi) Vendor and Supply Chain Security

Since platforms are dependent upon 3rd party vendors, logisticians, and payment processing services, protection of contracts and auditing are required. Verification and adherence to security conventions mitigate indirect breaches.[2676]

IV. DETERMINING LIABILITY AND ACCOUNTABILITY OF PLATFORMS

A. Safe Harbour Immunity of Platforms

Sec 79 of the IT Act, 2000 grants Conditional immunity to intermediaries from third-party data, communication or information which is hosted, transmitted or made available on their platform. Intermediaries cannot monitor every user-generated content, which makes their liability conditional.[2677]

Conditions to avail protection - The intermediaries must act as a facilitator and not initiate the transmission. They must not have actual knowledge of the content and must not be an active participant. On the date of attaining knowledge of the illegal content, they must remove it within an appropriate time and on notice received.

They must follow due diligence and publish their privacy policies. There must be a grievance redressal officer on board to address the complaints. They must display their seller details to ensure transparency and protect customer interests. In case of any conspiracy proven, the protection is lost.

E-Commerce platforms' Role as intermediaries – Platforms like Flipkart, Amazon and Myntra are intermediaries as per section 79. If they are actively involved, which includes controlling price, warehouse, logistics, and ads, then they may be held liable along with the seller. The more a platform moves from a neutral intermediary to an active participant, the weaker its protection becomes.

Consumers can approach consumer forums for compensation (e.g., hacked accounts, fake products). It is also pertinent to note that the active nature of an E-commerce platform in

[2673] SANS Inst., Incident Response: How to Plan and Prepare for the Worst (2021), https://www.sans.org/security-resources/glossary-of-terms/incident-response.
[2674] Ritik Raj, *Cybersecurity Issues and Challenges in E-Commerce*, 7 Int'l J. L. Mgmt. & Human. 1234 (2024).
[2675] Shopify, How Ecommerce Infrastructure Allows Your Online Store to Function (2021), https://www.shopify.com/in/blog/ecommerce-infrastructure.
[2676] Jennifer ThankGod, *Cybersecurity in the Age of E-Commerce: Defending Digital Trade Platforms from Emerging Threats* (SSRN Working Paper No. 4858731, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4858731.
[2677] Information Technology Act, No. 21 of 2000, § 79, India Code (2000).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

transactions like promotion, warehouse handling, and pricing control, the more diminished is the protection under section 79. This will lead to scrutiny under specific liability provisions.

For Instance, if the occurrence of the breach is caused due to a failure to adopt reasonable security practices, then the section 79 application will be barred. Nowadays, Courts are interpreting this section narrowly, having the necessity of strict due diligence to protect consumer interests.

B. Judicial Precedents

(i) Active/ Passive Role of Platforms

(a) Shreya Singhal v. Union of India (AIR 2015 SC 1523)

This case challenged 66A of the IT Act, which was finally struck down. The decision reinforced the limits of the state to restrict online speech and gave clarity that all intermediaries are subject to safe harbour protection. However, they must comply with due diligence and take the content down on judicial notice. It established intermediary compliance and their role as passive or active players in the e-commerce market for claiming immunity.[2678]

(b) Flipkart Internet Private Limited v. State of NCT of Delhi & Anr.

Flipkart petitioned against the allegation of unauthorised sellers listing trademarked goods on their platform. The intermediary's duty to remove the content and validity of filing an FIR against Flipkart is assessed. The court held that the intermediary is liable to remove the content based on a judicial order, which is mandatory, and it is not a criminal offence where there is no judicial order received for the e-commerce platforms to adhere to. This case affirms the importance of judicial orders and notices for content removal and narrows down the criminal liability of intermediaries for third-party listings.

(c) Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. & Ors.

There is a dispute between Amway (a direct selling company) and Amazon/ online platforms regarding the sale of direct selling products and alleged contravention of the dispute selling guidelines. The issue in this case is the role of e-commerce platforms as passive or active members and the enforceability of the direct selling Guidelines. "The judgment did not treat the Direct Selling Guidelines as binding law under Article 13 due to questions over their legislative status, but it highlighted that platforms that provide value-added services and facilitate transactions may lose Section 79 protection if they don't comply with due diligence"

(d) Luxottica Group S.P.A. & Another v. M/s Mify Solutions Pvt. Ltd. & Ors.

It was an alleged sale of infringing goods where the seller's identity wasn't disclosed on the platform. It was held that the defendants are not intermediaries and therefore section 79 is not applicable. This case highlights practical due diligence requirements and how their failure leads to liability.[2679]

(e) Skullcandy Inc. v. Shri Shyam Telecom & Ors.

This site was alleged to sell counterfeit items on the platform, and they failed to take it down despite notices. It was held that due to a lack of due diligence and an active role played by the site in protecting replica products, the platform did not get protection under Section 79. The court ordered remedial steps like certification of the platform, assurances to be given by the seller and removal of replicas by the site.[2680]

(f) Amazon India v. State of Maharashtra

This site failed to deliver and refund on time, and therefore, the role of intermediary in payment processing is being assessed in this case. It was held that the respondent relied on the platform role to process payments and give

[2678] Ujwal Sharma & Gargi Bhadoria, *Legal Challenges and Regulations for E-Commerce Companies*, 7 INT'L J. L. MGMT. & HUMAN. 1314 (2024).

[2679] 2018 SCC OnLine Del 3208 (India).

[2680] 2018 AIR Online Del 1987 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

refunds. Therefore, the consumer redress needs to be properly maintained to avail immunity.[2681]

(ii) Trademark / IP infringement on marketplaces

(a)Tiffany (NJ) Inc. v. eBay, Inc. (US – persuasive)[2682]

It was held in this case that eBay was not directly liable for the sellers ' trademark-infringing conduct but was asked to increase its safeguards to prevent such offences from happening in the future.

(b) Himalaya Wellness Co. v. Wipro Enterprises Pvtputta Ltd.

It was held in this case that marketplaces must be careful with listing the products and claims of the sellers, as trading off practice is being undertaken, which will confuse the consumer as to the goodwill of the brand.

(c) Chandigarh Consumer Disputes Redressal Forum — Amazon account hacking (2025)

In this case, the complainant's account was hacked, leading to 40k worth of fraudulent orders placed. It was held that Amazon should provide a refund and compensation to the consumer as they were negligent in the protection of the consumer's account. Section 43A of the IT Act for negligence to uphold reasonable security practices, and the E-Commerce Rules 2020 apply in this case.

(d) BigBasket data breach (2020)[2683]

The personal data of 2 crore customers was leaked on the dark web. Section 72A was applied. No direct penalties till now. It highlights the need for the implementation of data protection legislative frameworks. Penalty under this section under the act is extended to 3 years and a fine of up to 5 lakhs.

(e) MobiKwik alleged data leak (2021)

Know your customer details of 10 crore users were allegedly leaked. No public penalties imposed till now. An investigation was done by CERT-IN.[2684]

(f) BoAt Lifestyle data leak (2024) — FreshMenu (2024) — Angel One (2024)

User records were leaked in each case. There was a delayed notification to the regulators (CERT IN reporting rules within 6 hours). Current status is ongoing investigation with limited action undertaken.

The judicial trend across these precedents establishes that e-commerce platforms face legal vulnerabilities mainly due to the erosion of conditional immunity under section 79 and the lack of reasonable security practices under section 43A of the IT ACT 2000, which is currently replaced under the DPDP ACT 2023 for data breach prevention practices. The penalty stated is 250 Crore. The court imposes obligations like strict due diligence of platforms and proper mitigation strategies.

The growth in e-commerce led to a major advancement in trade and consumer behaviour, by way of easy transactions and global connections. Despite the progress made by the legal framework, there are still major shortcomings in cybersecurity protection.

V. GAPS AND REFORMS NEEDED IN CYBERSECURITY FRAMEWORK

A. Gaps in India's Cybersecurity Legal Framework

(i) Outdated and Rigid Structure of Laws

The IT Act 2000 forms the legal foundation for electronic transactions, signatures and contracts. It contains provisions addressing cybercrimes and provides penalties for them. However, it lacks the necessary provisions to tackle AI misuse, Blockchain vulnerabilities, quantum computing threats, and deepfake

[2681] 2021 SCC OnLine Bom 404 (India).
[2682] Mayank Raj, *E-Commerce Era: Legal Complexities and Digital Evolution for Companies*, 4 INDIAN J. L. REV. 1326 (2024).
[2683] Rahul De' et al., Lessons from BigBasket Security Breach (Indian Inst. of Mgmt. Bangalore 2020), https://www.iimb.ac.in/sites/default/files/2020-11/Lessons_BigBasket_security_breach.pdf (last visited Feb. 25, 2026).
[2684] Tech Desk, MobiKwik Database of 10 Crore Users Leaked on Dark Web; Company Denies Data Breach, Indian Express (Apr. 1, 2021), https://indianexpress.com/article/technology/tech-news-technology/mobikwik-database-leaked-on-dark-web-company-denies-any-data-breach-7251448/.

technology. This absence of adaptation of laws to present technological problems creates a limited scope for regulatory flexibility, which makes real-time incident response to cybersecurity incidents in e-commerce weak.[2685]

(ii) Weak enforcement and institutional fragmentation

There is an overlap of jurisdiction amongst institutional regulatory authorities like the "Ministry of Electronics and Information Technology, Cert-In, State-level cyber cells, and the RBI". This leads to effort duplication, inconsistency, and improper coordination. There is no single nodal authority for the implementation and compliance with cybersecurity. This fragmentation slows down swift responses to large-scale cyber incidents.

(iii) Limited scope of the Data Protection Regime and Incident Response

The DPDP Act of 2023, which was enacted to safeguard individuals' private data, contains a limited scope for enforcement. It is still not yet implemented. There is a lack of provisions for cross-border data protection and deterrent penalties. Broad exemptions are also made to government entities.

Furthermore, our Nation lacks a comprehensive framework that checks the compliance with the timely reporting of cybersecurity incidents. Many organisations delay/ fail to submit timely reports of data breach incidents, resulting in delayed and inadequate responses and assessments of the threat. Although CERT IN directions provide for 6-hour mandatory reporting, compliance still lacks. There are no strict penalties given in the legislation. It is vital for early detection, information sharing, combating, mitigating crimes, and protecting the end users.

(iv) Inadequate consumer awareness and Digital literacy:

Many users are not aware of threats due to cybercrimes, making them victim of it. When the users don't have knowledge of their rights stated under the act, they won't initiate grievance redressal. Therefore, it must be a priority to undertake Awareness campaigns and educational initiatives. [2686]

(v) Weak cross-border data governance and international Cooperation

There is a necessity to enter into bilateral and multilateral data sharing agreements, data localisation policies, and provide clarity on jurisdictional liability to protect Indian citizens' digital identity. India has failed to ratify major cybersecurity frameworks, such as the Budapest Convention on Cybercrime, and also doesn't have standardised mutual legal assistance treaties (MLAT). It hinders foreign agencies' coordination and increases the difficulty of extraditing cybercriminals. [2687]

(vi) Lack of consent clauses, accountability mechanisms and surveillance concerns

Often, E-commerce platforms use a blanket consent clause that gives consumers limited control over their personal data. It undermines their need for informed, transparent, and specific consent for entities to process, share, and not misuse it. Purpose limitations and easy opt-out provisions are to be provided to customers. [2688]

There is also a lack of clear accountability mechanisms in case of a breach. There must be encryption protocols, anonymisation and regular audits by e-commerce companies to prevent breaches. Consumer notification in case of any harm to their data must be mandated. The government employs facial recognition technologies that end up collecting

[2685] *Jennifer ThankGod, Cybersecurity in the Age of E-Commerce: Defending Digital Trade Platforms from Emerging Threats* (2025) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4858731.

[2686] Shwetang Rajendra Danekar & Ajit Kamble, *Online Privacy and Cybersecurity: Regulations and Challenges,* 7 INT'L J. L. MGMT. & HUMAN. 1827 (2024).

[2687] Sukrit Garg et al., *Cyber Security's Influence on Digital Consumer Trust*, *12 INT'L J. CREATIVE RSCH. THOUGHTS* 155 (2024).

[2688] Shweta et al., *Cyber Threats and Its Impact on E-Commerce Sites*, *10 INT'L J. CONTROL THEORY & APPLICATIONS* 15 (2017).

massive amounts of data. This raises concerns of intercepting communications and the right to privacy.

B. Reforms and Policy Recommendations

(i) Changes to Cybersecurity legislation: The cybersecurity framework must change to address modern technological advancements. This makes the provisions more flexible and adaptable. It must establish a National Cybersecurity Policy Council, conduct regular audits, and include sunset clauses within relevant laws. The creation of the National Cybersecurity Authority to coordinate cyber threat management, enforce compliance and train personnel is mandated. It must integrate the functions of current institutions to combat cybercrime. The National Cyber Coordination Centre must also act as a central hub for intelligence sharing, cyber drills, assessments, and give forensic support to the state.

(ii) Implementation of the DPDP Act: The DPDP Act must be implemented along with the support of the Independent Data Protection Authority, which is empowered to impose strict penalties and conduct inspections.

(iii) Mandatory Cyber incident reporting: It must be done for all e-commerce entities and creation of a secure, confidential reporting portal which allows the entities to come forward and report without reputational loss. There must be real-time information exchange and defence mechanisms in place at all times. Non-compliance with provisions must attract penalties.

(iv) Participation in international forums: India's participation in global cybercrime conventions, institutions and initiatives to be enhanced. Pacts must be formed to ensure global coordination. There must be standardisation of provisions, clear accountability and jurisdictional liability policies.[2689]

(v) Actions by Government: The Government must offer tax incentives, grants and awards to entities that develop and innovate security technologies, strategies and mitigation techniques. This includes Research and Development in Encryption methods, intrusion Detection systems, secure payments and biometric protection systems. Encouragement must also be offered to public-private partnerships. [2690]

(vi) Awareness Enhancement: National awareness campaigns and educational initiatives must be conducted to promote safe cybersecurity practices by consumers, reporting and grievance redressal mechanisms, secure payments, password non-sharing and phishing prevention techniques. [2691] Capacity building and training must be provided to e-commerce companies and their stakeholders to strengthen their internal defence and prevention techniques against cybercrime. [2692]

(vii) Prevention by e-commerce entities: The e-commerce entities must adopt safe encryption practices and a Privacy design framework embedding security in every stage of product development.[2693] They must have secure firewalls, multifactor authentication, and other security protocols up to standard. They must frequently update, change passwords when needed, hire cloud services, have the best threat detection software installed and regularly monitor the site. [2694] Furthermore, Regular audits must be conducted, along with obtaining compliance certificates. Consumer redressal mechanisms should be made effective to address the data breaches and misuse. Remedies must be given to them.

The above reforms must be implemented to transition our nation into a trustworthy and

[2689] D. Martinez, *Regulatory Challenges in Cross-Border E-Commerce Transactions, 35 EUR. L.J.* 134 (2020).

[2690] Kritika Parekh et al., *The Role of Legalisation in Combating Evolving Cybersecurity Challenges*, *7 INT'L J. L. MGMT. & HUMAN.* 2046 (2024).

[2691] Nat'l Cyber Sec. Ctr., Cybersecurity Awareness Guide for Consumers (2022), https://www.ncsc.gov.uk/section/advice-guidance/you-your-family.

[2692] Arun S. et al., *Cybersecurity Challenges in E-Commerce: Implications for Consumer Confidence, 5 INT'L J. PROGRESSIVE RSCH. ENG'G & MGMT. SCI.* 685 (2025).

[2693] Dash, An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy (2022), https://www.researchgate.net/publication/359772764_An_Effective_Cybersecurity_Awareness_Training_Model_First_se_of_an_Organizational_Security_Strategy.

[2694] Y. Chen & Z. Wang, *The Role of Digital Marketplace Regulations in Preventing Fraudulent Practices*, *29 CHINA BUS. REV.* 98 (2020).

future-ready digital economy. The confidence and trust of investors, global trade partnerships formed, and the overall credibility of cybersecurity governance will increase.

VI. CONCLUSION

The above research aims to identify cybersecurity threats that affect India's e-commerce sector. It can be found that the risks are increasing at a rapid rate. Types of cybercrime, such as Phishing, data breaches, identity theft, ransomware and payment fraud, became prevalent. It is being facilitated due to IOT Vulnerabilities and an increase in the value of e-commerce Transactions. They cause excessive financial loss and lead to a decrease in trust of the customer in the credible nature of the platform. Cybersecurity standards are a must to adhere to for the sustainability of the intermediary.

After thorough examination of the legal framework, the study found that the IT Act, 2000, the Consumer Protection Act, 2019 and its E-Commerce Rules, the DPDP Act, 2023, along with CERT-In guidelines form the base for cybersecurity. This legislation also states the obligations, like data security, mandatory reporting of breaches and grievance redressal, to be adhered. They also offer limited safe harbour protections to the e-commerce platforms.

The Analysis of Landmark Judicial precedents and statutory process reveals that the enforcement and implementation are not adequate, and there is a lack of strict penalties. there is a presence of jurisdictional overlap, lenient compliance and cross-border protection. The legal liability and accountability of these e-commerce platforms are ambiguous due to the Section 79 Active/ Passive intermediary Test. It shows significant gaps like uneven regulation, improper sector-specific safeguards, poor customer redressal and inadequate global coordination.

Therefore, it is necessary for reforms to be implemented to meet the increasing intricacies. It includes strengthening the liability framework, improving implementation and coordination and the consumer redressal mechanism. A strong legal framework reverses the growth of cyber threats and offers protection and trust to the customers. For Instance, the DPDP Act of 2023 brings huge financial deterrence, making the compliance stricter.

By resolving these gaps and transitioning from reactive to proactive risk-based governance, our nation will grow into a more secure and accountable digital environment. This will ensure the twin objective of safeguarding customers and the long-term resilience of the e-commerce sector, which fosters long-term trust and growth of India's economy.

VII. REFERENCES

A. Cases

1. *Google India Pvt. Ltd. v. Visaka Industries*, (2020) 4 S.C.C. 410 (India).
2. *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).
3. 2018 SCC OnLine Del 3208 (India).
4. 2018 AIR Online Del 1987 (India).
5. 2021 SCC OnLine Bom 404 (India).

B. Statutes

1. The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
2. The Digital Personal Data Protection Act, No. 40 of 2023, Acts of Parliament (India).
3. Information Technology Act, No. 21 of 2000, India Code (2000).
4. Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament (India).

C. Books & Book Chapters

1. D. Halder & K. Jaishankar, Cyber Governance and Data Protection in India: A Critical Legal Analysis, in *The Routledge Companion to Global Cyber-Security Strategy* 337 (Scott N. Romaniuk & Francis Grice eds., 2021).

2. S. Kethineni, Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms, in *The Palgrave Handbook of International Cybercrime and Cyberdeviance* 305 (T.J. Holt & A.M. Bossler eds., 2020).

D. Journal Articles

1. V. Agarwal, Privacy and Data Protection Laws in India, 5 Int'l J. Liability & Sci. Enquiry 205 (2012).

2. H.A. Aljifri et al., Global E-Commerce: A Framework for Understanding and Overcoming the Trust Barrier, 11 Info. Mgmt. & Comput. Sec. 130 (2003).

3. Arun S. et al., Cybersecurity Challenges in E-Commerce: Implications for Consumer Confidence, 5 Int'l J. Progressive Rsch. Eng'g & Mgmt. Sci. 685 (2025).

4. H. Desamsetti, Crime and Cybersecurity as Advanced Persistent Threat: A Constant E-Commerce Challenge, 8 Am. J. Trade & Pol'y 239 (2021).

5. Srinivasa Rao Dokku & Deenamma Kandula, A Study on Issues and Challenges of Information Technology Act 2000 in India, 1 Annals Just. & Human. 39 (2021).

6. S. Dwivedi, From Privacy to Data Protection in India: Evaluating the Personal Data Protection Bill, 2019, 3 Int'l J. L. Mgmt. & Human. 2136 (2020).

7. Shwetang Rajendra Danekar & Ajit Kamble, Online Privacy and Cybersecurity: Regulations and Challenges, 7 Int'l J. L. Mgmt. & Human. 1827 (2024).

8. Sukrit Garg et al., Cyber Security's Influence on Digital Consumer Trust, 12 Int'l J. Creative Rsch. Thoughts 155 (2024).

9. R. Gupta, Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies, 1 J. Advanced Mgmt. Studs. 1 (2024).

10. Amit Kumar Kashyap & Mahima Chaudhary, Cyber Security Laws and Safety in E-Commerce in India, 2 Punjab B.J.L. & Safety 207 (2023).

11. J.K. Malik & S. Choudhury, Privacy and Surveillance: The Law Relating to Cyber Crimes in India, 9 J. Eng'g Computing & Architecture 74 (2019).

12. D. Martinez, Regulatory Challenges in Cross-Border E-Commerce Transactions, 35 Eur. L.J. 134 (2020).

13. Debika Mukherjee, A Study of E-Commerce and Cyber Crime: Chances, Challenges and Prevention, 6 Int'l J. Multidisciplinary Rsch. 1 (2024).

14. George Caleb Oguta, Securing the Virtual Marketplace: Navigating the Landscape of Security and Privacy Challenges in E-Commerce, 18 GSC Advanced Rsch. & Reviews 84 (2024).

15. Yatin Pandit, Compliance Challenges before Indian Businesses under the Digital Personal Data Protection Act, 2023, 11 Int'l J. Rsch. & Analytical Revs. 15 (2024).

16. Kritika Parekh et al., The Role of Legalisation in Combating Evolving Cybersecurity Challenges, 7 Int'l J. L. Mgmt. & Human. 2046 (2024).

17. Mayank Raj, E-Commerce Era: Legal Complexities and Digital Evolution for Companies, 4 Indian J. L. Rev. 1326 (2024).

18. Ritik Raj, Cybersecurity Issues and Challenges in E-Commerce, 7 Int'l J. L. Mgmt. & Human. 1234 (2024).

19. Ujwal Sharma & Gargi Bhadoria, Legal Challenges and Regulations for E-Commerce Companies, 7 Int'l J. L. Mgmt. & Human. 1314 (2024).

20. Shweta et al., Cyber Threats and Its Impact on E-Commerce Sites, 10 Int'l J. Control Theory & Applications 15 (2017).

E. Reports & Institutional Publications

1. Fin. Action Task Force, Annual Report 2021–2022 (2022).

2. Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, FIPS PUB. 197, Advanced Encryption Standard (AES) (2001).

3. PwC, Global Consumer Insights Survey 2020 (2020).

Verizon, 2021 Data Breach Investigations Report (2021).

F. Online Sources & Working Papers

1. Avinash Patil, Navigating the Digital Landscape: India's Evolving Legal Framework for E-Commerce, Data Protection, and Cybersecurity (May 29, 2024) (unpublished manuscript).

2. Dash, An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy (2022).

3. Jennifer ThankGod, Cybersecurity in the Age of E-Commerce: Defending Digital Trade Platforms from Emerging Threats (SSRN Working Paper No. 4858731, 2023).

4. KnowBe4, Security Awareness Training (2021).

5. Nat'l Cyber Sec. Ctr., Cybersecurity Awareness Guide for Consumers (2022).

6. G. Nikita Reddy, A Study of Cybersecurity Challenges and Its Emerging Trends on Latest Technologies, ResearchGate.

7. SANS Inst., Incident Response: How to Plan and Prepare for the Worst (2021).

8. Shopify Security Team, DDoS Protection Strategies for E-Commerce Businesses (2022).

9. Tech Desk, MobiKwik Database of 10 Crore Users Leaked on Dark Web; Company Denies Data Breach, Indian Express (Apr. 1, 2021).

10. Torsha Sarkar, The Legal Challenges to India's Proposed Surveillance Regime, Ctr. for Internet & Soc'y (2019).