SAFEGUARDING CONSUMERS IN THE DIGITAL AGE: EMERGING CHALLENGES AND SOLUTIONS

Rhythm Sharma*

ABSTRACT

Digital technology has revolutionized consumer interaction, offering numerous advantages and opportunities worldwide. However, it has also created new challenges for online consumers, including data privacy breaches, deceptive advertising, phishing attacks, and counterfeit goods. As part of the article, the existing legislative frameworks in India, including the Consumer Protection Act, E-commerce Guidelines, and Information Technology Act, are discussed, with international initiatives like GPEN, ICPEN, and OECD guidelines emphasizing the need for international cooperation in addressing consumer protection issues, aimed at protecting consumers in the digital space. Besides highlighting the need for education and dispute-resolution mechanisms, the conclusion emphasizes the importance of collaboration, innovation, and robust regulatory frameworks for online safety.

INTRODUCTION

From online shopping to social media platforms, the digital landscape provides countless conveniences and opportunities for consumers throughout the world. The global number of digital buyers in 2021 was 2.14 billion, and in India, there were 450 million e-commerce users. By 2025, there will be 2.41 billion digital buyers worldwide, an all-time high, due to the advantages and convenience of the digital landscape. India and other countries have a growing number of internet users and smartphones, suggesting that digital commerce will flourish shortly. There were almost 624 million internet users in India in 2022, the second-highest number in the world after China. In addition, nearly 820 million Indians owned smartphones in 2021, also making it the second-largest smartphone market. While technological advancements have created new opportunities, they have also caused new challenges in the process as well. The annual cost of cybercrime worldwide has been on the rise as n 2020, cybercrime was estimated to cost the global economy over $1 trillion, as reported by Cybersecurity Ventures. These costs include financial losses, data theft, and expenses related to cybersecurity measures. This Article dives into the issues of online fraud

*ALIGARH MUSLIM UNIVERSITY.

and scams, examines the legislative frameworks in existence, and emphasises the need for cooperation and consumer awareness in safeguarding users in the digital environment.

KINDS OF CHALLENGES FACED BY ONLINE CONSUMERS In the annual report 2020-21, 24% of complaints the National Consumer Helpline received were related to e-commerce, indicating the issues consumers face when shopping online. Understanding these issues is crucial to effectively resolve them.

Data Privacy and Security: During online transactions, consumers often share personal information, including financial details, resulting in identity theft or unauthorized access to sensitive information or any other injurious use, causing concerns surrounding consumer privacy and security. Over 6.95 million records were compromised in 2020, according to the Data Security Council of India (DSCI). Supreme Court in *R Rajagopal v. State of Tamil Nadu (1994),*[1] while giving a wider interpretation of the Article 21 recognized the right to privacy within the ambit of the right to life and personal liberty thus highlighting the need for consumer protection in this digital era.

Deceptive Advertising and Product Information: Consumers may face misleading or deceptive advertising practices, such as exaggerated product claims, false discounts, or manipulated reviews, which can result in wrong purchasing decisions. In 2020, ASCI received 10,773 complaints about misleading advertisements, including those online. This problem is made worse when consumers are bombarded by multiple ads online. In addition, the Advertising Standards Council of India (ASCI) has taken action against Fair & Lovely for perpetuating stereotypes, Dettol for promising "100 times better protection" without substantiation, and Horlicks for misleading claims about growing taller. Due to misleading ingredient claims, Maggi noodles ads were withdrawn.

Phishing is a type of cybercrime in which scammers try to trick you into giving them personal information, such as your passwords, credit card numbers, or Social Security numbers by sending emails that looks like it's from a legitimate company or by setting up a fake website that looks like a legitimate website. Over 220,000 unique phishing websites were detected by the Anti-Phishing Working Group (APWG) in the first quarter of 2021, demonstrating the threat phishing attacks pose.[2] State Bank of India (SBI) customers were

[1] R Rajagopal v. State of Tamil Nadu (1994),1995 AIR 264, 1994 SCC (6) 632
[2]<https://apwg.org/trendsreports/>accessed 20 July 2023

targeted in 2020 in a scam known as the SBI Phishing Scam. In the message, recipients were asked to update their account information by clicking a link and entering their login information, which allowed the scammers to access their accounts and steal money.

Online Auction and Marketplace Fraud: The Consumer Complaints received by the Department of Consumer Affairs in India highlight the grievances associated with online shopping, with 19,990 complaints registered related to online transactions in 2020-21, including non-delivery, defective product delivery, and refund issues[3]. Fraudulent sellers misrepresent products or fail to deliver them after receiving payment. The "Snapdeal Fraud" case involved several instances where buyers purchased electronic products from Snapdeal, an Indian e-commerce platform, but received counterfeit or fake items. One such incident involved a customer, who ordered a branded smartphone from a seller on Snapdeal. When the package arrived, the customer found a counterfeit replica of the smartphone instead of the original product he ordered. The product listing displayed genuine images and specifications, and he made the payment trusting the reputation of the platform. The seller failed to respond to his contact, and Snapdeal's customer support initially provided little assistance. A great amount of frustration and disappointment was felt by the customers after it was revealed that the seller intentionally misrepresented the product.

Counterfeit and pirated products: Online marketplaces are vulnerable to the sale of counterfeits and pirated goods since consumers do not have any prior physical interaction with the products. *The Karnataka High Court held in Amazon Seller Services Pvt Ltd v. Amway India Enterprises Pvt Ltd (2019)*[4] that e-commerce platforms are responsible for counterfeit products sold by third-party sellers on their platforms, emphasizing the responsibility of online marketplaces to ensure the quality of products they sell. The Authentication Solution Providers' Association (ASPA) found that counterfeit products make up 20% of the Indian product market, causing serious financial losses to consumers and legitimate businesses.

Advance Fee Fraud: This type of fraud typically involves tricking victims into paying upfront fees or charges to receive promised goods, services, or financial benefits. Examples include lottery, inheritance, or job scams that require payment before employment. In 2016,

[3] https://consumeraffairs.nic.in/sites/default/files/file-uploads/annualreports/1617263115_AR2020-21.pdfaccesed 20 July23
[4] Amway India Enterprises Pvt. Ltd. &Ors. vs. 1MG Technologies Pvt. Ltd. &Ors., MANU/DE/2146/2019

the "IRCTC Tatkal Ticket Scam" came to light. Fraudsters exploited the Tatkal booking system of the Indian Railways by creating software that would automatically book Tatkal tickets for a fee, bypassing the regular booking process. They charged customers exorbitant fees for the service.

Investment and Financial Fraud: Digital payments are on the rise, but there's not enough awareness about the risks associated with online banking and other digital payment methods. According to the Reserve Bank of India (RBI), there have been 6,801 fraud cases in India in 2019-20, up from 5,076 fraud cases in 2017-18. These include online banking scams, credit card fraud, and unauthorized transactions. This leads to significant losses as in 2019-20, the Reserve Bank of India recorded Rs 1,85,772.42 crore (approximately USD 25.4 billion) lost through financial fraud and investment.[5] Increasing financial fraud rates in India is like watching a snowball roll downhill, growing larger and faster as it goes, and failing to take appropriate measures to protect consumers increases this rate. Nonetheless, the first step has been taken in *Reserve Bank of India v Jayantilal N Mistry (2016)*, which holds consumers not liable for unauthorized credit or debit card transactions unless they are negligent, so the burden of proof has been transferred to the banks. Investment advisors can target consumers directly by promising high returns or exclusive opportunities, and by promoting fraudulent investment schemes (Ponzis or multilevel marketing). As an example, SpeakAsia Online, a high-profile scam, promised high returns for completing surveys and referring others but instead turned out to be a Ponzi scheme that defrauded thousands of investors. Moreover, this type of crime is not uncommon, as the National Crime Records Bureau (NCRB) of India reports that in the first quarter of 2019, there were 44,546 reports of cybercrime, including 11,587 cases involving financial fraud.[6]

Online Ticketing Scams: Scammers offer fake or counterfeit tickets for popular events, concerts, or sports games, which consumers buy unknowingly, only to discover they are invalid. Similar to "BookMyShow Fraud," scammers created fake websites that looked like the popular online ticketing platform BookMyShow and sold fake tickets to victims.

[5] ChethanKumar,India loses Rs 100 crore to banking fraud every day (Times of India, 29 March 2022) <https://timesofindia.indiatimes.com/business/india-business/india-loses-rs-100-crore-to-banking-fraud-every-day/articleshow/90509071.cms>accesed 20 June 23

[6] Bharti Jain, 'NCRB Crime Data 2019: Cases registered up 1.6%; crimes against women rise 7.3%, cybercrimes jump 65.3%' (Times of India, 30 Sep 2020) <http://timesofindia.indiatimes.com/articleshow/78394087.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst>accessed 18 July 2023

Tech Support Scams: Tech support scams are prevalent in India, in which scammers impersonate support personnel from well-known companies such as Microsoft or Dell to contact individuals. They claim that their computers are infected with malware or technical problems, then convince victims to provide remote access or pay for unnecessary services or software.

THE LEGAL MEASURES FOR PROTECTING CONSUMERS ONLINE

Consumer Protection Act, 2019 is the primary legislative body providing a comprehensive framework for consumer protection, encompassing both offline and online transactions. It sets out consumer rights and responsibilities, regulates consumer dispute resolution, and holds manufacturers, sellers, and service providers accountable for defective products.

The Ministry of Consumer Affairs, Food and Public Distribution issued the E-commerce Guidelines in 2020, specifically addressing consumer protection issues in online transactions. These guidelines mandate e-commerce platforms adopt transparent and fair business practices, disclose relevant information about products and sellers, and establish mechanisms for grievance redressal.

The Information Technology Act 2000 (IT Act)deals with electronic transactions, data protection, and cybersecurity. It has been amended several times to keep up with technological advancement The IT Act also seeks to regulate digital signatures, protect intellectual property, and prevent cybercrime. In addition to protecting consumers from online fraud, identity fraud, and data breaches, the legislation also defines the role and responsibilities of intermediaries, such as e-commerce platforms, in protecting consumers. *Dr. NareshKadyan v State of Haryana (2013)*, the Delhi High Court emphasized that cybercrime constitutes a serious offence under the Information Technology Act of 2000 and that all of these crimes should be fought for the safety and security of online users. The online community needs to be protected from online scams, phishing, identity theft, hacking, data interference, and illegal access to computer systems. Without strong action against these cybercrimes, online users will remain vulnerable and exposed to potential security threats.

The Personal Data Protection Bill, of 2019 was intended to provide enhanced protection for consumers' personal information and establish mechanisms for obtaining consent and resolving data breaches. It was later withdrawn from the Lok Sabha and reports suggested a

more comprehensive version may be introduced. As reported by certain sources, the Government may consider introducing a Digital India Act instead of a Data Protection Bill.

The Advertising Standards Council of India (ASCI) self-regulates advertising content to ensure that advertisements are truthful, and fair, and do not mislead consumers. ASCI's codes and guidelines play a vital role in protecting consumers from false or misleading advertisements, including those in the digital space. ASCI took action against Fair& Lovely ads for perpetuating stereotypes, Dettol's claim of "100 times better protection" without substantiation, and Horlicks' misleading claim about helping children grow taller. Maggi noodles ads were withdrawn due to misleading claims about ingredients. ASCI ensures accurate and non-misleading advertising.

Consumer Dispute Redressal Mechanisms provide for the establishment of consumer dispute redressal commissions at the national, state, and district levels. These commissions serve as quasi-judicial bodies to hear consumer complaints, provide remedies, and impose penalties on erring parties. A lot of dispute resolution platforms, like the National Consumer Helpline, let consumers resolve disputes online.

INTRODUCTION OF NEW DEVELOPMENTS IN THE FIELD OF CONSUMER PROTECTION

As consumers navigate the digital world, they have access to a variety of online consumer protection measures. During transactions, SSL encryption has been used to protect sensitive data, and in a study by GlobalSign, 84% of consumers prefer to shop on sites that have SSL certificates.[7]It has been shown that two-factor authentication enhances security. According to TeleSign, 74 % of consumers consider 2FA to be a reliable and secure method of protecting their online accounts, and Google reported in their study that implementing 2FA resulted in spectacular 99.9% fewer hijacked accounts. A comprehensive security approach is implemented on the website through firewalls, intrusion detection systems, periodic audits, and following the country's data protection regulations to ensure consumer information is handled appropriately. For instance, EU privacy laws, such as the General Data Protection Regulation (GDPR), require companies to gain the consent of consumers and inform them about how their data will be used.

[7] Lea Toms85% of Online Shoppers Avoid Unsecured Websites (Global Sign,19 Nov 2014) <https://www.globalsign.com/en/blog/85-of-online-shoppers-dont-buy-on-unsecured-websites> accessed 19 July23

Amazon, eBay, and Alibaba use AI and machine learning algorithms to detect and remove harmful or fraudulent content It's like having an invisible security guard patrolling the premises. This invisible security guard helps protect these companies from cyber threats and malicious intent, ensuring their customers receive only the highest quality of service. Through artificial intelligence algorithms, banks and financial institutions detect and flag suspicious activity to prevent fraud, money laundering, and cyberattacks. These algorithms act as a watchful eye, detecting suspicious behaviour and alerting authorities when things go wrong. An organisation can also use artificial intelligence to detect suspicious activity by detecting anomalous user behaviour, such as unusual login times or locations. Secure payment gateways and anti-phishing measures minimize the risk of fraud and data breaches. The average cost of a data breach globally increased to $4.35 million in 2022.[8]

Consumer reviews and ratings, as well as trust seals and certifications, assist buyers in making informed decisions about trustworthy sellers, as a study by BrightLocal revealed that 82% of consumers read online reviews before making a purchase, and positive reviews can lead to increased consumer trust in a brand.[9] Additionally, the Baymard Institute found that displaying trust seals and certifications can improve the perceived trustworthiness of websites and boost conversions.

Additionally, education and awareness campaigns inform consumers about online safety, while dispute resolution mechanisms provide recourse for addressing issues that may arise in online transactions. Campaigns aimed at promoting cyber safety encourage people to be aware of security threats, protect them, enable e-commerce to be secure, and promote responsible online behaviour. There have been several such initiatives, including the "Cyber Swachhta Kendra" of the Indian government, the "Surakshit Net" and "Digital India Cyber Awareness Campaign" from the Ministry of Electronics and Information Technology (MeitY), RBI Kehta Hai from RBI, and "Think Before You Click" from the Cyber Peace Foundation. These initiatives are important steps to ensure the safety of digital assets and build a secure online environment.

[8]Anastasia Dergacheva, Jesse R. Taylor 'Study Finds Average Cost of Data Breaches Reaches All-Time High in 2022' (Morgan Lewis, 04 Jan 2023)<https://www.morganlewis.com/blogs/sourcingatmorganlewis/2023/01/study-finds-average-cost-of-data-breaches-reaches-all-time-high-in-2022> accessed 19 July 2023

[9] Sammy Paget,LocalCustomerReview Survey2023(BrightLocal, 7Feb2023) <https://www.brightlocal.com/research/local-consumer-review-survey/>accessed 20 July 23

CONSUMER PROTECTION INITIATIVES AT THE GLOBAL LEVEL

By doing annual privacy enforcement surveys and facilitating cross-border collaboration, the **Global Privacy Enforcement Network (GPEN)**[10] and **International Consumer Protection and Enforcement Network (ICPEN)**[11] encourage data cooperation and consumer protection. GPEN and ICPEN provide a means for data protection authorities to share information and coordinate enforcement activities. As a member of GPEN and ICPEN, India contributes to global efforts to strengthen collaboration among data protection authorities. Through signing Memorandums of Understanding (MoU) with various countries, India has strengthened its ties with other countries in the field of data protection and privacy. For example, India signed an MoU with Canada in 2018 to facilitate cross-border data transfers and investigations related to cybercrimes and data protection.

NCTAD's Guidelines for Consumer Protection[12] are another effort to promote a secure and transparent online environment. Member states can implement these guidelines to ensure consumer protection, including e-commerce and digital services. Despite not being legally binding, these guidelines serve as an international standard for consumer protection, and their strength is derived from their adoption by the United Nations General Assembly, and the consensus among countries and experts. As a member of this organization, India is committed to upholding the guidelines and standards set forth and continues to strive to ensure the best level of consumer protection for its citizens.

Additionally, the **Internet Corporation for Assigned Names and Numbers (ICANN)** manages the domain name system and promotes domain name registrant privacy, with whom India has collaborated multiple times. For example, in February 2020, ICANN and India's Ministry of Electronics and Information Technology signed a Memorandum of Understanding to foster collaboration between the two organisations. To develop guidelines for consumer protection in the digital economy, India has also partnered with the **Organisation for Economic Co-operation and Development (OECD).**[13] Further, Indian companies, governments, and consumers have been partnering with international partners to combat cyber threats, such as the **Global Cybersecurity Alliance (GCA),** via initiatives like this. For instance, in 2019, the GCA launched the India-GCA Cybersecurity Cooperation

[10] <https://www.privacyenforcement.net/>accessed 18 July 23
[11] <https://icpen.org/>accessed 18 July 23
[12] <https://unctad.org/>accessed 18 July 23
[13] <https://www.oecd.org/>accessed on 19 July 23

Program to help the Indian government and its citizens tackle cyber threats and strengthen cybersecurity measures.

According to a TrustArc study, over 65% of organizations have already achieved **GDPR compliance** by early 2021, setting a high standard for data protection. The study indicates that businesses are ensuring consumer privacy rights are respected and data protection regulations are followed. While not directly applicable to India, some speculative reports suggest that the GDPR has influenced the creation of the Digital India Act. India's commitment to protecting consumer data and security standards is in line with global standards.

CONCLUSION

Despite all the efforts made and the comprehensive legislation and framework in place, there is still a lot of ground to cover. An effective consumer protection program requires a multifaceted approach, combining legal measures, technological advancements, public awareness campaigns, and collaborative efforts from all stakeholders. This collaborative effort needs to be ongoing and adaptive, as consumer threats change over time. Boosting consumer protection laws, strengthening enforcement mechanisms, promoting education and awareness, and leveraging technology are crucial to making online activities safer. "Digital technologies offer immense opportunities, but they also carry risks," noted Nilekani, co-founder of Infosys and chairman of UIDAI. "Online fraud and scams require the involvement of governments, industry, and civil society, so collaboration, innovation, and strong regulatory frameworks are essential for consumer protection."