IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Legal Architecture of E-Commerce in India: IT Act, DPDP Act, and Judicial Interpretation

Vidyadhara vedhavarma T
Assistant Professor
R.L. Law college, Davangere

Dr. Rajendra Kumar Hittanagi
Assistant Professor
Karnataka State Law University, Hubballi

Abstract

The high rate of e-commerce growth in India has created the necessity of a broad legal framework to control online dealings, guard consumer rights as well as to hold online sites responsible. The paper reviews the changing regulatory framework of e-commerce in India; specifically, the Digital Personal Data Protection Act, 2023 (DPDP Act), the Information Technology Act, 2000 (IT Act), and the Information Technology (Intermediaries Guidelines) Rules, 2011. It examines the combined effect of these legislative tools in solving data privacy, intermediary liability, electronic contracts, consumer protection and platform responsibility.

The DPDP Act which came into effect after the constitutional right to privacy was identified in Justice K.S. Puttaswamy (Retd.). v. Union of India, implements an organized system of protection of digital personal information, where data fiduciaries and data principals are identified, along with the introduction of consent-based processing and severe consequences of failure to do so. The IT Act, 2000 gives a legal acknowledgement to the electronic records and digital signatures, authorizing a contract through the Internet, and permitting digital business. The Intermediary Guidelines Rules, 2011 read together with Section 79 of the IT Act, offer conditional safe harbor protection to the intermediaries on the condition of due diligence.

The paper also analyzes some of the major judicial precedents such as Shreya Singhal v. SAS, Christian Louboutin Union of India v. Nakul Bajaj, and Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd., which have provided the understanding of the intermediary immunity and the notion of real knowledge. The research arrives at a conclusion that the legal framework of India aims at achieving a balance between innovation, consumer protection, and constitutional freedoms and gradually enhancing responsibility in the digital marketplace.

Keywords *- E-Commerce; Intermediary Liability; Digital Personal Data Protection Act, 2023; Information Technology Act, 2000; Safe Harbor.*

1 Introduction

Due to the exponential development of digital commerce in India, the processes of the production, marketing, and consumption of goods and services have been changed. E-commerce platforms have now transformed into multi-faceted digital ecosystems that include data gathering, decision-making algorithms, cross-border buying and selling, and third party sellers. As this has grown, issues associated with consumer protection, data confidentiality, intermediary liability, infringement of intellectual property and cyber fraud have gained critical importance. The necessity to weigh between innovation and financial growth and accountability and user rights has thus become one of the key issues in the Indian digital regulation context.

Application of the right to privacy as a fundamental right by the Supreme Court in Justice K.S Puttaswamy (Retd.). v. Union of India was a constitutional milestone, and the trailblazer toward the all-inclusive data protection law. This led to the Digital Personal Data Protection Act, 2023 (DPDP Act) creating a framework on the regulation of digital personal data, consent, and data fiduciary duties and a system of enforcement via the Data Protection Board of India. At the same time, the Information Technology Act, 2000, including its amendments and the Information Technology (Intermediaries Guidelines), 2011, still serves as the heart of the cyber law provisions in India. All these tools are in control of electronic agreements, digital signatures, data security requirements, the liability of intermediaries and safe harbor.

The judicial interpretation has been very instrumental in determining the edges of e-commerce regulation. Such landmark cases as the Shreya Singhal v. V. Christian Louboutin SAS Union of India. It has been made clear by Nakul Bajaj, Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd., and others that there is an extent of intermediary immunity in terms of Section 79 of the IT Act, the interpretation of the term actual knowledge, as well as the difference between passive and active participants in the online transactions. Indian courts have increasingly through these decisions established the boundaries of platform neutrality, due diligence and corporate responsibility.

The paper will discuss the changing legal framework of e-commerce in India, considering the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, the Intermediary Guidelines Rules, 2011, and the major case law. It tries to assess how all these statutory and judicial developments are trying to find a compromise between consumer rights protection, data privacy, digital innovation and intermediary immunity in the fast growing digital economy.

2 The Digital Personal Data Protection Act (DPDP Act) of 2023

2.1.1 Background

The Digital Personal Data Protection Act, 2023 (DPDP Act) is one of the important milestones in the Indian history of enacting a law to secure privacy of information about individuals in the digital area. The judgment in Justice K.S. Puttaswamy (Retd.)[1]was laid down by the Supreme Court in the creation of the Act. v. In Union of India, the right to privacy was held to be recognized as a fundamental right under Article 21 of the

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

Indian Constitution. This is a landmark case in the history of the Indian Constitution that established a constitutional requirement of a data protection regime in India[2].

Next, the Ministry of Electronics and Information Technology (MeitY) formed a committee headed by Justice B.N. Srikrishna that has provided its findings in 2018. Multiple versions of data protection bills were presented such as the 2019 Personal Data Protection Bill which was withdrawn in 2022 after a full committee examination[3]. In November of 2022 a revised version known as the Digital Personal Data Protection Bill, 2022 was published as a feedback period. The final, version known as The Digital Personal Data Protection Bill, 2023 was introduced in Parliament in August of 2023, given Presidential assent on August 11, 2023, and established as the original of India[4]

The Act aims at striking a balance between individual privacy and the necessity of data-driven management and business effectiveness[5]. It regulates electronic personal information that are processed in India and also extends to data processing outside of India when these involve the offering of goods or services to anyone in India.? The legislation also provides a regulatory structure through the Data Protection Board of India in the form of an enforcement mechanism.[6]

2.1.2 Legal framework

In India the Digital Personal Data Protection Act, 2023 (DPDP Act) offers the legal basis of protecting the digital personal data. This law is paramount to the e-commerce sector that depends extensively on gathering and storing consumer data and conducting processing of this data. The Act determines the principles according to which online platforms receive the consent of the user, manage personal data, and provide data security and responsibility. It complies with the international principles such as the GDPR and imposes a duty of responsibility in Indian and foreign electronic commerce companies providing products and services to Indian customers.

[2]PRS LEGISLATIVE RESEARCH, https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023 (last visited July 29, 2025). PRS LEGISLATIVE RESEARCH, https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023 (last visited July 29, 2025).

[3]MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, *The Digital Personal Data Protection Bill, 2022 – Public Consultation*, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf (last visited July 29, 2025).

[4]LOK SABHA, https://loksabha.nic.in/ (last visited July 29, 2025).

[5]USERCENTRICS, https://usercentrics.com/knowledge-hub/india-digital-personal-data-protection-act-dpdpa/ (last visited July 29, 2025).

[6]Anirudh Burman, Understanding India's New Data Protection Law, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Oct. 17, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law.

Table 1- Digital Personal Data Protection Act, 2023 (DPDP Act) and e-commerce

Section	Provision	Implication for E-Commerce
§2(h), §2(j)[7]	Definitions of "Data Fiduciary" and "Data Principal"	E-commerce companies are "data fiduciaries"; customers are "data principals".
§3[8]	Applicability	Applies to digital personal data in India and also foreign entities offering goods/services to Indian users.
§4[9]	Obligation to process data for lawful purposes with consent	E-commerce platforms must obtain consent before collecting personal data.
§6[10]	Notice before consent	Platforms must inform users of data usage in plain language.
§7[11]	Validity of consent	Consent must be free, specific, informed, and capable of being withdrawn.
§9[12]	Duties of data fiduciaries	E-commerce entities must ensure data accuracy, security, and prevent misuse.
§10[13]	Special duties of significant data fiduciaries	Large e-commerce companies (determined by volume of data or risk) have additional compliance obligations like DPO appointment and audits.
§12[14]	Rights of data principals	Customers have rights to access, correction, and erasure of their data.
§14[15]	Grievance redressal	Platforms must establish grievance mechanisms.
§21[16]	Data Protection Board of India	Regulates, monitors, and enforces compliance.
§33[17]	Penalties	Non-compliance may lead to penalties up to ₹250 crore, affecting e-commerce firms significantly.

The Digital Personal Data Protection Act, 2023[18] creates an overarching legal framework that provides guidance on the manner in which digital personal data are required to be treated especially by the e-commerce sites. The Act under the section §2 (h) and (j) classifies the e-commerce companies as data fiduciaries and individual users as data principals. This classification makes direct accountability on e-commerce operators as being responsible, fair and legal in the management of data.

[7] Digital Personal Data Protection Act, 2023, § 2, No. 22, Acts of Parliament, 2023 (India).
[8] Id. § 3.
[9] Id. § 4.
[10] Id. § 6.
[11] Id. § 7.
[12] Id. § 9.
[13] Id. § 10.
[14] Id. § 12.
[15] Id. § 14.
[16] Id. § 21.
[17] Id. § 33.
[18] Digital Personal Data Protection Act, 2023, § 2(h)–(j), No. 22, Acts of Parliament, 2023 (India).

Under section 3[19], the Act applies in a broad sense not only to those entities that exist in India, but also to foreign e-commerce companies that process personal data in relation to the provision of goods or services to users in India.

Sections 9 and 10 place certain responsibilities on data fiduciaries, which means e-commerce companies must verify data, provide security measures, and have limited data retention[20]. Moreover, the extra requirements include the appointment of Data Protection Officer (DPO) to e-commerce companies that are designated Significant Data Fiduciaries (SDFs), regular audits, and Data Protection Impact Assessments (DPIAs), based on the volume or sensitivity of processed data[21].

On the one hand, consumers, or in other words, data principals, obtain rights according to section 12, which include the right to access, correct, update, and erase their personal data.[6] They also have the right to an effective grievance redressal mechanism, which is to be provided by platforms under section 14. On the other hand, the adjudicatory and enforcement bod is the Data Protection Board of India, established under section 21, and its mandate is to monitor compliance and address violations.[8] In case of violations,

2.1.3 Judicial precedents concerning e-commerce in India

Since the Digital Personal Data Protection Act, 2023 (DPDP Act) is the new law, as of writing no judgment has been reported interpreting its clauses directly before Indian courts. Nevertheless, a number of ongoing court challenges (including some landmark cases), as well as an earlier landmark case, also take issue with the fundamental concerns dealt with under the DPDP Act particularly the e-commerce scenario such as the issue of user consent and data misuse, platform liability and intermediary liability.

3 Information Technology Act, 2000 (the IT Act)

3.1.1 Background

First legislation action taken by India includes the Information Technology Act, 2000[22], an initial step to the system of control of the digital environment. This arose as a response to the increased necessity of India to have a legal framework in which to regulate electronic commerce, online authentication and prevention of cyberspace crimes. To a great extent, the UNCITRAL Model Law on Electronic Commerce, 1996[23] formed the basis of the Act, which aimed to harmonize the legal regulations governing the e-commerce between various jurisdictions.[2] This harmonization meant that electronic records and e-signatures had legal recognition and therefore online contracts and digital records were able to have the same legal strength as the physical records.

The IT Act was given the Presidential assent on June 9 2000 and came into force in October 17 2000[24]. It brought about important authorities like the Controller of Certifying Authorities (CCA) to regulate digital signature certificates and criminal punishment to offences like hacking, data theft, and transmission of

[19] Id. § 3.
[20] Id. § 9.
[21] Id. § 10.
[22] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[23] U.N. *Comm'n on Int'l Trade Law, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996*, U.N. Doc. A/RES/51/162, https://uncitral.un.org/en/model-laws/e-commerce (last visited July 29, 2025).
[24] Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

obscene content. Subsequently, the scope of the Information Technology (Amendment) Act, 2008 was further expanded with incorporation provisions of data protection, intermediary liability (SS 79)[25] and cyber terrorism (SS 66F)[26]. The IT Act has thus become the chief source of law of cyber law in India that provides a foundation basis to e-commerce, content regulation on the internet, and the right to privacy (digital) during the time when the DPDP Act was in its pre-gestation period.

3.1.2 Legal framework

The Information Technology Act, 2000 is the pillar of law on the electronic commerce (e-commerce) in India. The Act was enforced to meet the challenges of skyrocketing internet usage and digital business backed up by the fact that the Act acknowledges the validity of electronic records and the validity of digital signatures hence the ease in terms of online contracts and transactions. The latter two sections, 4 and 5[27], give legal status to electronic records and computer technology-based digital signatures, and treat them as identical to their physical equivalents in the more conventional world of commerce. This has enabled companies to transfer major business processes to the web like invoice creation, order validation and contract signing.

Section 10A[28] is one of the most significant provisions of the online commerce since it legitimizes electronic contracts. It explains that an electronic agreement (including clickwrap agreements, operations of online acceptance of terms and electronic bidding) cannot be outlawed as being enforceable merely because it was made electronically. This has been of great importance in facilitating the use of online agreements like terms of use, privacy policy and subscription contracts underlying e-commerce websites like Amazon, Flipkart and Myntra.

As a measure of safeguarding user data and privacy, which happens to be of paramount importance in the course of e-commerce operations, Section 43A[29] holds companies liable in case they neglect reasonable security procedures to safeguard the personal data. In case of a company being careless with data security and this careless attitude leads to the wrongful loss or acquisition, the concerned party can be compensated. In addition to this, Section 72A[30] also provides it with criminal sanction against unlawful disclosure of personal information regardless whether this disclosure takes place in contravention of official contracts. Such requirements put a strict liability upon the e-commerce providers, as such forums involve dealing with sensitive information such as names, addresses, financial, and shopping patterns regularly.

The Act also presents severe provisions of crime to combat e-commerce fraud. Identity theft is also criminalized under sec 66C[31] and this develops to refer not only to the unlawful usage of identifiers, but it also covers illicit usage of password, digital signatures, among other distinctive identifiers. Equally, s 66D[32] is a criminal offence of cheating by personation under computer facility, it can be applied to phishing, false

[25] Information Technology Act, 2000, §§ 79
[26] Id. §§ 66F
[27] Information Technology Act, 2000, §§ 4–6
[28] Id. §§ 10A
[29] Id. §§ 43A
[30] Id. §§ 72A
[31] Id. §§ 66C
[32] Id. §§ 66D

product ad, or pretence in the identity of a seller or purchaser. These are also the sections that play a vital role in the protection of consumers who utilize the digital platforms against online fraud and deception.

Responding to it, the importance of Section 79[33] should be mentioned that offers a safe harbor to the intermediaries, and e-commerce platforms are not an exception. It relieves intermediaries of liability of third party information, data, or communication links that are present on their platforms- as long as they carry out due diligence and take quick literate redress, when they become aware of information or obtain knowledge of unlawful content on their websites under actual knowledge or by informing them. This clause balances the interests of making a platform responsible and not subjecting them to excessive punishment of user behaviors. Finally, the Section 85[34] offers the corporate liability, where senior officials will be held responsible of the offense occurred by the companies, thus enhancing adherence at the top echelons.

Table 2 - Information Technology Act, 2000 (the IT Act) and ecommerce

Section	Title / Subject	E-Commerce Relevance
§ 4	Legal recognition of electronic records	Treats e-documents like physical contracts
§ 5	Legal recognition of digital signatures	Enables signing of contracts online
§ 6	Use of electronic records in government and commerce	Promotes e-governance and e-filing
§ 10A	Validity of electronic contracts	Recognizes formation of valid online contracts
§ 43A	Compensation for failure to protect personal data	Imposes civil liability on platforms for data breaches
§ 66C	Identity theft	Protects e-commerce users from impersonation
§ 66D	Cheating by personation using computer resources	Penalizes online fraud by impersonation
§ 72A	Disclosure of information in breach of contract	Criminal liability for breach of consumer data confidentiality
§ 79	Exemption from liability for intermediaries	Defines intermediary role for e-commerce platforms, grants conditional immunity
§ 85	Offenses by companies	Holds directors and officers accountable for company violations

[33] Id. §§ 79
[34] Id. §§ 85

3.1.3 Judicial precedents concerning e-commerce in India

1. Christian Louboutin SAS vs. Nakul Bajaj &Ors.[35]The Delhi High court had ruled that the Darveys.com could not exercise intermediary protection under the IT Act, Section 79 since it actively assisted in marketing and selling luxury goods without permission. The platform was actively involved in terms of the use of trademarked meta-tag, curated listings, and promotional materials. Consequently, it was not granted the safe harbor immunity and instructed to take down infringing posts and provide information about sellers.

2. Amazon Seller services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. and others.[36]In the present case, an injunction barring the sale of direct-selling products to the Amazon and Flipkart was overturned by the Delhi High Court Division Bench. The Court declared that the 2016 Direct Selling Guidelines were advisory and did not have a legal obligation. It restated that platforms may invoke safe harbor under Section 79 when they are intermediaries and are undertaking due diligence without knowing that there is infringement.

3. SnapdealPvt. Ltd. v. State of Punjab.[37]Snapdeal was criminally liable in selling substandard sanitizers in times of COVID-19. The Haryana and Punjab High Court ordered the cancellation of the FIRs, as Snapdeal was identified as an intermediary as per the 2 (1) (w) of the IT Act. According to the decision made by the Court, Section 79 immunity will be used in cases where the platform practices due diligence and does not know about the wrongdoing.

4. Kent RO Systems Ltd. v. Amit Kotak and ORs.[38]Kent RO was against illegal sale of its products over the internet without the right warranties or quality inspection. The Delhi High Court underlined that it is the duty of e-commerce platforms to ensure compliance and safety, particularly of health-related products. It uncoded the implausible listing, suggesting that the intermediary immunity might lack where there is not enough diligence.

5. Myspace Inc. vs Super Cassettes industries Ltd.[39]The Delhi High Court ruled that intermediate is only liable to copyright infringement when they get actual knowledge of the infringement by virtue of a court or a government order. Myspace enjoyed safe harbor in the Section 79 because it had no such knowledge. The case laid the foundation of the principles of the notice-and-takedown that determine intermediary liability in India.

[35] Christian Louboutin SAS vs. Nakul Bajaj, 2018 SCC OnLine Del 13032 (India).
[36] Amazon Seller Servs. Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd., 2019 SCC OnLine Del 11152, appeal disposed by Division Bench, 2020 SCC OnLine Del 454 (India).
[37]Snapdeal Pvt. Ltd. v. State of Punjab, 2020 SCC OnLine P&H 402(India).
[38] Kent RO Sys. Ltd v. Amit Kotak, (2017) SCC OnLine Del 7220 (India).
[39] Myspace Inc. v. Super Cassettes Indus. Ltd., (2017) 236 DLT 478 (India).

4 Information Technology (Intermediaries Guidelines) Rules 2011 (the IT Intermediary Rules)

4.1.1 Background

The Information Technology (Intermediaries Guidelines) Rules 2011 have been issued by the Ministry of Electronics and Information Technology (MeitY) under the Section 87(2)(zg) read with Section 79(2) of the Information Technology act, 2000. These regulations were declared on April 11, 2011, to offer a notion on the due diligence of the intermediaries including internet service providers, social networking sites, e-business websites, and online trading sites[40].

These rules were introduced due to the increased amount of user-generated content and alarm with the issue of cybercrime, defamation, copyright violation, hate speech, and misinformation on the internet. Although in Section 79 of the IT Act conditional protection on grounds of safe harbor was applied on intermediaries, it failed to mention a clear statement defining as to what was meant by due diligence. The 2011 Rules tried addressing this loophole by dictating what responsibilities intermediaries should abide by in order to avail themselves of this exemption.

The regulations forced intermediaries to post terms of use, warn users against uploading unlawful or harmful materials and endeavor to take it down within reasonable time after they got actual knowledge or receive information on the same by government agencies. It also placed the burden of content moderation such as bans on obscene, defamatory, encouragement of gambling, national security threats and acts of violence.

In the years that came by, the 2011 Rules were assailed on the account of being opaque, open to censorship and the absence of procedural protection when it comes to material removal, which triggered scrutiny by the court. In Shreya Singhal v., it is worth noting that very few cases do not even apply. The Supreme Court of India held that the Union of India had to read the laws down to safeguard freedom of speech with respect to the content takedown systems. The government notified the revised Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 in reaction to the increase in the digital platform and the ineffective nature of the 2011 Rules against the burgeoning technologies.

4.1.2 Legal framework

The Information Technology (Intermediaries Guidelines) Rules, 2011 that have been framed under the Information Technology Act, 2000, Section 79(2)[41], are central in determining the legal liability of the e-commerce platforms in regulating as intermediaries. These rules provide a list of the due diligence that intermediaries must comply with in availing themselves to the protection due to safe harbor pursuant to s.79 of the IT Act. In the case of e-commerce a vital protection, since third-party sellers conduct a large proportion of the listings on platform, and might have to be held liable in the event of infringing or illegal contents/products unless they adhere to such due diligence standards.

[40] Information Technology (Intermediaries Guidelines) Rules, 2011, Gazette of India, Extraordinary, Part II, sec. 3(i), G.S.R. 314(E) (Apr. 11, 2011) (India), available at https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf.
[41] Information Technology Act, 2000, §§ 79(2)

Significant Regulations Applied to Electronic Commerce Sites

- Rule 3(1)[42] - Imposes an obligation on the intermediaries (e.g. e-commerce websites) to make the terms of use, privacy policies and agreement of use public knowledge to make the users aware of the proscribed content and conduct.
- E-commerce relevance: The platforms should warn sellers and buyers against listing and dealing with banned goods either in the form of counterfeiting goods, illegal substances or even defaming information.
- Rule 3(2) - Disallows the people to host or transmit material that is abusive, offensive, invasive of privacy, infringement of intellectual property or harmful to minors, etc.
- E-commerce relevance: Avoids sale of quality offensive goods, infringement goods, like fake branded products or pirated products. The e-commerce intermediaries are expected to make reasonable effort to avoid such misuse.
- Rule 3(3) - provides that the intermediary must not knowingly host or publish any of the prohibited information and must take action when it has been notified that "actual knowledge" has been received of such information being hosted and published by the intermediary.
- E-commerce relevance: E-commerce sites such as Amazon or Flipkart, need to remove anything that is marked as illegal, counterfeit, or malicious in time, as otherwise, they may face a penalty of no longer having intermediary immunity.
- Rule 3(4) - Requires intermediaries to take problematic material down or block it in 36 hours of actual knowledge or a court order or a government.
- E-commerce relevance: This sets a tight takedown schedule to delist counterfeit goods or delisting false listings upon receipt of notice.
- Rule 3(5) - The rule dictates that the intermediaries store user records not less than 90 days and share it with the government, when requested.
- E-commerce applicability: Facilitates regulatory control and the enforcement of legislation of consumer fraud, cybercrime, or the violation of IP in e-commerce transactions.

Effects on E-Commerce Business

The 2011 Rules have successfully made the safe harbor protection under 79 conditional upon prompt notice-and-takedown obligation and content guidelines enforcement. In the case of an e-commerce business, this becomes the requirement that platform neutrality is necessary but not sufficient and firms need to make sure that:

- Immediate response to take-down violating listings,
- Correct authentication of users,
- Presentation of seller information,
- Upkeep of data notes, and

[42]*Information Technology (Intermediaries Guidelines) Rules, 2011*, r. 3(5), G.S.R. 314(E), Gazette of India, Extraordinary, Part II, sec. 3(i) (Apr. 11, 2011) (India).

- Conspicuous expression of policies to the users.

Their non-observance may lead to the loss of immunity and civil or criminal liability of illegal user-generated material or acts of a third party.

4.1.3 Judicial precedents concerning e-commerce in India

1. Shreya Singhal v. Union of India[43] The IT Act in Section 66A was deemed by the Supreme Court to be unconstitutional in that it infringed upon the freedom of speech guaranteed by Article 19(1)(a). It also interpreted the Rule 3(4) of the Intermediary Guidelines which provided that intermediaries should only act upon being ordered to by the court or after the government notifies them. This ruling guaranteed e-commerce sites against false takedown requests and defined what constitutes actual knowledge in Section 79.

2. Dinesh Agrawal Chandra Agrawal v. State of Bihar.[44] The High Court of Patna said that intermediary status per se does not warrant immunity under Section 79 of the IT Act. Although IndiaMART had been identified as an intermediary, the Court stressed that safe harbor would require adherence to the due diligence requirements. As there was no sufficient evidence of seller authentication and precautionary measures, the criminal process was permitted to run its course.

3. KunalBahl v. State of Karnataka[45]Karnataka High Court determined that Snapdeal was eligible to be classified as an intermediary under Section 2(1)(w) of the IT Act despite coming up with listings of regulated products. Since the platform possessed apparent policies, ban lists and complaint channels, it was discovered to have due diligence. This resulted in the quashing of the FIRs against Snapdeal and its directors as it proceeded to affirm protection under Section 79.

4. Flipkart Internet Pvt. Ltd. v. State of NCT of Delhi &Ors.[46]Criminal charges against Flipkart on the ground of selling counterfeit cosmetics by third party sellers were quashed by the Delhi High Court. It believed that middle-level immunity by Section 79 is applicable to criminal responsibility, as long as due diligence is observed. The Court restated that platforms must comply solely with court or government directives, and not with individual complaints, which further protects safe harborto the e-commerce marketplaces.

5 Recommendations

Considering the changing legal landscape of e-commerce in India, some proposals can be made to enhance the effectiveness of the regulations and maintain the innovation and development of the digital environment.

To begin with, the implementation guidelines under the Digital Personal Data Protection Act, 2023 (DPDP Act), especially regarding the consent management, cross-border data transfer, and Significant Data Fiduciary (SDF) classification, can use a better clarification. Specific regulations and compliance standards

[43] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[44] Dinesh Agrawal @ Dinesh Chandra Agrawal v. State of Bihar, Cr. WJC No. 347 of 2018, Patna H.C. (India, May 2, 2018).
[45]Snapdeal Pvt. Ltd. (KunalBahl&Ors.) v. State of Karnataka, Crl. P. No. 100652-53 of 2021 (Karn. H.C. Feb. 24, 2022) (India).
[46] Flipkart Internet Pvt. Ltd. v. State of NCT of Delhi &Ors., Writ Petition (Criminal) No. 1376 of 2020 (Del. H.C. Aug. 17, 2022) (India).

(based on the sector) would help limit the confusion of e-commerce platforms and create consistency in enforcement of the law. Data Protection Board of India needs to be operationalized with transparent procedures, appellation and publication of compliance advisories.

Second, the Intermediate liability in Section 79 of Information Technology Act, 2000 ought to be aligned with the changing judicial practice. An integrated system of compliance that includes the IT Act, the Intermediary Guidelines Rules, and the DPDP Act would assist the platforms to be more familiar with the overlapping responsibilities concerned with the due diligence, data protection, and takedown process. Clarity in statues by creating a distinction between active participation and passive facilitation would minimize legal ambiguity.

Third, online stores must embrace effective internal compliance policies, such as automatic counterfeit identification methods, improved seller verification policies, open grievance redressal procedures, and regular legal audits. The active compliance and adherence does not only protect the safe harbor coverage, but also increases consumer confidence.

Lastly, regulators, judicial, and enforcement agencies should be able to deal with complicated digital conflicts through capacity-building programs. Consultations with stakeholders on a regular basis with government, industry, consumer groups, and legal experts would keep regulatory reforms up to date with the advancements in technology.

All these would result in a balanced ecosystem that safeguards the rights of consumers, enhancing the privacy of the information, and ensuring the continuance of innovation in the Indian digital economy.

6 Conclusion

The regulatory environment of e-commerce in India is an indication of a slow but consistent change of a facilitative regime to a more structured and accountability-oriented regime. Information Technology Act, 2000 provided the legal acknowledgement of electronic records, digital signatures and online contracts and thus facilitated the expansion of digital business. It was through Section 79 that it brought the idea of intermediary safe harbor, and this has been pivotal in the operation of online marketplaces. Nonetheless, the courts have always made it clear that conditionality of such immunity is based on due diligence and the fact that they do not actively engage in illegal activities.

The Information Technology (Intermediaries Guidelines) Rules, 2011 further rationalized the responsibilities of the intermediaries by establishing the standards of due diligence and the processes of examples of notice-and-takedown. Intervention of the Supreme Court in Shreya Singhal allowed keeping these requirements within the constitutional provisions on the freedom of speech, limiting the interpretation of actual knowledge and eliminating arbitrary deletion of content. The subsequent decisions made in the High Court regarding the e-commerce platforms added to the idea that the intermediary protection is not absolute and depends on the exhibited compliance, transparency, and good faith practices.

The introduction of the Digital Personal Data Protection Act, 2023 is a major step in the development of the digital system of governance in India because the new law deals with the past scattered concept of protection of the data. The DPDP Act improves the user autonomy and accountability of corporations in the digital economy by setting clear boundaries on the roles of data fidelicers and data principals, requiring consent-based processing, and imposing significant fines on non-compliance. Its universal applicability provides that foreign e-commerce players that do their business in India are covered by the same India standards of data protection, thus promoting regulatory consistency.

Taken together, these legislative tools and judicial statements are manifestations of India trying to balance economic development and constitutional principles, consumer protection, and online trust. Though the structure is still being improved, particularly due to the practical implementation of the DPDP Act, the direction is showing a move to more responsibility, transparency, and structured compliance of e-commerce platforms. The future of digital commerce in India will not only be the statutory enforcement but also the capacity of the platforms to incorporate these legal standards into their working models hence creating a safe, privacy-conscious and innovation-friendly marketplace online.

7 References

Statutes and Rules

1. The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
2. The Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
3. The Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2009 (India).
4. The Information Technology (Intermediaries Guidelines) Rules, 2011, G.S.R. 314(E), Gazette of India, Apr. 11, 2011 (India).
5. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Feb. 25, 2021 (India).
6. The Constitution of India, 1950.
7. The Drugs and Cosmetics Act, No. 23 of 1940, Acts of Parliament, 1940 (India).
8. The Trade Marks Act, No. 47 of 1999, Acts of Parliament, 1999 (India).
9. The Copyright Act, No. 14 of 1957, Acts of Parliament, 1957 (India).

Judicial Decisions

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
3. *Christian Louboutin SAS v. Nakul Bajaj &Ors.*, 2018 SCC OnLine Del 12215 (Delhi High Court).
4. *Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd.*, 2020 SCC OnLine Del 454 (Delhi High Court).
5. *SnapdealPvt. Ltd. v. State of Punjab*, 2020 SCC OnLine P&H 516 (Punjab & Haryana High Court).
6. *Kent RO Systems Ltd. v. Amit Kotak &Ors.*, 2017 SCC OnLine Del 7801 (Delhi High Court).
7. *Myspace Inc. v. Super Cassettes Industries Ltd.*, 2017 SCC OnLine Del 11625 (Delhi High Court).

8. *Dinesh Agrawal Chandra Agrawal v. State of Bihar*, Cr. WJC No. 347 of 2018 (Patna High Court).
9. *KunalBahl v. State of Karnataka*, Crl. P. Nos. 100652–100653 of 2021 (Karnataka High Court).
10. *Flipkart Internet Pvt. Ltd. v. State of NCT of Delhi &Ors.*, W.P. (Crl.) No. 1376 of 2020 (Delhi High Court).

Reports and Secondary Sources

1. Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Report of the Committee of Experts on Data Protection, Ministry of Electronics & Information Technology, Government of India, 2018).
2. Ministry of Electronics and Information Technology (MeitY), *Digital Personal Data Protection Bill, 2022 – Explanatory Note*.
3. UNCITRAL Model Law on Electronic Commerce, 1996.