ILE CONSUMER PROTECTION LAW AND REVIEW

VOLUME 3 AND ISSUE 1 OF 2025

APIS -3920-0023 | ISSN - 2583-8024

Published by

Institute of Legal Education

https://iledu.in

REDEFINING CONSUMER RIGHTS IN THE AGE OF ALGORITHMS: DATA PRIVACY, CONSENT, AND PLATFORM ACCOUNTABILITY

AUTHORS - ADV MONICA MADAAN* & ARRYAN MOHANTY**

* LLM STUDENT OF KR MANGALAM UNIVERSITY, GURUGRAM

** STUDENT OF SYMBIOSIS LAW SCHOOL, NAGPUR

BEST CITATION - AMAN MUJEEB, REDEFINING CONSUMER RIGHTS IN THE AGE OF ALGORITHMS: DATA PRIVACY, CONSENT, AND PLATFORM ACCOUNTABILITY, *ILE CONSUMER PROTECTION LAW AND REVIEW*, 3 (1) OF 2025, PG. 01-16, APIS -3920-0023 | ISSN - 2583-8024.

Abstract

The swift advancement of digital markets has significantly altered the consumer experience, brought about new conveniences, and also subjected consumers to intricate and frequently unclear digital practices. In this digital age, algorithms, data analysis, and artificial intelligence are central to influencing consumer decisions, customising content, and regulating access to products and services. This paper offers a critical examination of the changing landscape of consumer rights in response to these technological advancements, focusing specifically on data privacy, informed consent, and the accountability of digital platforms. It contends that existing consumer protection laws, crafted initially for physical goods and straightforward transactions, are increasingly insufficient in tackling the challenges introduced by algorithmic decision-making, deceptive design practices, and data-driven profiling. The study delves into the overlap between consumer rights and data protection regulations, evaluating whether consumers genuinely have significant control over their data given the existence of long, complex, and often misleading consent processes. Additionally, it explores the responsibility of e-commerce platforms and digital intermediaries concerning problems such as misleading advertisements, fraudulent reviews, and the impact of sponsored promotions. This paper highlights effective practices and reveals deficiencies in the current legal structure by conducting a comparative analysis of global regulatory frameworks. In conclusion, the paper advocates for rediscovering consumer rights in the digital realm, which guarantees transparency, fairness, and accountability from digital service providers, while equipping consumers with genuine control over their digital identities and decisions.

Introduction

Technological progress during the Fourth Industrial Revolution has profoundly improved human productivity and effectiveness across various industries. This revolution signifies a thorough transformation in production, marked by integrating digital technologies and the internet into traditional manufacturing systems. Consequently, the global economy has transitioned into a new phase, often called the digital economy, where internet-based communication plays a pivotal role in economic activities. A key indicator of this transition is the remarkable increase in e-commerce, which has become a favoured transaction method. The digital age has instigated substantial alterations in consumer behaviour and preferences, fostering a strong tendency toward online shopping. E-commerce platforms attract consumers due to their convenience, extensive product variety, and competitive pricing. Nonetheless, this shift has

ILE CONSUMER PROTECTION LAW AND REVIEW
VOLUME 3 AND ISSUE 1 OF 2025
APIS -3920-0023 | ISSN - 2583-8024
Published by
Institute of Legal Education
https://iledu.in

also presented challenges, including consumer rights, data privacy, cybersecurity, product authenticity, and efficient grievance resolution. Ensuring secure transactions has become a central concern, necessitating the implementation of encryption technologies and safe computing practices. Simultaneously, upholding product standards and fair pricing remains crucial for preserving consumer trust and satisfaction. In this changing environment, consumer protection has become an essential area of law, consisting of principles and regulations designed to protect consumer interests and tackle the novel risks and complexities within the digital marketplace.[1]

A consumer buys and uses products or services in exchange for money. The responsibility of ensuring consumer protection is an ongoing social and economic obligation that the government and businesses share, primarily focused on defending consumer interests and guaranteeing fair treatment. This protection covers various elements, including the safety of products, proper labelling, transparent pricing, prevention of fraudulent market practices, and resolving complaints that may emerge from corporate mergers or acquisitions. Consumer rights are essential for the operation of fair and ethical commerce. They are designed to protect individuals from exploitative business practices and ensure they have access to quality, affordable, and safe products and services. Necessary consumer rights include the right to safety, the right to be informed, the right to choose, and the right to express concerns. These rights are backed by a legal and regulatory system intended to facilitate the resolution of grievances and ensure that companies are held accountable. Moreover, government agencies and consumer advocacy organisations are vital in raising awareness and enforcing consumer protection measures. This regulatory framework faces increasing challenges in the digital era, where issues like online scams, data misuse, and privacy infringements create new complexities. The contemporary consumer protection system must adapt to tackle these challenges and safeguard the rights of individuals in an ever-evolving marketplace.[2] We live in a digital age where machines increasingly take over tasks that people once completed. The growing dependence on technology is so substantial that this year's World Consumer Rights Day focused on the theme: "Fair and Responsible AI for Consumers." Generative Artificial Intelligence, which monitors user behaviour and provides tailored recommendations, has advanced rapidly. While this technology offers convenience in our fast-paced, technology-driven society, it raises significant concerns about data privacy and user consent. As AI becomes more prevalent in consumer interactions and business practices, it is crucial to ensure consumer rights are not violated. Safeguarding privacy, promoting transparency, and holding digital systems accountable are now vital aspects of consumer protection in the era of intelligent machines.

Hillary Clinton once remarked that efforts should focus on reinforcing consumer protections rather than diminishing them. The growth of e-commerce has heightened the necessity for enhanced consumer safeguards. Technological advancements in India have significantly transformed how businesses and consumers interact. Consumers play a crucial role in the economic framework, as their preferences drive the entire production and distribution process. Today's consumers are increasingly drawn to the convenience of online shopping instead of navigating busy marketplaces or engaging with aggressive sales staff. The internet provides transparency in pricing and a broader selection of products, making it a more appealing choice for many. In the current digital environment, safeguarding consumer interests has become more essential

[1] Achmad Zulfa Andikatama & Bambang Eko Turisno, Consumer Protection Law in the Digital Era, Vol 7 Issue 7, IJSSHR, 4552-4557 (2024) https://ijsshr.in/v7i7/Doc/3.pdf

[2] Dr Amar Vijay Jamnekar, Consumer Rights In The Digital Age: Navigating Modern Challenges, Vol 4 Issue 2, TIJCM, 67-76 (2024) https://ij.darshan.ac.in/Upload/DIJCM/December-2024-Vol-4-Issue-II/December-2024-Vol-4-Issue-II_JD_2408.pdf

than ever. The rise of e-commerce platforms has brought about various legal and regulatory challenges. Implementing new technologies and economic liberalisation policies in India has greatly influenced sectors like finance and retail. While conventional retail outlets and shopping malls cater to customers within specific geographic areas, online marketplaces break these barriers and provide access to a global audience. The digital transformation has revolutionised consumer habits, with e-commerce platforms eliminating many physical limitations, allowing individuals to discover a wide array of products and services at the click of a button. However, this change has impacted local enterprises' viability and outreach. The online shopping sector has grown rapidly in the last twenty years. Consumers' purchasing behaviours have changed considerably due to this digital advancement. In 2022, India's e-commerce sector was valued at $78.5 billion and is expected to reach $130 billion by 2025. Factors such as widespread internet availability, increased mobile shopping, and the convenience of online payments have played a crucial role in this growth. At the same time, advertising has adapted alongside evolving societal norms and values. Nevertheless, pinpointing when deceptive advertising began is challenging, as these tactics have slowly developed in response to societal shifts.[3]

Evolution of AI in Consumer Interactions

Artificial intelligence has become crucial to people's everyday lives, providing convenience, personalisation, and efficiency through various digital tools and platforms. Virtual assistants like Amazon Alexa, Samsung Bixby, and Apple Siri make daily tasks easier, respond to voice commands, offer quick information, and give personalised recommendations on streaming services and e-commerce sites, influenced by users' preferences and behaviours. AI-driven customer service tools, such as chatbots, deliver instant assistance and continually learn to improve their problem-solving skills. Similarly, AI-enhanced navigation systems in ride-hailing applications enhance travel experiences by optimising routes and minimising delays. AI customises outreach efforts in marketing to match particular consumer interests, ensuring that promotional messages reach the right audience. Smart home and office devices also automate daily tasks, boost energy efficiency, and enhance overall convenience.

AI integrates across various platforms, including mobile apps, websites, social media, and face-to-face interactions. No matter how consumers interact with these systems, AI aims to provide consistent, efficient, and valuable experiences. Companies also gain significantly from AI by analysing consumer behaviours, preferences, and buying patterns, which enables proactive engagement with potential customers. Post-sale support has experienced notable enhancements, with AI facilitating real-time language translation and consumer sentiment analysis. These technologies aid in prioritising and resolving issues swiftly, often without human intervention. Given AI's potential to revolutionise consumer experiences and streamline business operations, it is increasingly essential to change our perspectives. AI should be regarded as a commercial asset and a powerful tool to uphold consumer rights, guarantee privacy, and safeguard against unfair trade practices. Using AI responsibly can help bridge the enforcement gaps that consumers and regulatory bodies face in the digital era.

AI-driven consumer goods and services are swiftly making their way into the market, leading to an increase in AI-related products taking over the consumer landscape. Businesses have recognised this as a lucrative opportunity and, in some instances, have utilised a strategy known as "AI-washing," a marketing approach that inflates the genuine use of artificial intelligence in their products. Items described as "smart" or "digital," including cameras,

[3] Arryan Mohanty, Consumer Rights in the Digital Era: Online Shopping and Legal Safeguards (6 October, 2023, 12:46 AM) https://lawinsider.in/columns/consumer-rights-in-the-digital-era-online-shopping-and-legal-safeguards

doorbells, speakers, refrigerators, and washing machines, frequently integrate AI components. These products are anticipated to fulfil standards of quality, durability, and safety to be suitable for consumer use. Nevertheless, numerous smart home devices present considerable cybersecurity threats due to their susceptibility to hacking. With minimal encryption and rare software updates, they can serve as gateways for cyber-attacks, jeopardising consumer privacy and data security. The potential for unauthorised access and exploitation of these devices is an increasing worry.[4]

On the service side, AI-enhanced products can sometimes act as service providers. Instances include digital assistants and platforms like Digi Yatra, which depend on tangible hardware or software interfaces. Consumers expect these services to provide precise, pertinent, and valuable recommendations. However, the liability issue becomes intricate if these services falter, such as delivering incorrect answers, missing reminders, or giving advice that could jeopardise safety. Since these systems operate based on algorithms, identifying responsibility for service failures is complicated. Generally, service providers have a duty of care toward consumers, but applying the same legal standards is challenging when the actions originate from machine learning algorithms instead of human intent. In these situations, the liability may lie with the developers or corporations behind these AI systems, as they create and implement the technology consumers rely upon.

As artificial intelligence technologies broaden their influence, gathering user information has become more extensive, prompting significant privacy concerns. People often cannot control or comprehend how their data is collected, processed, and used. The lack of clarity surrounding AI operations makes it challenging for users to understand the reasoning behind algorithmic choices. Furthermore, the data utilised to train these systems is often tainted with existing societal prejudices. Consequently, AI applications may yield biased or unfair results based on race, gender, age, or other personal traits. When training datasets lack diversity or do not accurately represent the population, the risk of producing unjust or harmful outcomes is significantly increased. There have already been cases of privacy violations and biased practices across different industries. For instance, one educational institution used students' internet browsing information for behavioural assessments without securing their consent, which raised ethical and legal issues. In another case, AI-driven recruitment tools were shown to favour male applicants over female ones, perpetuating gender biases. Likewise, the swift adoption of facial recognition technology has sparked widespread fears about personal privacy and constant surveillance. However, it is possible to create AI technologies with confidentiality and ethical considerations at their foundation. This requires enhancing transparency in data handling, ensuring accountability, and utilising a diverse and representative dataset in AI training methodologies. Giving users increased control over how their data is gathered and used is crucial. Advancements like federated learning and differential privacy exhibit considerable promise in developing systems that safeguard user data while delivering value.

In today's digital landscape, where significant amounts of personal information are collected during online activities, safeguarding sensitive data has become increasingly vital. While such information is essential for generating insights and innovation, it must be protected to prevent misuse. Privacy fundamentally entails having authority over who can access one's personal information and how it is utilised. It is vital to individual freedom and autonomy, allowing individuals to maintain control over their identities, safeguard their relationships, and shield themselves from fraud, surveillance, or

[4] Sonia Maan and Dr. Ankita Sharma, Protecting Consumer Rights in the Age of Artificial Intelligence: Legal Implications and Challenges in Consumer Protection, Atlantis Press (26 July 2025, 07:33 AM) https://www.atlantis-press.com/proceedings/nseppda-25/126011901

ILE CONSUMER PROTECTION LAW AND REVIEW
VOLUME 3 AND ISSUE 1 OF 2025
APIS -3920-0023 | ISSN - 2583-8024
Published by
Institute of Legal Education
https://iledu.in

manipulation. Upholding privacy also plays a role in the ethical application of AI. Individuals may face unjust repercussions when personal data is abused or subjected to biased algorithmic decision-making. AI systems should be designed with definitive lines of responsibility and must function transparently to mitigate such risks. As AI increasingly integrates into daily life, establishing robust privacy protections is crucial. Empowering individuals with control over their data and employing privacy-oriented technologies can enable AI to serve society effectively while upholding fairness, dignity, and personal rights.[5]

In the current digital landscape, users benefit from various online safety measures while browsing the internet. A fundamental security feature for online transactions is SSL encryption, which protects sensitive information by establishing a secure connection between users and websites. Many individuals tend to trust and favour sites that showcase these security indicators. Another commonly utilised method for enhancing online account safety is two-factor authentication (2FA), which adds a layer of security. This approach confirms a user's identity through two distinct steps, greatly minimising the risk of unauthorised access. Websites also utilise comprehensive security strategies, including firewalls, intrusion detection systems, regular assessments, and strict compliance with national and international data protection regulations. These actions help guarantee that consumer information is handled with care and security.

Artificial intelligence and machine learning are vital in improving digital security. Large e-commerce platforms adopt these technologies to oversee content, detect threats, and remove fraudulent or harmful content, functioning like an invisible security guard. Likewise, financial institutions utilise AI to identify atypical patterns in user behaviour—such as unusual login times or different locations—to thwart fraud, identity theft, and cyberattacks. Solutions like secure payment gateways and anti-phishing tools further reduce the likelihood of data breaches and financial fraud. Besides technological measures, user-generated content, such as reviews and ratings, offers essential insights into seller reliability and product quality. Positive responses frequently bolster consumer trust and influence buying decisions. Trust seals and certifications found on websites further enhance perceptions of reliability and can boost customer conversion rates. Initiatives for education and awareness are equally crucial in fostering a secure digital environment. These campaigns seek to inform users of online dangers and encourage safe practices. Numerous programs have been initiated to elevate cybersecurity awareness, including governmental and non-profit organisations' initiatives. Programs like Cyber Swachhta Kendra, Surakshit Net, Digital India Cyber Awareness Campaign, RBI Kehta Hai, and Think Before You Click exemplify efforts to empower users and cultivate a safer online space. Collectively, these endeavours contribute to protecting consumers and establishing a secure and trustworthy internet experience.[6]

While artificial intelligence offers considerable potential, key challenges must be overcome to guarantee its responsible application enhances rather than undermines consumer protection. A significant issue is the risk of algorithmic bias. As AI systems heavily depend on historical data, there is a possibility that any existing biases within that data could lead to unjust or discriminatory results. For example, if biased data influences its programming, an AI tool to detect fraudulent commercial practices might inadvertently focus on specific businesses or consumer groups. Regulatory frameworks should mandate transparency in AI-driven decision-making to address these risks and ensure that human supervision is incorporated

[5] Navmi Joshi and Dr Monica Kharola, Safeguarding Personal Privacy in the Era of Artificially Intelligent Systems, Academike (26 July 2025, 03:58 P.M.) https://www.lawctopus.com/academike/safeguarding-personal-privacy-in-the-era-of-artificially-intelligent-systems/

[6] Rhythm Sharma, Safeguarding Consumer in the Digital Age: Emerging Challenges and Solutions, Vol 2 Issue 4, JLRJS, 563-571 (2023) https://jlrjs.com/wp-content/uploads/2023/08/59.-Rhythm-Sharma.pdf

into crucial processes. Another urgent concern pertains to data privacy. The functioning of AI in overseeing digital transactions involves collecting and analysing large volumes of consumer data. This raises significant privacy issues, especially regarding potential misuse or overreach in managing personal information. AI systems must adhere to privacy regulations and legal standards to preserve consumer trust and safeguard individuals against inappropriate data exploitation.

The integration of AI technologies into present regulatory frameworks also presents intricate challenges. It necessitates collaboration among technology developers, government bodies, and industry stakeholders. Current legal frameworks must be revised to accommodate technological advancements while upholding consumer rights. This endeavour calls for technological innovation and harmonising policy and enforcement procedures across national and international spheres. Achieving a balance between innovation and regulation is equally essential. Although AI has the potential to improve regulatory functions significantly, overly stringent regulations could inadvertently stifle market competitiveness and impede technological progress. Policymakers must foster an environment that protects consumer interests while encouraging innovation and economic development. Promising instances of AI use in consumer protection are already emerging. Some e-commerce platforms have implemented automated systems that monitor transactions in real-time, detecting irregularities such as unexpected increases in returns or sudden price changes. These tools assist in identifying fraudulent activities early, although they are not yet widely adopted.

Initiatives aimed at enhancing algorithmic transparency are also in progress. Experimental projects that assess AI decision-making have demonstrated promise in clarifying the basis for product recommendations or price determinations. These initiatives strengthen regulatory oversight and empower consumers by increasing their awareness of digital operations. Moreover, expanding international collaboration in data sharing and regulatory practices has allowed more effective utilisation of AI tools across borders. New frameworks facilitating real-time information exchange between global enforcement agencies establish the foundations for more coordinated approaches to international consumer protection challenges. The prospective integration of AI into consumer protection strategies holds significant transformative potential. However, realising this vision will necessitate ongoing investment in AI research and the creation of global standards for accountability and ethical utilisation. Governments, industry players, and technology developers must collaborate to ensure that AI systems operate in the public interest while functioning transparently and fairly.[7]

Digital Market

The digital marketplace has experienced substantial changes in recent years, making it increasingly crucial for consumers to have trust in this evolving and interactive environment. The online space has become a significant centre for trade and commerce. E-commerce, which encompasses the online buying and selling of products and services, has grown in parallel with worldwide improvements in internet access. Online consumers enjoy numerous advantages, such as a broader selection of options, convenient delivery methods, and competitive prices. Online commerce now goes beyond just retail, encompassing services like e-banking and digital payments, allowing consumers to perform transactions from the comfort of their homes, facilitated by widespread internet access. However, the online marketplace continues to carry inherent risks due to uncertainties in the legal frameworks regulating these transactions. A primary challenge is the disorganisation among online

[7] D Amrish Shiyamily, Consumer Protection in the Digital Marketplace: Addressing Deceptive Practices and Leveraging Emerging Technologies, Vol 5 Issue 3, IJIRL, 182-195 (2025) https://ijirl.com/wp-content/uploads/2025/03/CONSUMER-PROTECTION-IN-THE-DIGITAL-MARKETPLACE-ADDRESSING-DECEPTIVE-PRACTICES-AND-LEVERAGING-EMERGING-TECHNOLOGIES.pdf

consumers. A significant concern is the lack of sufficient legal protections for consumers engaged in digital transactions, an extensive domain often neglected by current laws. Thus, it is vital to enhance the comprehension and development of regulations regarding e-commerce and consumer rights. Typical problems encountered by consumers online include data privacy breaches, identity theft, and receiving products that do not correspond with their online representations. Frequently, consumers find themselves without adequate recourse because of jurisdictional complexities and deficiencies in digital regulation. Creating strong legislation in this field is challenging, particularly in developing countries like India, where there is apprehension that implementing strict consumer protection laws could hinder the growth of the digital economy if done too quickly.[8]

The digital environment has opened up new avenues for fraudulent activities to thrive, particularly through mass emails and misleading websites. Deceptive marketing strategies are frequently camouflaged as authentic offers and may utilise various forms of communication beyond internet channels. For instance, an email or website could present a contact number or address to lend credibility and win over the consumer's trust. The likelihood of fraud increases when transactions occur online, where authentication is limited, and oversight is often lacking. One prevalent instance is pyramid schemes, where individuals pay to participate in a system that claims to generate income through recruitment instead of product sales. Such schemes typically collapse, leading to significant financial losses for most participants. Some schemes operate as Ponzi schemes, utilising funds from newcomers to provide returns to earlier members, thus creating a false appearance of profitability. Chain letters are another type of fraud. These communications often guarantee considerable returns if recipients send small amounts of money to people listed in the letter and then add their names to the list. Despite their straightforward nature, they exploit people's aspirations for easy profits.

The internet is also utilised to advertise false business opportunities. These can include promotions for credit repair services, work-from-home positions, online franchises, or shopping schemes. Dishonest credit repair services falsely assert their ability to eliminate accurate negative information from credit reports, deceiving consumers with pledges that are not legally possible. A common form of scam involves purported "magical remedies" for health issues like AIDS, hair loss, skin conditions, or mental health challenges. These unverified products and claims target vulnerable consumers in search of quick fixes. Some consumers are taken in by online vendors who accept payments for goods or services that are never delivered. In these instances, buyers are left with no recourse. For example, there have been significant cases where online platforms took advance payments but failed to deliver the promised products. Additionally, there are frequent grievances regarding items that do not correspond to their online representations, are of subpar quality, or are packaged without the legally mandated information, such as price, weight, manufacture date, or producer's contact details. These packaging issues have led to legal action against major e-commerce companies for breaching consumer packaging regulations. Moreover, some platforms impose stringent return policies, requiring issue reporting within 48 hours, making it challenging for consumers to find remedies. These unjust terms frequently leave consumers with little to no opportunity for recourse.

Online investment scams are also widespread, featuring inflated claims about high returns in endeavours ranging from securities and commodities to unconventional businesses like livestock breeding or offshore drilling. Misleading information is often disseminated through forums, newsletters, or chat rooms to

[8] Swathy Nair & Swetha Nair, Applicability of Consumer Protection Laws in Online Transactions, iPleaders (26 July 2025, 04:01 PM) https://blog.ipleaders.in/consumer-protection-laws/

ILE CONSUMER PROTECTION LAW AND REVIEW
VOLUME 3 AND ISSUE 1 OF 2025
APIS -3920-0023 | ISSN - 2583-8024
Published by
Institute of Legal Education
https://iledu.in

boost interest and inflate prices artificially. Once prices escalate, fraudsters profit by selling their shares, leaving others with worthless investments. Other fraudulent activities include selling unregistered securities, orchestrating illicit investment schemes, and delivering unauthorised or misleading financial guidance. Another deceptive practice is spoofing, where criminals create fake websites with names similar to legitimate businesses. These sites showcase popular products but are intended to deceive consumers into purchasing from impostors. The nature of the internet facilitates such fraud, as domain names can be registered with minimal verification.[9]

Spamming constitutes a pervasive issue within the digital landscape. It entails the distribution of bulk unsolicited electronic correspondence or irrelevant promotional content within online discussion platforms. Although not intrinsically illegal, spam is frequently utilised to disseminate fraudulent propositions. Typical instances encompass unsolicited communications that purport to offer rapid loans, credit cards, complimentary insurance consultations, retail discounts, or stock trading recommendations. Although these communications may ostensibly appear beneficial, they often function to obfuscate or manipulate consumer decision-making processes. Misleading advertisements represent another prevalent strategy, wherein assurances of complimentary offers on initial purchases or reductions on services entice consumers. Nevertheless, after the completion of a transaction, consumers may realise that the promotion did not apply to their selected product or service. This form of deceptive marketing erodes consumer confidence and frequently precipitates disputes. As the domain of online commerce continues to expand, misleading marketing practices are anticipated to proliferate concomitantly. Annual consumer losses attributable to online fraud amount to billions of dollars. Merchants are not immune to these consequences, particularly when credit card fraud results in chargebacks for unauthorised transactions without physical validation. Deceptive marketing practices can vary from outright fraud to negligent misrepresentation, wherein a seller intentionally disseminates erroneous or misleading information, thereby purposefully deceiving the consumer regarding a product or service.

Data Privacy in India

To safeguard democratic rights and individual liberties, it is crucial to strengthen our data privacy laws. As society progresses, our comprehension and interpretation of privacy also advances. Historically, privacy has been understood as an individual's right to live free from unnecessary intrusion or disturbance by others. When the Indian Constitution was initially adopted, the concept of privacy was not explicitly included in its language. However, discussions around this topic evolved in the following years. In the pivotal 1954 case of M.P. Sharma v. Satish Chandra, the Supreme Court examined whether privacy could be recognised as a fundamental right. The majority opinion from the eight-judge panel determined that it was not.[10] A few years later, in Kharak Singh v. State of Uttar Pradesh (1962), the Court connected personal liberty and privacy, suggesting a more expansive interpretation of the Constitution.[11]

In today's digital environment, individuals frequently reveal personal information without realising it while using various online platforms. Numerous mobile applications possess privacy policies that users seldom read. These services typically gather personal and professional information without explicit consent, which can be exploited for targeted marketing, unwanted communication, or even more severe misuse. In numerous instances, user data is treated as a valuable asset. For example, websites commonly request users to accept cookies that

[9] Amit Dwivedi, Consumer Privacy and Government Technology Mandates in Digital Media Marketplace, iPleaders (26 July 2025, 04:10 PM) https://blog.ipleaders.in/consumer-privacy-and-government-technology-mandates-in-digital-media-marketplace/

[10] AIR 1954 SUPREME COURT 300
[11] AIR 1963 SUPREME COURT 1295

can lead to the monitoring of their online activities. After searching for a flight or a product, it is typical to encounter related advertisements on multiple platforms due to this data collection.

One of the most crucial judgments on privacy occurred in the Justice K.S. Puttaswamy (Retd.) v. Union of India case in 2017.[12] In this case, the Supreme Court affirmed that the right to privacy is a fundamental right under Article 21 of the Constitution, highlighting the importance of self-determination over one's personal information, including its collection, storage, and distribution.[13] Earlier rulings, such as People's Union for Civil Liberties v. Union of India (1996)[14] and R. Rajagopal v. State of Tamil Nadu (1994),[15] recognised privacy as a constitutional right. This perspective was further bolstered by cases like Ram Jethmalani v. Union of India (2011)[16] and the Maneka Gandhi case (1978),[17] reinforcing the privacy's association with Article 21.

Indian judiciary has been establishing the foundation for privacy rights long before they attracted widespread public notice, interpreting these rights as inherent to the larger framework of Articles 19[18] and 21. Individuals may pursue legal remedies for infringements of these rights under Article 32[19] by approaching the Supreme Court or via writ petitions in High Courts under Article 226.[20]

Laws Concerning Consumer Protection in the Digital Market and E Commerce

E-commerce, which stands for electronic commerce, entails purchasing and selling goods and services via digital platforms or the internet. It depends significantly on the World Wide Web as a crucial element in conducting transactions. Besides websites, other resources that aid e-commerce include email systems for communication, online banking services for payments, digital delivery solutions, and security measures for data protection. The changing workforce dynamics and global lifestyle shifts have greatly influenced the swift expansion of e-commerce, a trend anticipated to continue growing.

E-commerce mainly functions in three primary domains. The first domain is online retailing, where companies sell products directly to consumers through virtual stores. The second domain consists of electronic markets, where buyers and sellers conduct transactions through online platforms that enable pricing and product comparisons. The third domain encompasses online auctions, where online bidding systems make items and services available to the highest bidder.

Additionally, e-commerce can be categorised into three specific types based on the nature of transactions. The first category is Business-to-Business (B2B), where transactions occur between two business entities, such as a manufacturer and a wholesaler. The second category is Business-to-Consumer (B2C), which involves businesses selling directly to end consumers via websites or applications. The third category is Consumer-to-Consumer (C2C), where individuals market products or services to other individuals through platforms that enable peer-to-peer transactions, like online marketplaces.[21]

Numerous global organisations actively protect consumer rights within the digital economy. Leading these efforts are the Organisation for Economic Co-operation and Development (OECD), the International Chamber of Commerce (ICC), and the International Consumer Protection and Enforcement Network (ICPEN). The OECD has impacted consumer protection in the digital landscape, especially by creating guidelines specifically intended for

[12] 2019 (1) SCC 1
[13] The Constitution of India, 1949, Art 21
[14] 1997 (1) SCC 301
[15] 1994 (6) SCC 632
[16] (2011) 8 SCC 1
[17] Maneka Gandhi v. Union of India, 1978 AIR 597
[18] The Constitution of India, 1949, Art 19
[19] The Constitution of India, 1949, Art 32
[20] The Constitution of India, 1949, Art 226

[21] Palash Mahobiya, Consumer's Rights in Digital Era, Vol 3 Issue 3, IJLMH, 559 – 566 (2020) https://ijlmh.com/wp-content/uploads/Consumer%E2%80%99s-Rights-in-Digital-Era.pdf

e-commerce. These guidelines, developed through extensive discussions, have benefitted governments, consumers, and businesses. They are crafted to be flexible in response to advancing technologies and market conditions, establishing universal standards for online consumer protection while avoiding restrictive trade practices. Core principles include ensuring that consumers enjoy the same protection levels when shopping online as they do offline. Comprehensive disclosure regarding products and services is vital so consumers can make informed decisions before purchase. The order confirmation process should allow buyers to review and potentially cancel their orders if needed. Additionally, payment systems must be secure and dependable. For international transactions, where legal recourse may be difficult, the OECD advocates alternative dispute resolution methods to help resolve conflicts. The International Chamber of Commerce (ICC) also significantly impacted online commerce regulation by releasing its "Guidelines on Advertising and Marketing on the Internet" in 1996. These guidelines extend to all promotional activities carried out online, encompassing advertising and marketing. The ICC aims to bolster public trust in digital marketing, uphold advertisers' freedom of expression, lessen the necessity for government-imposed regulations, and ensure that consumer privacy expectations are honoured.

The International Consumer Protection and Enforcement Network (ICPEN) is another crucial organisation dedicated to consumer rights on a global scale. Its objective is to defend consumers worldwide by promoting the exchange of enforcement information across borders and fostering collaboration among international regulatory agencies. The Okinawa Charter on the Global Information Society, an initiative that aligns with ICPEN's objectives, tackles essential matters such as digital inclusion, equal involvement in the global digital economy, and the responsible utilisation of digital technologies. Widely accepted principles have been established to promote ethical business conduct in e-commerce. Consumers should have access to transparent, effective, and affordable protection systems, with cooperation between governments and stakeholders aimed at this objective. Businesses must refrain from deceptive practices or actions that violate consumer rights and disclose essential terms and conditions that may affect purchasing choices. If contracts contain penalties for consumers, these should be fair and proportional to the actual damage incurred. Moreover, companies should not obstruct consumers from publishing negative reviews, contesting charges, or filing complaints with appropriate authorities. All marketing and advertising initiatives must be distinctly marked as such, and pricing should be transparent without hidden fees. Payment terms must be communicated clearly to ensure consumers provide informed consent before completing transactions. Additionally, businesses should enable consumers to keep records of their purchases for future reference. Finally, companies are expected to effectively manage cybersecurity threats and implement strong protective measures to ensure the safety of consumers and their data in the e-commerce landscape.[22]

The Information Technology Act of 2000, established by the Indian Government, provides a thorough legal structure for managing electronic transactions, cybersecurity, and digital interactions. Its main objective is to validate electronic transactions legally, thereby promoting e-commerce, e-governance, and various digital activities. The Act is in harmony with global standards, especially those of the United Nations Model Law on Electronic Commerce and guidelines from UNCITRAL (the United Nations Commission on International Trade Law). A central aspect of the Act is its acknowledgement of digital signatures as equivalent to traditional handwritten signatures, legitimising and authenticating electronic

[22] Subhalagna Choudhury, Consumer Protection in E-Commerce, iPleaders (26 July 2025, 10:06 P.M.) https://blog.ipleaders.in/consumer-protection-e-commerce/

documents. The Act also tackles numerous types of cybercrime, outlining penalties for unauthorised computer access, hacking, identity fraud, and malware distribution. To manage the execution of digital signatures, the Act created the Controller of Certifying Authorities (CCA) role, which oversees the functioning of Certifying Authorities (CAs). These CAs are responsible for issuing digital certificates that confirm the identities of individuals or organisations involved in online transactions. The Act defines and prescribes penalties for cyber offences, including data protection violations, breaches of privacy, and cyber terrorism. It establishes jurisdiction and legal processes for addressing cybercrimes within India or involving Indian computer systems abroad.

The Information Technology Act of 2000 has been vital in fostering trust and reliability in the digital space. It has contributed to expanding electronic commerce and digital participation while tackling the legal and security issues that emerge online. One significant challenge in protecting consumer rights in the sharing economy is the lack of uniform regulatory standards. This sector spans multiple industries and platforms, utilising distinct business models and practices. Such variation results in inconsistent consumer protection measures, with different regions or countries frequently enforcing diverging or contradictory regulations. This disjointed framework poses challenges in applying standardised protections for consumers. Another critical issue is the vagueness concerning responsibility and accountability. In the sharing economy, traditional roles can become indistinct, complicating the determination of liability when disputes occur or consumer rights are infringed. Whether the responsibility rests with platform operators, individual service providers, or third parties is often unclear. This ambiguity can complicate legal recourse and discourage consumers from fully participating in the sharing economy.

Concerns regarding data privacy and security also pose considerable risks. Consumers must typically provide sensitive personal information when engaging with sharing platforms. The methods employed for collecting, storing, and potentially distributing this data raise concerns about breaches and misuse. These apprehensions highlight the necessity for stringent data protection policies and strong cybersecurity initiatives to ensure user information is managed securely and transparently. Another hurdle in this sector is the resolution of disputes. Issues related to payments, service quality, or contract conditions may frequently occur; however, often there are no established or consistent systems for resolving disputes. Without fair, accessible, and efficient mechanisms, consumers could encounter delays or prejudiced outcomes, undermining their trust in the system. Tackling these challenges is essential for creating an equitable and trustworthy environment within the sharing economy. This effort calls for coordinated action from policymakers, platform providers, and other stakeholders to develop harmonised regulations, establish clear accountability frameworks, strengthen privacy protections, and create effective dispute resolution systems. These measures are crucial for safeguarding consumers and ensuring the sustainable development of the sharing economy.[23]

The Information Technology Act 2000 was amended in 2008, offering a thorough legal structure for electronic commerce. This Act mainly regulates transactions between the government, its departments, and citizens, to support e-governance. It establishes methods for the authentication of electronic records via digital signatures, thus facilitating daily official activities such as submitting and examining documents in digital formats. The IT Act marks a significant advancement in the government's

[23] Yash Raj, Consumer Protection in the Digital Age: Analysing Legal Frameworks Safeguarding Consumers in the Sharing Economy, The Amikus Qraie (26 July 2025, 10:34 P.M.) https://theamikusqriae.com/consumer-protection-in-the-digital-age-analyzing-legal-frameworks-safeguarding-consumers-in-the-sharing-economy/

ILE CONSUMER PROTECTION LAW AND REVIEW
VOLUME 3 AND ISSUE 1 OF 2025
APIS -3920-0023 | ISSN - 2583-8024
Published by
Institute of Legal Education
https://iledu.in

endeavour to digitise its operations, ensuring that information is easily accessible online and that these digital exchanges are secure. It also outlines remedial measures, including appointing a Controller and creating a Cyber Regulations Appellate Tribunal to handle cyber offences specified in Sections 43 to 47 of the Act.[24] A key aspect of this legislation is its recognition of electronic records as legally valid. Furthermore, it amends other laws, such as the Indian Evidence Act, Indian Penal Code (now Bharatiya Nyaya Sanhita 2023), Bankers' Books Evidence Act, and Indian Stamp Act, to make them compatible with digital documentation and transactions. This legal validation is fundamental to e-commerce activities and plays a role in enforcing consumer rights when they are violated. Nevertheless, the Act does not thoroughly cover all aspects of e-commerce from the standpoint of consumer rights. Its primary focus is business-to-government transactions and the procedural requirements for recording, managing, and securing electronic documents using digital signatures and cryptographic technologies. Conversely, the typical consumer engages with e-commerce through activities like online shopping, digital banking, and electronic fund transfers, areas that the Act does not explicitly address. Although it aims to promote digital financial activities among banks and financial institutions, the legislation lacks distinct provisions to protect consumer rights in these everyday digital interactions. Thus, an essential facet of e-commerce remains inadequately addressed by the existing legal framework.

The Consumer Protection Act, 2019, marks a significant legislative advancement in safeguarding consumer rights, especially in the context of the digital economy. One of the notable features of this Act is the broadened definition of a "consumer." Unlike the earlier versions, the 2019 Act explicitly includes individuals who purchase goods or avail services through online platforms. According to the Act, a consumer is defined as any individual who buys goods or avails services for a consideration. This consideration may be paid in full, in part, or promised to be paid in the future.[25] Notably, the definition excludes those who acquire goods or services for resale or commercial purposes. Additionally, the Act clarifies that transactions carried out through digital means, including online platforms, telemarketing, and teleshopping, fall under its purview. As a result, individuals dissatisfied with products ordered via teleshopping or online advertisements have a legal avenue to file complaints under the consumer protection framework. The Act also expands the term "deficiency" scope, strengthening consumer rights. The new definition includes acts of negligence, omissions, or conduct that result in harm, loss, or injury to the consumer.[26] It explicitly states that withholding essential information is now considered a deficiency in service. This is especially relevant in digital commerce, where transparency is often compromised. For instance, if a seller fails to disclose the country of origin of a product, it could significantly influence a consumer's purchasing decision. Suppose a consumer buys an electronic item online without being informed about its origin, only to find later that this information was deliberately withheld. In that case, it constitutes a deficiency under the Act, offering the consumer valid grounds to raise a legal complaint.

Moreover, the Act addresses the evolving nature of commerce by incorporating the concept of "e-commerce." It defines e-commerce as the buying or selling of goods and services, including digital products, through digital or electronic networks.[27] This inclusion underscores the Act's adaptability to modern market practices. It introduces the term "electronic service provider" to individuals or platforms enabling merchants to advertise or sell goods and services online, including marketplaces

[24] The Information Technology Act, 2000, § 43-47

[25] The Consumer Protection Act, 2019, § 2(7)
[26] The Consumer Protection Act, 2019, § 2(11)
[27] The Consumer Protection Act, 2019, § 2(16)

ILE CONSUMER PROTECTION LAW AND REVIEW
VOLUME 3 AND ISSUE 1 OF 2025
APIS -3920-0023 | ISSN - 2583-8024
Published by
Institute of Legal Education
https://iledu.in

and auction websites.[28] With more consumers relying on online platforms for purchases, this legal recognition ensures they have a formal mechanism to address grievances and hold platforms accountable for service deficiencies. Another key provision is the definition of "endorsement" under Section 2(18) of the Act.[29] Endorsement is any verbal, written, visual, or representational communication that conveys a message to consumers through the identity, autograph, likeness, or other identifiable aspects of a person or institution. This provision aims to curb misleading advertising practices, especially those involving celebrity endorsements or reputed organisations. For example, advertisements promising unrealistic outcomes such as extreme weight loss in days, snow-white clothing, or drastic changes in skin tone often feature well-known personalities. The 2019 Act now imposes greater accountability on endorsers, compelling them to verify the authenticity of claims before endorsing a product or service. E-commerce platforms, too, must exercise due diligence in listing and promoting products, as they may also be held liable for deceptive practices.

The Act introduces the "product liability" principle, empowering consumers to file complaints against manufacturers, service providers, and sellers, including those operating via e-commerce platforms.[30] This principle ensures that responsibility can be affixed throughout the supply chain for defective goods or deficient services. Product liability is especially critical in online commerce, where consumers cannot physically examine products before purchase. Discrepancies between advertised and delivered products, such as differences in size, texture, or colour, can lead to legal claims.[31] For instance, a consumer who orders a chandelier online based on specific dimensions may receive a much smaller item due to incorrect measurements on the website. In such cases, the manufacturer and the platform can be held accountable for delivering a substandard product. To combat deceptive marketing, the 2019 Act includes explicit provisions on misleading advertisements. It defines a misleading advertisement as one that falsely represents the nature, quality, quantity, or efficacy of a product or service, thus misleading consumers.[32] If such misrepresentations are made by manufacturers, sellers, or service providers, they are considered unfair trade practices. The Act penalises those responsible for such misleading content, pushing companies to be more careful and truthful in their marketing strategies. As a result, consumers are better protected against exaggerated or dishonest claims in advertising across media platforms.

Another transformative feature of the Act is the establishment of the Central Consumer Protection Authority (CCPA). The CCPA is a central regulatory body dedicated to collectively protecting consumer rights. It is empowered to address violations that impact public interest, enforce consumer rights, and investigate unfair trade practices. The Central Government is responsible for establishing the CCPA, including an investigative wing led by a Director-General. This division is accountable for probes based on directives issued under the Act. The CCPA is also authorised to ensure transparency on e-commerce platforms. For example, it can mandate that online marketplaces display the country of origin for all listed products. In the event of non-compliance, it may direct platforms to implement visible and accessible grievance redressal mechanisms, including publicly displaying contact details of responsible officers. In addition to traditional legal remedies, the 2019 Act introduces the concept of "mediation" as an alternative dispute resolution mechanism.[33] This provision aims to streamline the dispute resolution process by allowing parties to resolve their issues amicably and efficiently without litigation. However, the Act outlines exceptions to mediation in severe

[28] The Consumer Protection Act, 2019, § 2(17)
[29] The Consumer Protection Act, 2019, § 2(18)
[30] The Consumer Protection Act, 2019, § 2(34)
[31] The Consumer Protection Act, 2019, § 83
[32] The Consumer Protection Act, 2019, § 2(28)
[33] The Consumer Protection Act, 2019, § 2(25)

cases, such as those involving widespread harm or fatal medical negligence.[34] Given the growing number of consumers engaging in online transactions, mediation presents an accessible, cost-effective, and time-saving method for resolving complaints. It offers a pragmatic approach to justice that benefits consumers across socio-economic backgrounds.

Under the Consumer Protection Act, 2019, significant procedural reforms have been introduced to enhance consumer access to justice and ensure a fair appellate mechanism. One such change pertains to the time limit for filing appeals against the decisions of the District Consumer Disputes Redressal Commission. Suppose an individual is dissatisfied with a verdict delivered by the District Commission and wishes to challenge the decision. In that case, the Act now allows an extended period of **45 days**, as opposed to the earlier **30-day** timeframe, to approach the State Consumer Disputes Redressal Commission. This extension gives consumers a more reasonable window to prepare their case and seek appropriate legal recourse.

Additionally, the Act empowers both the State and National Commissions to scrutinise and strike down contractual terms that are found to be unfair or prejudicial to the interests of consumers. Section 49(2) of the 2019 Act vests the State Commission's authority to declare specific contractual terms unjust or oppressive to consumers.[35] Similarly, Section 59(2) grants the National Commission equivalent powers to assess and nullify unfair contractual clauses.[36] These provisions prevent businesses from exploiting consumers through fine print or one-sided agreements, especially in digital and service-based transactions where terms and conditions are often non-negotiable.

Furthermore, in matters related to the rights of persons with disabilities, the Act provides the scope to escalate appeals to the National Commission on Disability Rights and Rehabilitation (NCDRR), if necessary. This provision ensures that vulnerable consumer groups receive adequate attention and a dedicated forum to address grievances related to their specific needs. Lastly, Section 71 of the Act equips the consumer commissions with execution powers under Order XXI of the Civil Procedure Code (CPC), 1908.[37] These powers enable consumer forums to enforce their orders effectively, like the procedures followed in civil courts. However, executing such powers remains subject to the conditions and limitations prescribed within the section, ensuring due process is observed.[38]

The Consumer Protection (E-Commerce) Rules, 2020, were established to safeguard consumer rights in the swiftly expanding digital marketplace. These rules are not mere optional guidelines but legal requirements that e-commerce platforms must adhere to. Their objective is to foster a transparent and reliable environment for online transactions, striking a balance between the needs of consumers and sellers, including intermediaries involved in e-commerce. Per the rules, every e-commerce platform, whether it follows a marketplace or inventory-based model, must provide consumers with comprehensive and transparent information. This encompasses the terms and conditions regarding the return, refund, and exchange of goods or services. Consumers must also be made aware of the warranty or guarantee associated with the product, the anticipated delivery timeframe, available payment options, safety measures in place for secure transactions, the process for addressing payment failures or defaults, and the product's country of origin.

Moreover, when a consumer submits a complaint about a product or service acquired

[34] The Consumer Protection Act, 2019, § 75
[35] The Consumer Protection Act, 2019, § 49(2)
[36] The Consumer Protection Act, 2019, § 59(2)

[37] The Consumer Protection Act, 2019, § 71, read with Code of Civil Procedure, 1908, O 21
[38] Amita and Dr Harvinder, The role of the Consumer Protection Act 2019 in addressing E-commerce challenges and consumer grievances in the digital age, Vol 7 Issue 1, IJLPSR, 87-91 (2025) https://www.lawjournals.net/assets/archives/2025/vol7issue1/7019.pdf

through an e-commerce platform, the platform must acknowledge the complaint within 48 hours. The resolution of the grievance must occur within 30 days from the date of receipt. To facilitate the redressal process, each e-commerce platform must designate a specific grievance redressal officer responsible for managing consumer complaints. In cases where a product received by the consumer is defective, damaged, delayed, or markedly different from its description online, the consumer has the right to initiate a return or request a refund. The seller cannot refuse to accept the return of such items, deny the provision of services, or unreasonably delay the refund process. Additionally, the rules explicitly forbid e-commerce companies from altering the prices of goods or services to make excessive profits. Such practices are considered illegal, and platforms that violate these provisions may face legal repercussions.[39]

Conclusion & Recommendations

Consumer protection has always been a critical issue across different eras. Even in ancient and medieval times, efforts were made to safeguard consumers from exploitation and fraudulent practices in the marketplace. Several pieces of legislation were introduced during the British colonial era to protect consumer interests. However, over time, inefficiencies and systemic flaws crept into the enforcement mechanisms, leading to a decline in consumer confidence and discouraging them from seeking legal remedies. Despite these setbacks, the government has consistently played a significant role in upholding consumer rights. Implementing the Consumer Protection Act has notably improved consumer protection, making legal recourse more affordable and accessible. Nonetheless, the responsibility does not lie solely with the state. Consumers must also become more informed, proactive, and alert to unfair trade practices to safeguard their interests effectively.

In today's digital age, rapid technological advancement is transforming how commerce is conducted. As Charles Clark aptly noted, "the answer to the machine is in the machine." This idea is reflected in the rise of e-commerce, which has revolutionised the traditional marketplace. However, an assessment of the current legal framework reveals that it has not evolved sufficiently to meet the unique challenges of online trade. One significant limitation of the Consumer Protection Act is its exclusion of services provided free of cost, which means that certain online transactions remain outside the law's protective umbrella. This gap leaves consumers vulnerable when digital services are offered without a direct charge. Although India has taken steps toward adapting its consumer laws to the digital environment, much more must be done to ensure comprehensive protection for e-commerce users. The journey has begun, but a considerable distance remains to cover.[40]

Revising current laws and regulations to reflect new technologies and changing business practices is crucial to improving consumer protection in today's digital world. Legislation should be consistently evaluated and updated to match advancements such as artificial intelligence (AI), the Internet of Things (IoT), and the sharing economy. A legal framework that is flexible and based on principles should be implemented to adapt to technological changes while preserving fundamental consumer rights. Standards that guarantee algorithms' transparency, fairness, and accountability must be established, particularly in pricing, credit scoring, and targeted advertising. Comprehensive data protection laws should also address privacy, portability, and ethical data usage. Collaboration among policymakers, industry players, and consumer advocates is vital to ensure that reforms are practical, supportive of innovation, and centred around consumer needs.

[39] Hariom Gupta and Amit Singh, Digital consumer rights: Navigating the challenges of e-commerce in India, Vol 4 Issue 2, IJCLLR, 127-133 (2024) https://www.civillawjournal.com/article/99/4-2-23-503.pdf

[40] Grishma Kanth and R Siva Rama Prasad, Consumer Protection in Digital World, Vol 8 Issue 12, JETIR, 492-499 (2021) https://www.jetir.org/papers/JETIR2112359.pdf

Equally key is the empowerment of consumers through education and awareness initiatives. National campaigns should aim to inform consumers about their rights, responsibilities, and available resources in the digital realm. Custom educational programs should cater to various age groups, backgrounds, and levels of digital literacy to ensure inclusivity. Collaborations with schools, community organisations, and media outlets can facilitate disseminating information about online safety, privacy, and fraud prevention. Digital businesses should be encouraged to present clear and transparent details concerning their products, services, and consumer policies, enabling customers to make informed choices. Moreover, consumers should be provided with practical guidance on understanding terms and conditions and confidently assert their rights.

On an international scale, cooperation across borders can significantly contribute to standardising consumer protection measures. Strengthening global initiatives like the UN Guidelines for Consumer Protection and the OECD can help establish common standards among countries. Multilateral agreements could create baseline protection measures for cross-border e-commerce, addressing jurisdiction, enforcement, and data privacy issues. Regional agreements, similar to those in the European Union, could encourage legal consistency among neighbouring countries. Finally, improving cross-border collaboration, dispute resolution methods, and sharing best practices among consumer protection agencies would ensure a more coherent and effective global consumer protection system.[41]

[41] Madhuri Mittal, Consumer Right in the Digital Marketplace: A Comparative Analysis, Vol 2 Issue 16, WBLILI, 1-20 (2024) https://www.whiteblacklegal.co.in/details/%E2%80%9Cconsumer-right-in-the-digital-marketplace-a-comparative-analysis%E2%80%9D-by---madhuri-mittal