REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 2 (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

'Impact Of Data Privacy Regulations On Consumer Trust And E-Commerce Success: A Comparative Analysis Of Global Perspective'

Megha Mishra[1*], Dr. Nupur Sony[2], Alpika Verma[3], Ms. Saloni Rathore[4], Mr. Moiz[5], Mr.Prakhar Saxena[6]

[1*]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[2]Official Designation/Institution Details- Associate Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[3]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[4]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[5]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[6]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh

Abstract
The rapid growth of e-commerce has sparked concerns about consumer privacy and data security, leading to an explosion in data collection and processing. Governments all around the world have therefore put in place a variety of data privacy laws to guarantee security and openness in data processing. The purpose of this study is to look into how data privacy laws affect consumer confidence and the performance of e-commerce globally. According to the research, nations with stricter data privacy laws—like the General Data Protection Regulation (GDPR) of the European Union—have better levels of perceived security and consumer trust. Conversely, countries with less stringent regulations, such as the United States, experience lower levels of consumer trust and perceived risk. The study also reveals that data privacy regulations have a positive impact on e-commerce success, as consumers are more likely to engage in online shopping when they feel their personal data is secure.
The study adds to the body of current work by offering a thorough assessment of the effects of data privacy laws on customer confidence and e-commerce performance across nations. The findings have significant implications for policymakers, businesses, and consumers, highlighting the importance of implementing robust data privacy regulations to foster trust and drive e-commerce success.

Keywords: Data Privacy, Consumer Trust, E-commerce, Regulations, Global Perspective

1. Introduction

Globally, the Covid-19 pandemic has compelled both people and governments to take hitherto unheard-of steps. Platform popularity has significantly increased as a result of required social distancing standards and a general trend toward a contact-free approach, particularly with the implementation of Unlock 3.0 measures.[1]
Modern consumers have different needs and expectations from businesses since they are well-educated and adept at using the power of online communication. Information that aids customers in choosing a certain product includes availability, accuracy, prior user experiences, delivery speed, and details on discounts and special offers. Additionally, since consumers can "go" from business to business and purchase a product with just one click in the current online age, it is advised that marketing departments be innovative, creative, and constantly evolving to maintain the interest of contemporary consumers (e-consumers). Search engine marketing, which includes pay-per-click and SEO advertising; email marketing; affiliate marketing; banner ads on websites; online video ads, also known as video marketing; social media marketing, of which Facebook marketing is the most prominent because of its broad consumer reach; Twitter marketing; modern viral marketing; and mobile marketing are some of the more contemporary marketing techniques that electronic marketing offers businesses. If effectively used in brand development, all of these techniques provide a number of benefits to businesses that can greatly impact the enhancement of their operations.
Concerns over customer privacy and data protection have been raised by the explosive rise of e-commerce, which has resulted in a boom in data gathering and processing. Governments all around the world have therefore put in place a variety of data privacy laws to guarantee security and openness in data processing. Among the numerous laws designed

[1] The Ministry of Home Affairs Order dated 29 July 2020 has allowed all essential activities (barring a few) in areas outside containment zones.

to safeguard customer data are the California customer Privacy Act (CCPA) in the US, the General Data Protection Regulation (GDPR) in the EU, and the Personal Data Protection Act (PDPA) in Singapore.

In recent years, there has been growing concern about the impact of data privacy regulations on consumer trust and e-commerce success.[2] On one hand, strong data privacy regulations can help build trust between consumers and businesses, as they provide a sense of security and protection for personal data.[3] Conversely, overly restrictive regulations can lead to increased costs and bureaucratic hurdles for businesses, which may negatively impact their ability to operate effectively.[4]
The study is important because it offers a thorough grasp of how data privacy laws affect consumer confidence and the success of e-commerce in various nations. We can find best practices and lessons gained by examining the experiences of different nations, which can then be used to guide company strategy and policy decisions.
The remainder of this introduction will provide an overview of the importance of data privacy regulations, the current state of global data privacy regulations, and the research questions that will guide our study.

1.1 Data Privacy Regulations: Why They Matter
Data privacy regulations are essential because they provide a framework for protecting consumer data from unauthorized access, use, or disclosure.[5] Personal data is becoming more and more important in the current digital era, and businesses are motivated to gather as much data as they can in order to obtain a competitive edge.[6] However, this raises serious concerns about consumer privacy and security.
The importance of data privacy regulations is evident in several ways. First, they provide a safeguard against identity theft and other forms of cybercrime.[7] Second, they ensure that consumers have control over their personal data and can make informed decisions about how their information is used.[8] Third, they promote transparency and accountability in data handling practices.[9]

1.2 Current State of Global Data Privacy Regulations
Although laws governing data privacy are not new, there has been a notable change in recent years toward stricter laws.[10] In 2018, the European Union implemented the General Data Protection Regulation (GDPR), which sets a high standard for data protection across all EU member states.[11] The GDPR gives people the right to access and remove their personal data, mandates that businesses get their express consent before collecting it, and imposes hefty fines for noncompliance.. Other countries have also implemented or are planning to implement similar regulations. For instance, customers in the US have protections comparable to those under the GDPR under the California Consumer Privacy Act (CCPA).[12]
The Market Study on E-Commerce was published by the Competition Commission of India ("CCI").[13] According to research released in January 2020, the sector's sales increased from USD 39 billion in 2017 to USD 120 billion in 2020, placing India among the world's fastest-growing e-commerce markets. Even while the industry has been expanding steadily, the current pandemic and its effects—such as widespread fear of the virus due to the growing Number of COVID-19 cases—have helped to support the rise of e-commerce platforms over traditional marketplaces.
Given the aforementioned, it is more important than ever to safeguard consumers and to enact the necessary legislation to do so in the realm of digital commerce. As a result, on July 23, 2020, the Ministry of Consumer Affairs, Food, and Public Distributions notified the Central Government of the Consumer Protection (E-Commerce) Rules, 2020 ("Rules") in accordance with Section 101(2)(zg) of the Consumer Protection Act, 2019 ("CPA 2019").[14]

2.E-Commerce

[2] Kumar et al. (2019). The Impact of Data Privacy Regulations on Consumer Trust.
[3] European Commission (2018). General Data Protection Regulation (GDPR).
[4] McKinsey & Company (2019). The Future of Data Privacy.
[5] Federal Trade Commission (2012). Protecting Consumer Privacy in an Era of Rapid Change.
[6] International Association of Privacy Professionals (2019). The Value of Personal Data.
[7] Ponemon Institute (2019). The Cost of Data Breaches.
[8] Federal Trade Commission (2012). Protecting Consumer Privacy in an Era of Rapid Change.
[9] European Commission (2018). General Data Protection Regulation (GDPR).
[10] International Association of Privacy Professionals (2019). The Evolution of Data Privacy Regulations.
[11] European Commission (2018). General Data Protection Regulation (GDPR).
[12] California Legislature (2018). California Consumer Privacy Act (CCPA).
[13] "Competition Commission of India, Market Study on E-Commerce in India (08 January, 2020)"
[14] "A preliminary draft of the Rules was released in November 2019, wherein consultation from various stakeholders had been invited by December 2019. The 2019 draft of the Rules was preceded by the E-Commerce Guidelines for Consumer Protection, 2019. The present version of the Rules comprises an upgraded version of the 2019 draft rules which replaces the E-Commerce Guidelines for Consumer Protection, 2019."

Internet-enabled trade is made possible in previously unheard-of ways by electronic commerce platforms. The architecture of electronic commerce, with its pervasiveness, offers businesses and consumers a dynamic and cooperative platform. Customers can choose from a wide variety of products and services available anywhere in the world at any time. Companies are continuously developing new technology to meet the ever-changing demands of the e-commerce industry. The increase in the number of people using information and communication technology (ICT) as a trading platform is one of the primary factors driving the expansion of e-commerce.

Put simply, electronic commerce involves buying and selling of goods and services through electronic means. Black's Law Dictionary defines Electronic Commerce as "business conducted without the exchange of paper based documents through the use of electronic and/or online devices. It includes activities such as procurement, order entry, transaction processing, payment, authentication and nonrepudiation, inventory control, order fulfilment, and customer support. The general public participates in ecommerce, almost unknowingly these days. Ecommerce devices include computers, telephones, fax machines, barcode readers, credit cards, automated teller machines (ATM) or other electronic appliances, whether or not using the internet."

The WTO Work Programme on Electronic Commerce defined "electronic commerce" to mean "the production, distribution, marketing, sale or delivery of goods and services by electronic means". The Committee further stated that "a commercial transaction can be divided into three main stages: the advertising and searching stage, the ordering and payment stage and the delivery stage. Any or all of these may be carried out electronically and may therefore be covered by the concept of "electronic commerce".[15]

In order to enable and facilitate commerce through electronic means, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce (MLEC) in 1999. This law gives national legislators a set of internationally recognized guidelines that are intended to eliminate legal barriers and improve legal predictability for electronic commerce. The Model Law is widely considered to be one of the foundational pieces of contemporary electronic commerce law because of its adoption of the core concepts of non-discrimination, technological neutrality, and functional equivalency.

Based on the UNCITRAL Model law, the Indian Information Technology Act, 2000, provides legal recognition to transactions carried out by electronic means. According to the Act, "electronic commerce" refers to transactions conducted using electronic data interchange and other electronic communication channels that substitute paper-based communication and information storage systems.

2.1 Kinds of E-commerce

a. **B2B – Business-To-Business** – E-commerce has enabled businesses to partner with other businesses for efficiently managing their business functions. Here businesses commonly use the Internet to integrate the value added chain that can extend from the supplier of raw materials to the final consumer. Indiamart.com is one such B2B online market place which provides a platform for businesses to find other competitive suppliers.
b. **B2C - Business-To-Consumer** – In a Business to Consumer (B2C) transaction, the distribution channel typically starts with manufacturer and goes through a distributor/ wholesaler to retailer, who interacts with the end customer. The B2C ecommerce model is not only cost effective in terms of investment to the seller, but also provides consumer with products at discounted price.
c. **C2C – Consumer-To-Consumer** – Here individuals use Internet, social media and mobile phones as means to sell goods and services, either through their personal websites, email, auction sites, text messages through mobile phones and sites providing classified advertising services. For example, portals such as eBay, OLX and Quikr enable consumers to transact with other consumers.
d. **B2B2C – Business to Business to Consumer or Intermediary Model –** The B2B2C model, also known as the Intermediary Selling model, is an expanded B2C model that is frequently utilized in e-commerce. In this case, a second intermediary company helps the first company deal with the final customer. Because the marketplace model allows the manufacturer to reach far-flung regions with his goods and services, this model is cost-effective for him. One of the most popular e-commerce sites, Flipkart, for example, offers a platform for customers to buy a wide range of products, including electronics, apparel, music, and books. Amazon, Jabong, and Snapdeal are just a handful of the e-commerce companies that have adopted this strategy in recent years, demonstrating its popularity. These online marketplaces collaborate with payment gateway providers who offer a platform for handling payments or only offer the option of cash on delivery, in which the customer pays for the items when they are delivered.

2.2 Modes of E-marketing

Teleshopping:

Advertisements extolling the virtues of body slimming gadgets, magical skin creams, and cleaning equipment with extensive demos on television are a common phenomenon today. There are channels such as telebrands and homeshop18,

[15] "World Trade Organisation, "Declaration on Global Electronic Commerce", (1998), available at http://r0.unctad.org/ecommerce/event_docs/colombo_wto.pdf,"

which are exclusively dedicated to telemarketing. Additionally, teleshopping includes time on many channels, such as news and entertainment. To allow customers to place their orders and provide simple payment choices, these ads typically display toll-free Numbers. Additionally shown on the screen are the product's price, code Number (if applicable), and seller's phone Number. A key benefit of teleshopping is that it allows a company with a single location to access a big Number of geographically dispersed potential clients.

Telemarketing:
Telemarketing is a method of selling goods or services using telecommunication devices such as Mobile phones, landlines, satellite phones and voice over Internet protocol (VoIP). It can be done from the seller's place of business or from a call centre or even from home. It is a form of distance selling where the business can reach far and wide without much effort and expense. For example, the call center is in India, yet the parent firm is in the UK. A call regarding a product in the UK will be placed to the customer from India. In these types of distance selling, it is crucial that the telemarketer adequately and correctly discloses the products or services to the clients.

Internet Shopping:
Internet shopping or commonly called online shopping is now one of the most convenient and quick modes of e-commerce to which consumers have adopted. Here the consumer browses the online catalogue on the product or service he desires to purchase and places an order. Payment is made by using some safe online payment modes. On receiving the order, the supplier or seller delivers the goods at the consumer's place through postal service or courier. Thus, internet shopping enables one to visit a world market, make best choice of goods at competitive prices by just a click of button.

Mobile commerce:
Mobile commerce (m-commerce) has also created immense platform for e-commerce transactions today. The phrase mobile commerce was originally coined in 1997 to mean "the delivery of electronic commerce capabilities directly into the consumer's hand, anywhere, via wireless technology." Mobile money transfers to mobile ATMs, mobile ticketing, mobile vouchers and coupons, sale of ring-tones, wallpapers, and games for mobile phones, information such as news, stock market etc. are some of the common transactions for which mobile commerce is extensively used. Likewise, with several online shopping portals providing mobile applications for purchase of goods and services, mobile commerce has been the most convenient mode for a consumer to purchase goods and services, without even using a computer or laptop.

Social media shopping:
A subset of electronic commerce known as "social media commerce" refers to the use of social media platforms like Facebook, Twitter, and YouTube for online business transactions. Because it facilitates social interaction and user contributions to help with online goods and service buying and selling, social media commerce is growing. It contains user recommendations, reviews, and ratings from customers that draw users to the site.

2.3 E-marketing Trends in India
Indeed, e-business has become a significant possibility for India. Due to the incredible growth of mobile phones and the introduction of 3G nationwide, a significant number of consumers from both urban and rural areas are making purchases online. It is a truth that the internet has eliminated the distinction between small and major cities, allowing consumers in small towns to purchase the same high-quality, branded goods that were formerly exclusive to consumers in bigger cities.[16] Over 2 billion people worldwide are connected by the thriving Internet sector. A McKinsey research from December 2012 provides seven important conclusions about the impact of and future prospects for the Internet in India. The research claims that India currently has the third-largest Internet user base in the world, with approximately 120 million users. With 330 million to 3.2 billion Internet users in 2019, India is predicted to have the second-biggest user base globally and the greatest in terms of incremental growth. Additionally, according to the analysis, India's economic contribution from the Internet might double over the next three years, rising from 1.6 percent of GDP to 2.8 to 3.3 percent by 2018.[17]
Additionally, the Rules apply extraterritorially to e-commerce companies that may not be based in India but routinely provide goods and services to Indian customers (Rule 2(2)).

[16] "Maitra Dilip, E-commerce is a new dream for India Inc., Deccan Herald, (10/07/2013) http://www.deccanherald.com/content/210955/e-commerce-dream-india-inc.html%20 on dated 09.06.2019"
[17] "Gnanasambandam Chandra, Madgavkar Anu et al, Online and Upcoming: The Internet's Impact on India, (December 2012), p.1, available at https://www.google.co.in/?gfe_rd=cr&ei=-ad1Vca7MsKM8QeF74GYCw#q=Gnanasambandam+Chandra%2C+Madgavkar+Anu+et.+Al.%2C+%E2%80%9COnline+and+Upcoming:+The+Internet%E2%80%99s+Impact+on+India%2C%E2%80%9D+December+2012%2C+www.mckinsey. com, on dated 12.06.2019"

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 2 (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

3.Legal Framework in India

3.1 Corporate Law and Regulatory Frameworks in India

Corporate law in India provides the legal framework for governing the establishment, operation, and regulation of corporations, including digital platforms and online marketplaces. The Companies Act, 2013[18], is the primary legislation governing corporate entities in India, prescribing rules related to incorporation, management, governance, and compliance. Company governance, consumer protection, competition law, and data privacy are just a few of the regulatory areas that interact with company law in the context of digital platforms. To foster competition and avoid market distortions, the Competition Act of 2002 forbids anti-competitive mergers and acquisitions, abuses of dominant positions, and anti-competitive agreements.

Additionally, consumer protection laws such as the Consumer Protection Act, 2019[19], strive to protect customers' rights and guarantee ethical and open business operations. Digital platforms are required by these rules to preserve customer data, give accurate information, and properly handle complaints.

Furthermore, data privacy and security have emerged as critical concerns in the digital age, prompting the introduction of the Personal Data Protection Bill, 2019. Once enacted, this legislation will establish a comprehensive framework for the processing and protection of personal data, imposing obligations on entities handling such data, including digital platforms and online marketplaces.

3.1.1 Corporate Governance and Accountability in Indian Digital Ecosystems

Effective corporate governance is essential for maintaining trust, integrity, and accountability within digital platforms and online marketplaces operating in India. Corporate governance frameworks dictate the structure, composition, and conduct of boards of directors, executives, and key stakeholders, ensuring transparency, oversight, and ethical behavior.

Section 3 of the Competition Act 2000 in India addresses anti-competitive agreements, which forbid contracts that have a significant negative impact on competition or are likely to do so (AAEC).It controls self-preferencing, exclusive tie-ups, and data-driven collisions, where competitors share consumer data and engage in algorithmic pricing. At the same place, Section 4 of this Act prohibits abuse by enterprises holding dominant market power. Discriminatory ranking of sellers/products using consumer data insights, and tying or bundling of services (e.g., forcing the use of the platform's own payment gateway). Exploitation of consumer data to exclude rivals or manipulate pricing. Competition Commission of India investigates platform practices like self-preferencing, tying, discriminatory ranking, and data misuse and Works in convergence with Digital Personal Data Protection Act, 2023 (DPDP Act) to ensure consumer trust, privacy, and fair competition in e-commerce.

Google Play Store Policies (CCI, 2022)

Google mandated that app developers using the Play Store must exclusively use its Google Play Billing System (GPBS) for in-app purchases.This amounted to a tie-in arrangement, restricting app developers from using third-party payment services. Google also imposed unfair conditions by mandating pre-installation of its apps (Chrome, YouTube, Gmail, etc.) on Android devices as part of licensing agreements. CCI found this to be abuse of dominant position under Section 4 of Competition Act, 2002.Self-preferencing and exclusion of rivals (payment providers, app stores) were highlighted as anti-competitive conduct.

In October 2022, CCI imposed a penalty of ₹936 crore on Google for anti-competitive Play Store billing policies.

Companies Act of 2013, in particular sections 134[20] (financial statements and board report) where it requires the approval and signing of financial statements and the contents of the Board's report to be laid before the company in a general meeting, it include the auditor's report attached, the Board's approval and signature by authorized directors, and important disclosures in the Board's report, like loans, energy conservation, technology absorption, and related party transactions. A company shall be liable to a penalty of three lakh rupees if it fails to comply with the provisions of this section, and every officer of the company who fails to do so shall be liable to a penalty of fifty thousand rupees.

149[21] (board composition and independent directors), 166 (duties of directors) describes a director's basic responsibilities, which include acting in line with the company's articles, promoting its goals in a way that benefits members and other stakeholders, exercising due care, skill, and diligence, using independent judgment, avoiding conflicts of interest, and avoiding undue gains. Additionally, directors are not allowed to assign their offices, and doing so is null and invalid.

[18] The Companies Act, 2013
[19] Consumer Protection Act, 2019
[20] The Companies Act, 2013
[21] The Companies Act, 2013

Sections 188 and 177[22] establish substantive requirements for related-party transactions, including shareholder approval, disclosure, and ratification. Section 177 ensures the Audit Committee examines and approves these transactions, while Section 188 empowers minority shareholders, prevents insider deals, and prevents oppression/mismanagement by limiting asset diversion and tunnelling. The legislation combines audit committee scrutiny and mandatory shareholder approval to ensure transparency, accountability, and prevent oppression/mismanagement by preventing insider deals and curbing asset diversion and self-dealing. Post-Satyam scandal (2009), these provisions were strengthened to avoid the recurrence of fraud through insider transactions.

Moreover, the Reserve Bank of India (RBI) and the Ministry of Corporate Affairs (MCA) have also issued guidelines and regulations pertaining to corporate governance, aimed at enhancing transparency, protecting shareholder interests, and preventing corporate misconduct.

RBI Circular on Corporate Governance in Banks (2002, updated 2015 & 2021)[23] mandates background checks, independent directors, board oversight, accurate reporting of risk exposures, non-performing assets, and financials, and related-party lending transparency. The RBI's 2006[24], 2014, and 2018 mandates background check, independent directors, board oversight, accurate reporting of risk exposures, non-performing assets, and financials, and related party lending transparency. The guidelines on the Fair Practices Code for NBFCs require clear disclosure of terms, interest rates, and grievance procedures. Banks must post fair dealing and customer rights policies on their websites and use "Pillar 3 disclosures" for market disciplines.

The Securities and Exchange Board of India (SEBI), which regulates listed companies through the Listing Obligations and Disclosure Requirements (LODR) regulations[25]. These regulations mandate disclosures related to corporate governance practices, board composition, remuneration, and related-party transactions, thereby promoting transparency and accountability.

Although their primary goal is to improve corporate governance and transparency requirements for listed businesses, the SEBI (Listing Obligations and transparency Requirements) Regulations, 2015 (LODR) also indirectly address issues related to data protection and digital privacy. In order to safeguard stakeholders and shareholders, SEBI highlights the importance of timely, accurate, and secure disclosures in light of the increasing digitization of company reporting and investor communication.

Companies are required by Regulations 30 and 46 to securely and transparently publish sensitive information, including financial data, shareholding patterns, and material events, on their official websites and stock exchanges. Regulation 17(9), which requires boards to establish internal measures to protect digital records, sensitive data, and stakeholder data, is making cybersecurity and data privacy a more integral component of a company's risk management system. Furthermore, by requiring robust IT systems, regular audits, and data protection procedures, SEBI's cybersecurity circulars for market infrastructure institutions (2017, 2022) align with LODR principles.

Therefore, LODR indirectly enforces digital privacy norms by requiring listed companies to maintain secure digital disclosures, transparency, and protection against misuse of sensitive information, thereby fostering investor confidence in the digital ecosystem, even though it does not explicitly legislate on personal data privacy like the proposed Digital Personal Data Protection Act, 2023.

The role of corporate law in regulating digital platforms and online marketplaces in India is integral to promoting competition, protecting consumers, and ensuring accountability in the digital ecosystem. By aligning regulatory frameworks with evolving market dynamics and technological advancements, corporate law can facilitate innovation, foster trust, and mitigate risks associated with digital platforms.

However, effective regulation requires a collaborative effort involving regulators, policymakers, industry stakeholders, and civil society to address the complex challenges posed by digital ecosystems. By leveraging the principles of corporate governance, transparency, and accountability, India can create a regulatory environment conducive to the sustainable growth and development of its digital economy.

SATYAM SCANDAL CASE 2009

The 2009 Satyam Computer Services affair is regarded as one of the largest business frauds in India. The founder and chairman of Satyam, Ramalinga Raju, acknowledged that he had been manipulating the company's financial statements for a number of years. Investors, regulators, and stakeholders were misled by the fraud, which involved misrepresenting revenues, earnings, and cash balances by around ₹7,000 crore. Up until it was discovered in January 2009, this deception increased market confidence and stock values. Concerns concerning the efficacy of corporate governance, auditing procedures, and regulatory supervision were highlighted by the incident, which rocked corporate India and damaged

[22] The Companies Act, 2013

[23] https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=1521

[24] https://www.rbi.org.in/commonman/english/Scripts/Notification.aspx?Id=1572

[25] https://www.sebi.gov.in/legal/regulations/feb-2023/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-regulations-2015-last-amended-on-february-07-2023-_69224.html

investor confidence. Satyam was eventually purchased by Tech Mahindra, who changed its name to Mahindra Satyam. In 2013, the two companies amalgamated.
Data is just as important as money in the modern digital economy. The Satyam case demonstrated how information manipulation can deceive stakeholders; similarly, the improper handling of customer data can undermine confidence in businesses and e-commerce.

3.2 Marketplace e-commerce entities (Rule 5)
To be eligible for the safe harbor exemption under Section 79(1) of the Information Technology Act, 2000 ("IT Act"), marketplace e-commerce businesses must adhere to the following requirements in addition to those outlined in the Intermediary Rules:
Records: To keep track of vendors who have regularly sold products or services that have been taken down or whose access has been restricted in accordance with the IT Act, the Trade Marks Act of 1999, or the Copyright Act of 1957. Such vendors' access to the marketplace's e-commerce platform may be terminated at the marketplace's discretion.

3.3 Sellers (Rule 6)
Fake reviews: It is against the law for sellers to publish reviews that pretend to be client endorsements of the products or services they are offering.
Duty to return: If products or services are flawed, inadequate, delivered late (unless there is a force majeure event), deviate from the claimed features, or are fraudulent, sellers must return the products or withdraw their services and issue a refund.
Implications: Although the Rules don't explicitly cover this, product grading and ranking should be included in the definition of "reviews." Furthermore, a new right to return or refund that was not previously available under the Consumer Protection Act of 1986 has been made possible by the sellers' obligation to take back or withdraw.
According to the Legal Metrology (Packaged Commodities) Rules, 2011 ("LM Rules"), which govern product labeling, all imported goods must include pertinent information on the packaging regarding the manufacturer, place of origin, or assembly. The vendors must, however, provide the information and notices mandated by the relevant laws (including the LM Rules) in accordance with the Atmanirbhar Bharat vision.

3.4 Consumer Protection (E-Commerce) Rules, 2020[26]
All goods and services, including digital products, that are transacted over an electronic or digital network are covered by Rule 2. All e-commerce models, including marketplace and inventory models (discussed below), all e-commerce retail, including retail trading under multiple brands and single brands, and all types of unfair trade practices across all e-commerce models are covered by Rule 2.
The following conditions must be met for the Rules to not apply to a natural person: (a) the activities are being carried out in a personal capacity; and (b) the activities do not constitute a regular or systematic part of any professional or commercial activity. This is true even though the Rules have been specifically made applicable to e-commerce entities. Simply put, the Rules would not apply if a person was conducting a transaction in their personal capacity rather than regularly or methodically for any kind of professional or commercial activity (for example, selling a used book online without using an e-commerce entity).

As a result, natural persons who occasionally engage in business-to-business or consumer-to-consumer interface transactions may be disqualified.
The Internet and Mobile Association of India (IAMAI) estimated in 2014 that approximately 1 million large and small retailers use online marketplaces to reach their customers, representing a wide range of categories such as electronics, books, apparel, accessories, footwear, jewelry, and more. E-commerce has become a booming business in India today, and it is at the forefront of all business sectors.
Lawmakers around the world, including in India, have long acknowledged the need of protecting fundamental rights to consumer welfare. In order to safeguard the interests of consumers, India passed the Consumer Protection Act in 1986 in accordance with the United Nations Guidelines on Consumer Protection (UNGCP). The enactment's stated goals of defining consumer rights and offering prompt, affordable remedies are what make it so popular. For business-to-consumer e-commerce, the existing provisions of the Consumer Protection Act, 1986, primarily the provisions of "Deficiency in Service" under Section 2(1)(g) or "Unfair Trade Practices" under Section 2(1)(r), are applied to disputes in online transactions, even though there are no specific laws governing e-commerce in India.

3.5 Information Technology Act 2000[27]
Section 43A Restitution for data privacy violations was suggested as Companies that handle sensitive personal data, such as e-commerce platforms, are required to provide compensation if they neglect to implement appropriate security measures

[26] https://www.consumerprotection.in/consumer-protection-e-commerce-rules-2020/
[27] https://www.meity.gov.in/content/information-technology-act-2000-0

and cause unjustified loss or profit. Section 72 Penalties Section 72 A r/w (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, prohibit unauthorized access, disclosure, or sharing of personal data obtained under legal authority. Suppose intermediaries or service providers reveal personal data without consent, for illegal gain, or to harm others. In that case, they risk imprisonment for up to three years and/or a fine of up to ₹5 lakh for breach of a lawful contract. If user data is misused or unlawful content is distributed, the intermediary is held directly accountable under Section 79.

3.6 Digital Personal Data Protection Act, 2023 (DPDP Act)

Intermediaries, who are referred to as Data Fiduciaries under the Digital Personal Data Protection Act of 2023, are subject to strict duties to guarantee the fair and legal processing of personal data. While Section 5 requires explicit notification of data use and Section 6 requires obtaining and properly honoring valid permission, Section 4 requires processing to be purpose-specific.

Additionally, under Section 8(3), Data Fiduciaries are required to keep personal data accurate and complete, implement reasonable security measures to prevent breaches in accordance with Section 8(5), which carries penalties of up to ₹250 crore for non-compliance, and report any breaches in accordance with Section 8(6), which imposes penalties of up to ₹200 crore for non-compliance.

Furthermore, Section 8(7) prohibits keeping personal information longer than is required for processing. According to Section 9, verifiable consent from the parent or guardian must be obtained in the prescribed manner before processing the personal data of a child, who is defined as an individual under the age of eighteen or a person with a disability who has a legal guardian. Failure to fulfill obligations pertaining to children's data may result in fines of up to ₹200 crore.

Sections 33 and 34 of the DPDP Act stipulate that non-compliance can result in financial penalties of up to ₹250 crore per occasion, especially when it comes to data security breaches or improper processing. Penalties for general noncompliance with duties might reach ₹50 crore.

4. Global Data Privacy Regulations

4.1 General Data Protection Regulation (GDPR) Compliance[28]

By placing requirements on data controllers and processors, the General Data Protection Regulation (GDPR) creates extensive guidelines to safeguard personal information in e-commerce. Obtaining freely provided, informed, specific, and revocable consent before to processing personal data is one of the main provisions Another is providing explicit notification regarding the types, recipients, retention, and purpose of data (Articles 4, 7). providing data subjects rights like access, rectification, erasure, restriction, portability, objection, and protection from automated decision-making (Articles 15–22); guaranteeing data accuracy, minimization, and limited retention (Article 5); and putting in place suitable organizational and technical security measures in addition to requiring breach notification within 72 hours (Articles 32–34). GDPR is a strict legal framework for protecting customer data in e-commerce, with harsh fines of up to 4% of the global annual turnover or €20 million, whichever is higher, for non-compliance.

Article 17 of the General Data Protection Regulation (GDPR) establishes the *"Right to Be Forgotten,"* also referred to as the right to erasure. Under certain conditions, it enables people (data subjects) to request that their personal information be removed from an organization's records. These include circumstances in which the data must be deleted to meet legal requirements, the data has been treated illegally, the data is no longer required for the reason it was collected, or the subject withdraws their consent.

Despite being an EU rule, U.S. businesses who handle the data of EU citizens are impacted by the GDPR's extraterritorial reach. In their decisions, U.S. courts are increasingly considering GDPR compliance. For instance, although though Schrems II was largely an EU case, it had significant ramifications for data transfer agreements between the EU and US corporations, which shaped the way US courts perceive cross-border data privacy issues.[29]

Information Commissioner's Office v. British Airways Plc 2018[30]

More than 400,000 customers of British Airways were impacted by a serious data breach that exposed private financial and personal data in 2018. Between June 22 and September 5, 2018, hackers took use of flaws in the airline's mobile app and website to cause the breach. Names, addresses, credit card numbers, and login credentials were among the leaked data. Customer data was vulnerable to unauthorized access for over two months before the incident was discovered.

British Airways was fined £20 million by the UK's Information Commissioner's Office (ICO) in October 2020 for failing to secure the financial and personal information of its customers. Compared to the original £183 million recommended in 2019, which was the highest amount permitted by the General Data Protection Regulation (GDPR) at the time, this fine represented a significant decrease. The airline's claims regarding the attack and the financial toll of the COVID-19 pandemic on the airline sector were blamed for the decrease. The case emphasizes how crucial it is to put strong security

[28] https://gdpr-info.eu

[29] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), C-311/18 (ECJ, July 16, 2020).

[30] https://www.whitecase.com/insight-alert/uk-ico-fines-ba-ps20m-data-breach

procedures in place to safeguard consumer data and the dire repercussions that businesses may suffer under GDPR if they don't.

Hamburg Commissioner for Data Protection and Freedom of Information v. H&M Hennes & Mauritz Online Shop A.B. & Co. KG,2020[31]

H&M Germany was fined €35 million in 2020 for handling employee personal data in violation of the GDPR. Without telling the workers or getting their permission, the corporation had gathered a lot of data about their personal lives, including family matters, religious convictions, and health concerns, and stored it in a centralized system that management could access.

The GDPR's tenets of lawfulness, fairness, transparency, and purpose limitation were all broken by this illegal and opaque handling of sensitive personal data. The fine, which was one of the biggest GDPR penalties at the time, was levied by the Hamburg Data Protection Authority. It emphasized that even internal employee data must be treated strictly in accordance with privacy regulations, as noncompliance can result in significant financial penalties under GDPR.

4.2 California's Consumer Privacy Act (CCPA)[32]

By giving customers the ability to know, access, and request the deletion of personal information that companies collect about them, the California Consumer Privacy Act (CCPA) gives them data privacy rights in e-commerce. These rights include the "right to opt-out" of the sale of personal data and protection from discrimination for exercising them. Companies must preserve customer data with acceptable security measures, give clear privacy disclosures, and respond to customer inquiries within the allotted time frames.

For-profit businesses that reach specific income or data processing thresholds are subject to the law. In addition to statutory damages in cases of data breaches, violations can result in civil penalties of up to $2,500 for inadvertent violations and $7,500 for willful violations. This ensures responsibility and fosters customer trust in e-commerce platforms.

The U.S. courts have also focused on it. Important precedents for interpreting state-level privacy regulations in the context of e-commerce were established when the court considered whether Google's data gathering activities violated the CCPA in **Calhoun v. Google LLC**.[33]

In the notable US privacy class action **Calhoun et al. v. Google LLC,** Google Chrome users claimed that Google collected their personal information without their consent, even though they had not chosen to link their browser to their Google accounts. The plaintiffs said that Google's privacy notice deceived consumers into thinking that unless they activated the sync option, no personal information would be gathered.[34]

The Ninth Circuit Court of Appeals overturned a district court ruling in favor of Google in August 2024. The district court's attention on whether the data collection was "browser agnostic" instead of determining whether a reasonable user would have realized that their data was being gathered was unduly emphasized by the appellate court. In order to assess whether Google's data practices breached users' expectations and consent, the matter was remanded for additional hearings..

U.S. District Judge Yvonne Gonzalez Rogers dismissed the class action with prejudice in June 2025, stating that user consent has to be determined by individual assessments. Although the class action was essentially dismissed by this ruling, individual claims could still be made. The case highlights persistent issues with user permission and openness in online privacy policies.

4.3 The Personal Information Protection and Electronic Documents Act (PIPEDA), 2000 [35]

It regulates how Canadian private sector businesses, especially e-commerce platforms, gather, utilize, and disclose personal data. Before collecting personal data, organizations are required by PIPEDA to get meaningful consent, make sure the data is accurate, comprehensive, and safeguarded by appropriate security measures, and use it solely for the purposes for which it was obtained. Customers are entitled to view and update their personal data.

As data controllers or processors, e-commerce intermediaries must put organizational and technical safeguards in place to protect data, report breaches to individuals and the Office of the Privacy Commissioner of Canada (OPC), and make sure third-party processors follow these rules. Although PIPEDA does not specify fixed fines, non-compliance can result in

[31] https://www.rpclegal.com/snapshots/data-protection/h-and-m-hit-with-35-3m-fine-for-gdpr-employee-breach/
[32] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf?
[33] Calhoun v. Google LLC, 526 F. Supp. 3d 605 (N.D. Cal. 2021).
[34] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cdn.ca9.uscourts.gov/datastore/opinions/2024/08/20/22-16993.pdf?utm
[35] https://laws-lois.justice.gc.ca/eng/acts/p-8.6/?utm

court-imposed damages, reputational loss, and mandatory compliance directives. As a result, adherence is crucial for safeguarding consumer trust in digital commerce. Non-compliance can also lead to investigations and corrective orders by the OPC.

4.4 Personal Data Protection Act (PDPA), Singapore[36]

It creates extensive data privacy requirements for intermediaries and e-commerce platforms. Before collecting, using, or revealing personal data, organizations are required by the Act to get consent. They also have to make sure that consumers are aware of the reasons for the collection, such as marketing and profiling. The obtained data must not be kept for longer than is required and must only be utilized for the intended purpose. Customers are entitled to see and update their personal data.

In the event of a breach, e-commerce intermediaries must notify individuals and the Personal Data Protection Commission (PDPC) and put in place appropriate security measures, such as encryption, secure storage, and third-party vendor monitoring. The Do-Not-Call (DNC) Registry regulates marketing communications, requiring consent checks prior to delivering advertising messages. In order to ensure strong security of customer data in digital commerce, non-compliance can lead to PDPC investigations, compliance instructions, corrective orders, and financial penalties of up to SGD 1 million.

5.Comparative analysis

The rapid growth of e-commerce has led to a surge in data collection and processing, raising concerns about consumer privacy and data protection.[37] In response, governments around the world have implemented various data privacy regulations to ensure transparency and security in data handling.[38] This comparative analysis will examine the impact of data privacy regulations on consumer trust and e-commerce success globally, with a focus on India.

The European Union's **General Data Protection Regulation (GDPR)** is a comprehensive framework for data protection that sets a high standard for data privacy.[39] The GDPR provides individuals with the right to be informed, to access, to rectify, to delete, and to object to the processing of their personal data.[40] In addition, the GDPR requires companies to obtain explicit consent from consumers before collecting their personal data.[41]

The **California Consumer Privacy Act (CCPA)** in the United States is another significant example of a data privacy regulation.[42] The CCPA provides consumers with the right to access and delete their personal data, as well as the *right to opt out* of the sale of their personal data.[43] The CCPA also requires companies to provide clear and conspicuous notice of their data collection practices.

In Canada, the **Personal Information Protection and Electronic Documents Act (PIPEDA)** sets out guidelines for handling personal information in commercial transactions.[44]

In contrast, India's **Digital Personal Data Protection Act 2023** (DPDP)[45] is still been criticized for being inadequate and ineffective. The DPDP provides for the protection of personal data, establishes a data protection authority, and outlines the obligations of data fiduciaries.[46] However, the Act has been criticized for the following issues-

1. The Act's definition of a child as under 18 raises concerns about implementing digital access initiatives due to the need for parental agreement and age verification. This rigid categorization may create unnecessary compliance obligations. Balancing the safeguarding of teenagers' rights with flexibility is recommended, setting specific data processing criteria and obtaining consent based on their maturity.
2. Concerns have also been raised over the DPDP Act of 2023's exclusion of willingly given personal data. Additionally, there is doubt regarding the extent of the act's requirements due to the imprecise language used in Section 3(c)(i), which refers to processing data for "any personal or domestic purpose" by an individual.
3. The Act now prioritizes processing over data protection, ignoring India's low digital literacy. To prevent businesses from exploiting consent lack, precise restrictions on data processing should be included, along with clear definitions of terms like "any other person" to prevent government overreach.

[36] https://sso.agc.gov.sg/Act/PDPA2012?WholeDoc=1
[37] European Commission (2018). General Data Protection Regulation (GDPR).
[38] International Association of Privacy Professionals (2019). The Evolution of Data Privacy Regulations.
[39] European Commission (2018). General Data Protection Regulation (GDPR).
[40] Ibid
[41] Id
[42] California Legislature (2018). California Consumer Privacy Act (CCPA).
[43] Ibid
[44] Government of Canada (2000). Personal Information Protection and Electronic Documents Act (PIPEDA).
[45] Digital Personal Data Protection Act 2023
[46] Ministry of Electronics and Information Technology (2019). Personal Data Protection Bill.

4. The absence of provisions for compensating victims of breaches involving personal data is a noteworthy problem. The Consolidated Fund of India will eventually be credited with fines up to Rs. 250 crores that the Data Protection Board can levy on organizations that violate the Schedule of the Act. This runs counter to the idea of restorative justice, which is a conflict resolution strategy that emphasizes healing the harm done to people and communities rather than only punishing offenders. Because of this omission from the present Act, users are left without a way to pursue just compensation for their losses, which is a crucial avenue for them to pursue.
5. Sensitive digital personal data includes information like financial data, biometrics, and health records. Levels of sensitivity for digital data might differ greatly. As a result, special security measures must be taken when handling and storing various kinds of data. Unlike earlier versions of the law, which made a fundamental distinction between personal data and sensitive personal data, the current version does not make this distinction. There are many reasons to be concerned about the effectiveness of data protection safeguards in light of this departure from earlier versions of the Act and current regulatory frameworks, such as the SDPI standards, especially when handling sensitive data.
In comparison to global data privacy regulations, India's DPDP still lacks clear provisions on key issues such as consent and data subject rights.[47] The DPDP also lacks a clear definition of the other person, which could lead to confusion and uncertainty for companies operating in India.[48]
In contrast, global data privacy regulations, such as the GDPR and CCPA, provide explicit provisions on key issues, including consent and data subject rights.[49] These regulations also provide strong enforcement mechanisms, including fines and penalties for non-compliance.

6.Case Laws-

6.1 Case Laws in India Ensuring Privacy

In India, there have been several cases involving data privacy and security. One notable case is **Reserve Bank of India v. Digital Payment Company Private Limited (2019).[50]** In this case, the Supreme Court of India held that the Reserve Bank of India (RBI) had the power to regulate digital payments and impose penalties on companies that failed to comply with its regulations.
Another significant case is Justice **K.S. Puttaswamy (Retd.) v. Union of India**.[51] In this case, the Supreme Court of India held that the right to privacy was a fundamental right under the Indian Constitution. The court also held that individuals had a right to control their personal information and to prevent its use for unauthorized purposes.

6.2 Case Law Ensuring Privacy Globally

In addition to Indian case laws, there have been several significant global cases involving data privacy and security. One notable case is **Schrems v. Data Protection Commissioner (2015).** In this case, the European Court of Justice (ECJ) held that the Safe Harbor agreement between the United States and Europe did not provide adequate protection for personal data.
Another significant case is Facebook **Ireland Ltd v. Maximillian Schrems (2019**)[52]. In this case, the ECJ held that Standard Contractual Clauses (SCCs) used by Facebook to transfer personal data from Europe to the United States were invalid due to concerns about mass surveillance.

7. Conclusion

Regulations about data privacy are essential in establishing consumer confidence and revolutionizing the online market. This study's comparative analysis reveals that stringent privacy laws, such as California's CCPA, Singapore's PDPA, and the EU's GDPR, have significantly enhanced consumer trust in online shopping. These regulations guarantee accountability, openness, and informed consent in the way businesses manage personal information, fostering a sense of security that motivates customers to participate more actively in online transactions. Consumer trust, on the other hand, frequently declines in nations with laxer or less enforceable laws because people worry about their information being misused or shared without authorization.
From the standpoint of the consumer, these laws give people the ability to manage their digital identities by granting them rights like data access, deletion, correction, and objection to processing. Users feel more independent and equitable in the digital world when they have this kind of control. However, as demonstrated by new frameworks like India's Digital Personal Data Protection Act, 2023, the lack of robust enforcement procedures or compensation rights can still erode consumer confidence.

[47] Indian Express (2019). Personal Data Protection Bill: Experts raise concerns about its effectiveness.
[48] Ministry of Electronics and Information Technology (2019). Personal Data Protection Bill.
[49] European Commission (2018). General Data Protection Regulation (GDPR).
[50] Reserve Bank of India v. Digital Payment Company Private Limited (2019)
[51] (2019) 1 SCC 1
[52] ECLI:EU:C:2020:559

Beyond merely ensuring legal compliance, privacy laws have a profound impact on daily life by shaping online behavior, promoting ethical business practices, and safeguarding individual dignity in a data-driven economy. Ultimately, protecting data privacy has become crucial to social welfare, economic growth, and consumer trust. Customers are more inclined to contribute data responsibly when they feel safe, which promotes innovation, confidence, and the development of sustainable e-commerce globally.

8. Suggestions-

- Extend the extraterritorial scope to include international cloud services and e-commerce platforms while guaranteeing the complete protection of Indian customer data.
- To ensure deterrent against big businesses, implement revenue-based proportional fines.
- Mandate a strict 72-hour reporting timeline to the Data Protection Board and affected users to improve responsiveness and accountability.
- "Introduce rights that allow users to transfer their data to other services (data portability), to refuse or limit how their data is used (objection to processing), and to understand how automated systems make decisions (algorithmic transparency), giving users more control over personalized services and AI-driven recommendations in e-commerce."
- Mandate impact assessments, transparency, and opt-out options for algorithmic profiling in e-commerce platforms as CCPA.
- Introduce digital verification mechanisms, mandatory audits, and safe design standards for children's apps and services.
- Empower regional offices or sectoral regulators, especially for high-risk e-commerce platforms, with audit, inspection, and enforcement powers
- Provide the Right to be forgotten when data is used and accessed.