BALANCING THE GROWTH OF E-COMMERCE WITH DATA SECURITY AND PRIVACY: AN ANALYSIS OF THE INDIAN LEGISLATIVE FRAMEWORK.

Dissertation submitted to the National University of Advanced Legal Studies, Kochi in partial fulfilment of the requirements for the award of the degree of Master of Law (LL.M.) in International Trade Law (2024-2025)

NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES,

Kalamassery, kochi-683503, kerala, India

2024-2025

Submitted by,

JEMIMA B.S.

(Reg. no: LM0224011)

LL.M. (International Trade Law)

Under the guidance and supervision of

MR. RAVEENDRAKUMAR D, ASSISTANT PROFESSOR

MR. HARI S. NAYAR, ASSISTANT PROFESSOR

MAY 2025

CERTIFICATE

This is to certify that **Ms. JEMIMA B S,** Reg. No. **LM0224011** has submitted her dissertation titled**," BALANCING THE GROWTH OF E-COMMERCE WITH DATA SECURITY AND PRIVACY: AN ANALYSIS OF THE INDIAN LEGISLATIVE FRAMEWORK"** in partial fulfilment of the requirement for the award of Degree of Master of Law in International Trade Law to the National University of Advanced Legal Studies, Kochi under our guidance and supervision. It is also affirmed that, the dissertation submitted by her is original, bona-fide and genuine.

Date:

Place: Ernakulam

MR. RAVEENDRAKUMAR D.
Guide & Supervisor
Assistant Professor
NUALS, Kochi

MR. HARI S. NAYAR
Guide & Supervisor
Assistant Professor
NUALS, Kochi

DECLARATION

I do hereby declare that the dissertation titled, "**BALANCING THE GROWTH OF E-COMMERCE WITH DATA SECURITY AND PRIVACY: AN ANALYSIS OF THE INDIAN LEGISLATIVE FRAMEWORK** "researched and submitted by me to the National University of Advanced Legal Studies, Kochi in partial fulfilment of the requirement for the award of Degree of Master of Law in International Trade Law, under the guidance and supervision of **MR. RAVEENDRAKUMAR D.** and **MR. HARI S. NAYAR**, is an original, bonafide and legitimate work and it has been pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this University or any other Universities.

Date:

Place: Ernakulam

JEMIMA B S

Reg. No: LM0224011

LL.M., International Trade Law

NUALS, Kochi

ACKNOWLEDGEMENT

Firstly, I would like to extend my sincere and heartfelt gratitude to my Guides **Mr. Raveendrakumar D.** and **Mr. Hari S. Nayar**, Assistant Professors, National University of Advanced Legal Studies, Kochi for their valuable guidance, constructive advice, and staunch support at all stages of my dissertation work. Also I would like to extend my profound gratitude to **Dr. Anil R Nair**, Associate professor, Chairperson, Centre for Post Graduate Legal Studies and Director, Centre for Parliamentary Studies and Law Reforms for his constant support and encouragement.

Next I place on record, my sincere gratitude to the Vice-Chancellor **Hon'ble Justice Mr. S. Siri Jagan (Retd.)** for his conscientious and insightful guidance.

I thank Registrar **Dr. Lina Acca Mathew**, for imparting impeccable wisdom and inspiration throughout for the completion of this work.

I also express my due respect and gratitude to all the faculty members of NUALS, for their constant encouragement.

I convey my thanks to librarian and library staffs for their timely assistance to carry out this work.

Words fall short of expressing love, appreciation, and gratitude to God Almighty, my beloved parents and friends for their constant support.

JEMIMA B S

PREFACE

This dissertation, titled "Balancing the Growth of E-Commerce with Data Security and Privacy: An Analysis of the Indian Legislative Framework", is submitted in partial fulfilment of the requirements for the degree of Master of Laws. It represents the outcome of independent research undertaken with the objective of examining the legal and regulatory tensions between promoting digital commerce and safeguarding individual data rights in the evolving Indian context.

The exponential growth of e-commerce in India has presented significant opportunities for economic development, innovation, and consumer convenience. Simultaneously, it has raised pressing concerns regarding data security, privacy protection, and regulatory accountability. This research aims to critically evaluate the Indian legislative framework, most notably the Digital Personal Data Protection Act, 2023, in light of these competing imperatives, and to assess whether the existing legal mechanisms are adequately equipped to strike a balance between technological progress and the protection of fundamental rights.

LIST OF ABBREVATIONS

AI - Artificial Intelligence

APEC - Asia-Pacific Economic Cooperation

AU- African Union

B2C- Business-to-Consumer

B2G- Business-to-Government

C2B- Consumer-to-Business

CAN-SPAM Act- Controlling the Assault of Non-Solicited Pornography and Marketing Act

CBPR- Cross-Border Privacy Rules

CCC- California Civil Code

CCPA- California Consumer Privacy Act

CMMC- U.S. Cybersecurity Maturity Model Certification

COPPA- Children's Online Privacy Protection Act

CPA- Consumer Protection Act

CPRA- California Privacy Rights Act

DMA- Digital Markets Act

DPA- Data Protection Authority

DPC- Data Protection Convention

DPDP- Digital Personal Data Protection Act

DPIA- Data Protection Impact Assessments

DPO- Data Protection Officers

DSA- Digital Services Act

e WTP- electronic World Trade Platform

EC- European Commission

ECJ- European Court of Justice

EDI- Electronic Data Interchange

EDPD- European Data Protection Directive

EU- European Union

FOIA- Freedom of information act

FTC- Federal Trade Commission

GCI- Global Cybersecurity Index

GDPR- General Data Protection Regulation

GLBA- Gramm-Leach-Bliley Act

GPA- Global Privacy Assembly

HIPAA- Health Insurance Portability and Security Act

IBM- International Business Machines

ICCPR- International Covenant on Civil and Political Rights

IT ACT- Information Technology Act

JPC- Joint Parliamentary Committee

MLEC- Model Law on Electronic Commerce

MNC- Multi National Corporation

NDPR- Nigeria Data Protection Regulation

NIST Cybersecurity Framework- National Institute of Standards and Technology Cybersecurity Framework

NITDA- National Information Technology Development Agency

NITI Aayog- National Institution for Transforming India

OECD- Organization for Economic Cooperation and Development

PDP- Personal Data Protection

PII- Personally Identifiable Information

PIPL- Personal Information Protection Law

RTBF- Right To Be Forgotten

SDG- Sustainable Development Goal

SDPI- Sensitive Personal Data or Information

UDHR- Universal Declaration of Human Rights

UN – United Nations

UNCTAD- United Nations Conference on Trade and Development

WWW- World Wide Web

LIST OF CASES

- Justice K.S. Puttaswamy (Retd.) v. Union of India, A.I.R. 2017 S.C. 4161 (India).
- Kharak Singh v. State of U.P., A.I.R. 1963 S.C. 1295 (India).
- R. Rajagopal v. State of Tamil Nadu, A.I.R. 1995 S.C. 264 (India).
- Mr. X v. Hospital Z, A.I.R. 1999 S.C. 495 (India).

CONTENTS

CHAPTER 1

INTRODUCTION

Data privacy has become a critical problem in today's digital world as more businesses and customers rely on online platforms for transactions, communication, and services. Data protection entails safeguarding information from unwanted access. Security of information is typically the main goal of data protection, which can include encryption, methods for confidential communication, quantifiable security measures and hence the aim of data protection is safety and security[1]. The legal and technological safeguards intended to prevent sensitive and personal data from being accessed, misused, or compromised are collectively referred to as data protection. Strong data protection measures are crucial to preserving trust, security, and legal compliance in the face of the exponential expansion of e-commerce, which involves the daily collection, storing, and processing of enormous volumes of consumer data.

E-commerce is the sale or procurement of goods or services using computer networks using mechanisms created especially for order placement or receipt.[2]As the exchange of services happens over internet it carries an associated risk on data protection and security risk. Business ecommerce sales grew by nearly 60% from 2016 to $27 trillion in 2022.[3]Therefore it is clear that the use of e commerce platforms have raised significantly in the recent years. In international trade or cross border trade, data flows through e commerce sites across borders have raised concerns about privacy and security[4]

Personal data means the information that pertains to a person who is identifiable[5]. The processing of personal data helps the companies and government to comprehend individual preferences that can be used for personalised customisation, advertising etc.

---

[1] Dave Brunswick, *Data Privacy, Data Protection and the Importance of Integration for GDPR Compliance*, ISACA J., Vol. 1 (2019), https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-1/data-privacy-data-protection-and-the-importance-of-integration-for-gdpr-compliance_joa_eng_0119.pdf.

[2]OECD, *Unpacking E-Commerce: Business Models, Trends and Policies* (OECD Publishing 2019), https://doi.org/10.1787/23561431-en.

[3] UNCTAD, *Estimates of Business E-Commerce and the Role of Online Platforms* (2024).

[4] OECD, *Recommendation on Consumer Protection in E-commerce* (OECD 2016).

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 4(1).

But if not regulated the processing of personal data can have negative consequences on individual's privacy which is a fundamental right. It could also cause financial losses, damages to reputation etc. Such incidents calls for stricter regulatory measures for the protection of data security and privacy of the information shared through the e commerce sites. Even Digital identities pose certain drawbacks, particularly for buyers. Privacy issues and lack of control of personal data may be exacerbated by digital identity schemes, which could share personal information with ecommerce sites[6] . In this scenario, it was very essential for a legislation to deal with personal data protection.

One of the major ways through which data breach happens is through e commerce websites. India was identified as one of the top five nations impacted by cybercrime, according to a 2022 October report by online security firm "Symantec Corp".[7]The data breach which happens through e commerce sites have a negative impact on the customers and it adversely affects the trade. India also faces severe data breach cases. According to the 2023 Annual Data Breach Report, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).[8] To offer individualized shopping experiences, make product recommendations, expedite payment procedures, and improve marketing tactics, e-commerce platforms like Amazon, Alibaba, eBay, Flipkart, and Shopify mostly rely on data collection. The following categories of data are gathered in e-commerce:

- Name, email, phone number, and address are examples of personal information.
- Financial Information like transaction history, credit/debit card information.
- Behavioural Data such as searches, past purchases, and browsing habits.
- Location Information like geolocation tracking and IP addresses.

[6] Supra note 2
[7] NITI Aayog, Cyber Security Conclave at Vigyan Bhawan, New Delhi (2019), https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.
[8] Identity Theft Resource Center, 2023 Annual Data Breach Report Reveals Record Number of Compromises-72 Percent Increase over Previous High (Jan. 25, 2024), https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/.

However, if not handled correctly, it may also create privacy concerns. Consumers could face the dangers of fraud, identity theft, and financial losses resulting from unauthorized access, data breaches, and unethical sharing of information.

Strict data privacy rules have been enacted by governments all around the world to control how companies handle personal information. The goal of laws like the Nigeria Data Protection Regulation (NDPR), the California Consumer Privacy Act (CCPA) in the US, and the General Data Protection Regulation (GDPR) in the EU is to make sure businesses manage customer data in an ethical and open manner. Serious fines, legal action, and reputational harm may result from breaking these rules.

To address this stricter regulations was necessary. Earlier in India there was only Information Technology Act, 2000. Recently in 2023 the Digital personal data protection act was passed in 2023. But the act is alleged to have certain shortcomings with respect to promotion of e commerce. All these calls for revitalising the legal measures in India regarding the data breach and privacy issues in e commerce sites without hindering the growth of e commerce.

1.1 LITERATURE REVIEW

The article "Balancing privacy and accountability: a closer look at India's DPDP act of 2023"[9] analyses DPDP act and the growing concerns over data privacy and security. It outlines the key provisions like consent, data fiduciaries. It also discusses the merits and the probable shortcomings of the act. The article highlights important clauses such as user consent, data localization, data fiduciaries' responsibilities, and sanctions for noncompliance. It also looks at issues with government exemptions, possible effects on enterprises, and enforcement difficulties.

The article "India's new data frontier; a critical legal insight of the personal data protection act, 2023"[10], analyses that the data protection act is essential to safeguard individual privacy and to ensure responsible data handling. It gave an insight to the act and the privacy concerns and business. The articles also identifies certain shortcomings of the act especially on right to information etc.

[9]Patial, Tushar & Gupta, Aashi, Balancing Privacy and Accountability: A Closer Look at India's DPDP Act of 2023, 6 *Indian J. L. & Legal Research* 6709 (2023).
[10]Kumar Abhishek, Deep Prabhat, Raghuvanshi Shivam & Kumar Vivek, India's New Data Frontier: A Critical Legal Insight of the Personal Data Protection Act, 2023, 44 *Library Progress Int'l* 3 (2024).

The article "Advancement of technology, lack of privacy: pre requisite of the digital personal data protection act, 2023 "[11]examines how the violations brought by technological advancements prompted the passage of DPDP act. With the increase use of internet we use technology for social media, online shopping, web browsing, cloud storage of personal data, and other activities, we leave digital trails behind. The article explains the salient points of the DPDP Act and the threats and shortcomings it pose on the technological field.

The book "Data privacy law: An International perspective", by Lee A Bygrave deals with the data privacy laws and codes of the world. It analyse the aims and scope of the data privacy laws their basic principles governing them etc. from an international perspective.It also deals with the various initiatives by international cooperations like OECD, UN, EU etc.[12]

The article "Data Breach Disclosure Laws Reduce Identity Theft?" by Sasha Romanosky, Rahul Telang and Alessandro Acquisti, deals with the goals, requirements of data breach laws, whether they are successful and the debate on it especially in US. The authors begin by contextualizing the issue of identity theft, which resulted in significant financial losses estimated at $56 billion in 2005 alone. It underscores the need for a multifaceted approach to address identity theft comprehensively, combining legislative measures with enhanced corporate responsibility and consumer education initiatives.[13]

In the article "Privacy, E-Commerce, and Data Security" by W. Gregory Voss, Katherine Woodcock, David Dumont, Nicholas D. Wells, Jonathan I. Exor, João Luís Traça, Bernardo Embry and Fatima Khan, authors systematically analyse various legislative changes and regulatory frameworks that emerged in 2012, focusing on how these changes impact businesses and consumers engaged in e-commerce. The article also addresses consumer protection issues arising from e-commerce practices. It outlines how legal frameworks are evolving to better safeguard consumer rights in

[11] CA Shagun Kabra and Ms. Khyati Lad, Advancement of Technology, Lack of Privacy: Pre-Requisite of the Digital Personal Data Protection Act, 2023.
[12] Bygrave, Lee A., *Data Privacy Law: An International Perspective* (Oxford University Press 2014).
[13] Sasha Romanosky, Rahul Telang and Alessandro Acquisti, *Data Breach Disclosure Laws Reduce Identity Theft?*, JPAM, 30(2), 256-286,(2011)

online transactions, particularly concerning identity theft and unauthorized data access.[14]

1.2 STATEMENT OF PROBLEM

Data security and privacy is one of the challenging issues that the world face today because of the rise in the use of internet. E commerce sites are at the risk of data breach. There is a need to comprehensively investigate and address the complex issues arising out of e commerce and the potential risk associated with it on data security and privacy in this information technology era. This study seeks to illuminate these challenges, suggest viable solutions, and enhance the legal framework for safeguarding data security and privacy matters. The dissertation addresses the legislative framework on data security and privacy issues in India and its strengths and weaknesses and need for stringent measures for regulating e commerce sites on data security and privacy. The study analyses the role of the existing legal framework in India and the possible threats the law can impose on the smooth running of ecommerce transactions.

1.3 RESEARCH OBJECTIVES

1. To analyse the key provisions of the existing legislative framework that is not conducive with the growth and expansion of e commerce
2. To examine the current Indian scenario on the conduct and regulation of data privacy and ecommerce.
3. To analyse the universal standards on data protection with the legislative standards in India.
4. To study the strengths and weaknesses of the existing legislative framework and suggest solutions if necessary.

1.4 HYPOTHESIS

"THE CURRENT LAW IN INDIA IS NOT CONDUCIVE FOR THE DEVELOPMENT OF ECOMMERCE AND IS IMBALANCED IN FAVOUR OF DATA SECURITY AND PRIVACY."

1.5 RESEARCH QUESTIONS

[14] W. Gregory Voss, Katherine Woodcock, David Dumont, Nicholas D. Wells, Jonathan I. Exor, João Luís Traça, Bernardo Embry and Fatima Khan, The International Lawyer,46(1), 97-112,(2012)

1. What are the international regulations on protection of data security and privacy and e commerce?
2. What are the key provisions in the Indian legislative framework on data privacy and security which could not be conducive with the growth and expansion of ecommerce?
3. What are the legislations in India dealing with the conduct and regulations of ecommerce and data privacy?
4. Whether there is a need for the change in legislative framework in India to deal with e commerce data privacy and security?

1.6 RESEARCH METHODOLOGY

The study analyses the efficiency of the data protection laws and their strengths and weaknesses in protecting data security and privacy and their implications in conduct of e commerce. The study aims to analyse through a doctrinal approach. In order to effectively analyse the issue, data is collected through both primary and secondary sources.

- Primary sources: General Data Protection Regulation, 2018, IT Act, 2000, DPDP Act, 2023 etc.
- Secondary sources: UNCTAD reports, OECD reports, Journals, articles, websites, newspaper, Government reports etc.

1.7 CHAPTERISATION

Chapter 1 – Introduction

Chapter 2 – History and evolution of data protection laws

Chapter 3 – Global scenario on E commerce

Chapter 4 –International frameworks on data privacy and security

Chapter 5 – Indian legislative framework on data protection and privacy

Chapter 6 – Analysis of the Indian legislation in the light of international regime

Chapter 7 – Suggestions and Conclusion

CHAPTER 2

HISTORY AND EVOLUTION OF DATA PROTECTION LAWS

1. INTRODUCTION

The development of data protection legislation has been influenced by the widespread adoption of technology, the expanding importance of personal data, and the increasing concern about privacy, security, and abuse of information. As concerns over privacy, security, and the potential misuse of data have surfaced, we've seen a significant shift in how we think about and legislate these issues. From early legal debates regarding privacy in the 19th century to the development of robust data protection frameworks in the digital era, the evolution of data protection legislation mirrors the balancing act between individual rights, technological innovation, and regulatory oversight. The advent of computers, the internet, and artificial intelligence (AI) has further underscored the necessity of robust data governance policies. Nations across the globe have come up with different legislations to tackle data privacy, cyber threats, international data flows, and corporate responsibility.

This chapter discusses the history and development of data protection legislation, tracing their development from early privacy ideas to current regulations like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and India's Digital Personal Data Protection (DPDP) Act, 2023. Knowledge of this development sheds light on the global movement toward more severe data protection mechanisms and how they have affected businesses, governments, and individuals.

2. EARLY DEVELOPMENTS OF GLOBAL DATA PROTECTION LAWS

By methodically identifying Jewish communities throughout Europe, the Nazi authority collaborated with International Business Machines (IBM), a private census tabulating corporation, to create a card-sorting system that made it possible to automate human annihilation. After allies won the World War II due to their involvement in gathering and compiling this data, some IBM officials faced legal action following the conflict[15].

[15] Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation* (2001).

This incident was one of the earliest cases of data breach and violation though not in the form as we see today.

Later in the 1960s, when governments found computerized data processing to be a useful tool for cataloguing their populace, privacy became a major topic once more. Many European countries implemented various "data-protection" legislation to prohibit any misuse of such centrally kept information, in remembrance of the Nazis' exploitation of detailed public records during World War II, which made it easy for them to locate the Jewish population of each city they stormed. The rise in credit card usage and, most importantly, the development of the internet have recently reignited interest in privacy protection.[16]

The first piece of privacy legislation in the US is the 4th Amendment to the US Constitution, which was ratified in 1789 and prohibits the government from unlawfully searching or seizing someone's property. The 4th Amendment established the fundamental idea that people's property belonged to them and could not be altered without their consent, even if it had nothing to do with data as we currently understand it.[17]

Another notable event in the realm of data protection and privacy laws was a book by Samuel Warren. As far back as the 19th century, when Samuel Warren and Louis Brandeis wrote the landmark paper "The Right to Privacy", individuals were worried about privacy. This was largely because of the invention of modern photography and the printing press. Most individuals today conceive of privacy as "the right to choose what personal data about me is known to whom," although Brandeis had characterized it as "the right to be let alone" (objecting to intrusive journalists who would photograph individuals without their consent; in the past, one had to remain stationary for a considerable period of time, or else the photograph would be all blurred).[18]

3. EVOLUTION OF GLOBAL DATA PROTECTION LAWS

3.1 UDHR, 1948

[16] Marc Langheinrich, Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems, Distributed Systems Group, Institute of Information Systems, IFW Swiss Federal Institute of Technology, ETH Zurich, 8092 Zurich, Switzerland, www.inf.ethz.ch/~langhein/ (last visited Apr. 7, 2025).
[17] https://www.skyflow.com/post/a-brief-history-of-data-privacy-and-what-lies-ahead
[18] Supra note 16

Article 12 of the UDHR mentioned right to privacy. The significance of this article is that it is the foundation of the privacy laws which prohibits arbitrary interference to one's dignity and reputation[19]. This article reinforces the significance of privacy as an inherent human right, safeguarding individuals against unauthorized intrusions in their private life and communications. It sets up that all human beings are guaranteed legal protection from such interference with their personal autonomy and dignity being upheld.

3.2 Freedom of information act, (FOIA) 1967

It is one of the earlier landmark legislations of US which laid down the basic principles related to the right to privacy. The aspects that are covered under the act are right to access, mandatory disclosure, consideration on the basis of public interest. It mainly focused on the right to access to the public documents of the federal agencies.[20]

3.3 OECD guidelines on data protection, 1980

The OECD Guidelines pertaining to the Protection of Privacy and Trans border Flows of Personal Data, agreed upon on 23 September 1980, remain an example of international consensus for general recommendations relating to collection and personal data handling. By establishing fundamental principles, the Guidelines are instrumental in helping governments, business and consumer representatives in their work to safeguard privacy and personal data, and to avoid unnecessary limitations to trans-border data flows, both on and off line. The culmination of two decades of experience and knowledge embodied among OECD government officials, business and industry, and civil society members, this publication contains the tools that serve as the foundation for privacy protection on an international scale, the 1980 OECD Privacy Guidelines, the 1985 Declaration on trans-border Data Flows and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks.[21]

---

[19] Universal Declaration of Human Rights, art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).

[20] "Freedom of Information Act (FOIA)," U.S. Department of Justice, https://www.foia.gov/about.html (last visited Apr. 24, 2025).

[21]OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, OECD (2013),https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.

3.4 Data Protection Convention (Treaty 108), 1981[22]

In the field of automated processing this convention holds immense relevance. Adopted on January 28, 1981. The convention provides basic principles for the protection of personal data, and it recognizes the right to privacy as a fundamental component of human dignity. It seeks to ensure that people are in charge of their personal information.it is one of the pioneer effort in the international data protection law regime.

3.5 European Data Protection Directive, 1995[23]

The European Data Protection Directive, adopted on October 24, 1995, was a landmark legal framework enacted by the European Union to control the processing of personal data and facilitate its free movement within the member states. It set personal data broadly and put duties on data controllers to process data openly, in a fair way, and for lawful purposes while ensuring people's rights to access, correct, and erase their data. The directive prioritized the protection of sensitive data[24] and required cross-border transfers to be subject to proper privacy protections in the recipient nations. Although it harmonized data protection legislation throughout the EU, it was criticized for having uneven enforcement between member states. In the end, the directive set the stage for contemporary privacy law and was superseded by the General Data Protection Regulation (GDPR) in 2018, which further enhanced the rights of the individual and accountability in data processing.

3.6 Sectoral legislations of US- HIPAA

Then in 1996 the Health Insurance Portability and Security Act (HIPAA) was enacted in the United States to streamline and also lawfully protect an individual's health information further. This Law has undergone numerous amendments and additions to it in the years after its enactment. Apart from HIPAA there were many legislations for states like CCPA in US unlike a comprehensive rule in EU. Then in 1998 the Data Privacy Act was enacted by the European Union which worked towards regulating the movement of personal data within the EU and also for data moving out of the EU.[25]

---

[22]Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, Jan. 28, 1981.
[23] Directive 95/46/EC, 1995 O.J. (L 281) 31
[24] Directive 95/46/EC, 1995 O.J. (L 281) 31, art. 8.
[25]"History of Data Privacy Laws," Accountable HQ, https://www.accountablehq.com/post/history-of-data-privacy-laws (last visited Apr. 24, 2025).

3.7 Directive on Privacy and Electronic Communications, 2002[26]

The ePrivacy Directive was adopted by the European Union on 12 July 2002 in order to frame privacy and data protection within the electronic communications area. This directive is supplementary to the previous Data Protection Directive and addresses a number of priority areas, such as the secrecy of communications, handling of traffic data, unwanted communications (spam), and cookie usage. One of its most notable provisions is the need for consent from users prior to the storage or collection of data from their devices, specifically on cookies. It requires that electronic communications services should provide security for information and notify users of risks. The directive also introduces an opt-in system for unsolicited marketing communications, such that companies should first get consent before contacting individuals through email, SMS, or other electronic communications. Amendments in 2009 further tightened controls over cookies and privacy safeguards. The ePrivacy Directive is designed to improve user privacy in the internet age and will be replaced by a more overarching ePrivacy Regulation that harmonizes with the General Data Protection Regulation (GDPR) to counter contemporary technological issues.

3.8 EU Electronic Communications Regulations, 2009

In the marketing and sales campaigns, the European Union's communications regulations of 2009 was an untouchable edge.

3.9 The General Data Protection Regulation (GDPR),2016

Approved by the EU parliament after 4 years of discussions in the year 2016. In the year 2018 GDPR was enforced, replacing the Data Protection Act. The GDPR mandates protections to adhere to data. Businesses that collect personal data need to screen third party service providers and place contractual restrictions on data usage. Consequently, the GDPR has spread way beyond first parties, to numerous third parties involved in some form of data services. Any large multinationals need GDPR compliance, therefore, an awesome number of service providers to such businesses need to enter contractual promises on data usage, security, breach notification, and data preservation.

[26] Directive 2002/58/EC, 2002 O.J. (L 201) 37.

These providers of services view obligations to implement the GDPR as economic coercion imposed by their business partners instead of government coercion.[27]

3.10 CCPA (California Consumer Privacy Act), 2018

In 2018, California passed the CCPA, becoming the first U.S. state with comprehensive consumer privacy rights. It granted residents rights such as accessing, deleting, and opting out of the sale of their personal data. The California Consumer Privacy Act (CCPA), signed into law in 2018 and taking effect from January 1, 2020, is an all-encompassing privacy legislation aimed at strengthening the privacy rights of Californians. The law provides consumers with a number of rights in their personal data, such as the right to know what information is being gathered about them, how it is being used, and with whom it is being shared. Further, consumers are allowed to have their personal data erased and opt-out of its sale to third parties. CCPA is applicable to for-profit businesses that meet or exceed certain criteria, including exceeding $25 million in yearly revenue or handling information of over 100,000 consumers.[28] Clear notices regarding the practices of businesses concerning data need to be made, and channels of exercising the rights of consumers must be instituted. The legislation also contains provisions for safeguarding sensitive personal data and requires non-discrimination against consumers exercising their CCPA rights.

Today, the realm of the data protection laws have widened as a result of the advancement in technology like Artificial Intelligence (AI) and newer forms of hacking and computer attacks.

4. EVOLUTION OF INDIAN LAWS ON DATA PROTECTION

4.1 TIMELINE

- A P Shah committee,2012

The former Planning Commission formed an Expert Committee on Privacy in 2011 with Justice A.P. Shah as its chairman. The committee's duties included "identifying privacy issues, studying privacy laws in various countries, and preparing a report with

[27] Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z., The European Union General Data Protection Regulation: What It Is and What It Means, 28 Info. & Commc'ns Tech. L. 65 (2019)
[28] California Civil Code S. 1798.140(d)

specific suggestions to facilitate authoring of the Privacy bill."[29] The committee also recommended some principles that need to be included in the privacy bill

The committee considered the contextual nature of the concept of privacy and recommended that, as the concept of privacy is constantly changing based on context, societal norms, and emerging technology, the Privacy Act should be technology and sector neutral. Because of the dynamic nature of privacy, the Privacy Act should create a right to privacy that is applicable to all situations and does not require that a 'reasonable expectation' be present, for the right to be evoked. This is to ensure that when seeking redress, the individual is not required to prove that he/she had a 'reasonable expectation of privacy' before being awarded remedy.[30]

- Justice K S Puttuswamy case, 2017[31]

The Court ruled that human dignity includes the right to privacy. The freedom to govern important parts of one's life and make personal decisions is protected by the right to privacy. It also stated that a person's sexual orientation and other private matters, like as marriage, having children, and family, are fundamental to their dignity.The Court noted that Article 21 is the primary source of the right to privacy. The principles contained in other fundamental rights, however, also serve to reinforce it. As a result, it promoted a comprehensive understanding of fundamental rights.

- Draft Personal Data Protection (PDP) Bill, 2018

In 2018, the Draft Personal Data Protection (PDP) Bill, 2018 was submitted by the Justice B. N. Srikrishna Committee, establishing the framework for data protection in India.

- Joint Parliamentary Committee (JPC)

Following the introduction of the Personal Data Protection (PDP) Bill in the Lok Sabha in 2019, a Joint Parliamentary Committee (JPC) was established to examine its contents.

- Draft Data Protection Bill,2021

After carefully reviewing and proposing changes, the Joint Parliamentary Committee released its updated draft of the Data Protection Bill in 2021.

- Withdrawal of PDP Bill

---

[29] Press Information Bureau, https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503 (last visited Apr. 24, 2025).

[30] *id*

[31] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.

The PDP Bill was withdrawn from Parliament in August 2022 after the government chose to revise the law in response to stakeholder complaints.

- Draft Digital Personal Data Protection (DPDP) Bill

In November 2022, the government posted the Draft Digital Personal Data Protection (DPDP) Bill for public comment, asking input from professionals, businesses, and the general public.

- DPDP Act, 2023

Ultimately, the DPDP Bill became an official legislation governing data protection in India in August 2023 after passing both houses of Parliament and receiving the president's assent.

4.2 K S Puttuswamy V. Union of India[32]

Digital services proliferated in India as a result of the telecom revolution that began in the late 1990s and the expansion of the country's IT sector.[33] One of the landmark judgment in the evolution of the data protection laws in India, the judgment was rendered in the year 2017. The constitutionality of Aadhar was contested by twenty-two petitioners. The primary petitioner, retired judge K. S. Puttaswamy, 91, challenged the requirement that individuals acquire an Aadhar number in order to buy grains from the public distribution system and obtain cooking gas. The need that children have an Aadhar number in order to get free school meals was contested by several petitioners, including children's rights activist Shanta Sinha.

The Supreme Court of India, in a unanimous verdict, held that the Right to Privacy is a fundamental right enshrined under Article 21 (Right to Life and Personal Liberty) and other clauses of the Indian Constitution. The Court held that privacy is an integral component of human dignity, autonomy, and liberty, and any invasion must satisfy the test of reasonableness, necessity, and proportionality.[34] K.S. Puttaswamy case is particularly noteworthy because of this judicial imagination of privacy, which is crucial to both an individual's right to self-determination and the survival of a constitutional

[32] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
[33]Anirudh Burman, *The Growth of Privacy Regulation and the Bill*, in *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?* (Carnegie Endowment for International Peace, 2020),https://carnegieendowment.org/2020/07/06/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-82217.
[34] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.

democracy. Given its capacity to alter the fabric of India, K.S. Puttaswamy's case is unquestionably India's identity judgment[35]

However, the right to privacy is not an "absolute right," as the Supreme Court has made clear, like the majority of other fundamental rights. Competing governmental and private interests may take precedence over an individual's privacy interests, provided that specific requirements and standards are met. The standards established by the Supreme Court in the Puttaswamy case, which will be used to assess privacy violations moving forward, are covered in this piece. According to this analysis, the majority of the judges in this ruling concur that future tests of privacy violations will be conducted using the European proportionality criteria. [36]

4.3 Justice B.N. Srikrishna Committee and PDP Bill

India's swift digital transition raised issues with data security, privacy, and misuse, making a robust legal framework for data protection necessary. In response, the Indian government established the Justice B.N. Srikrishna Committee in 2017 to create a thorough framework for data protection that would strike a balance between corporate interests, national security concerns, and individual privacy rights. In July 2018, the committee, led by Justice B.N. Srikrishna, filed the draft Personal Data Protection (PDP) Bill, 2018 and its report, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians."

The committee's recommendations greatly impacted India's approach to data governance, privacy rights, and regulatory enforcement, and they served as the foundation for the country's Digital Personal Data Protection (DPDP) Act, 2023.

4.4 Objectives of the Committee

The committee's objectives included:

- Evaluating India's need for a framework for data protection.
- Juggling privacy issues with advancements in technology and the economy.
- Defining people's rights with relation to personal information.

---

[35] Menaka Guruswamy, *Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors*, Writ Petition (Civil) No. 494 of 2012, The American Journal of International Law, Oct. 2017, at 994-1000.

[36] Bhandari, V., Kak, A., Parsheera, S., & Rahman, F., An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict, IndraStra Global, 11, 1-5 (2017), https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2.

- Creating a regulatory framework to monitor data protection legislation.
- Addressing issues with national security and data localization.
- Ensuring adherence to the Supreme Court's historic ruling in Justice K.S. Puttaswamy v. Union of India (2017), which maintained the right to privacy as a fundamental right guaranteed by Article 21 of the Indian Constitution.

4.5 Recommendations Put Forward

1. Enhancing Privacy Rights and Data Protection[37]

Individual privacy rights should be given top priority in India's data protection system by guaranteeing robust legal protections. Unambiguous provisions pertaining to user consent, data access, rectification, and erasure should be part of the right to privacy. People should also be able to request the deletion of their personal data when it is no longer needed and to opt out of needless data collecting

2. Creating an Independent and Robust Data Protection Authority (DPA)[38]

The Committee advised the creation of an independent Data Protection Authority (DPA) to enforce compliance and facilitate effective implementation of the data protection regime. The DPA would oversee complaints, investigate, impose penalties, and facilitate public awareness regarding data privacy rights.

3. Putting Tighter Data Localization Measures in Place

The Committee recommended localization of personal data and suggested that a minimum of one copy of the data be retained within India so that there would be greater control and governance over the data. Specifically, sensitive personal data was to be processed and stored only within Indian Territory, limiting its transfer outside borders.

4. Improving Data Fiduciaries' Accountability and Transparency[39]

Organizations and businesses that gather personal information ought to be held to high standards of accountability. They must guarantee user-friendly privacy policies, purpose limitation, and data reduction. To identify possible dangers and stop the misuse of customer data, regular audits, risk assessments, and privacy impact reports ought to be required.

---

[37] PRS Legislative Research, Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy (last visited Apr. 24, 2025).
[38] id
[39] ELP, Discussion Paper: Justice B.N. Srikrishna Committee – Data Protection, https://elplaw.in/wp-content/uploads/2023/09/ELP-Discussion-Paper-Justice-BN-Srikrishna-Committee-Data-Protection-2.pdf (last visited Apr. 24, 2025).

5. Enhancing Consent Procedures for Gathering and Processing Data[40]

The report focused on a consent-based data processing approach, under which individuals need to give clear, explicit, and informed consent before their data gets collected or processed. It also suggested individuals being given a number of rights on their data, such as the right to access, correction, erasure, portability, and the right to be forgotten, giving them the ability to take charge of their personal data.

6. Applying Strict Sanctions for Data Violations

To achieve compliance, organizations who fail to protect user data should be subject to severe fines. To ensure that businesses and government organizations continue to be held accountable, the penalty structure ought to be commensurate with the extent of the data breach. Victims of data breaches should have a well-defined compensation plan that offers both monetary assistance and legal options.

7. Limiting Surveillance Methods and Government Exemptions

Although certain access to personal data is necessary for national security and law enforcement, these exceptions should be well-defined and subject to court review. The fundamental rights of citizens could be undermined by widespread surveillance and privacy abuses resulting from unfettered government access to private data. It is necessary to implement an open review process to keep an eye on how the government gathers data.

8. Responsibilities of Data Fiduciaries

Data fiduciaries, organizations that decide on the purposes of data processing, were encouraged to apply privacy by design to their systems and processes. They would also be mandated to perform Data Protection Impact Assessments (DPIAs) for high-risk data processing operations and to have Data Protection Officers (DPOs) in place to meet the data protection law.

9. Bringing India's Data Protection Laws into Compliance with International Guidelines[41]

To guarantee cross-border data interoperability and seamless commercial operations, India should align its data protection regulations with international frameworks such as the California Civil Code and the EU's GDPR. Adopting global best practices will help

[40] id

[41] PRS Legislative Research, Legislative Brief: The Digital Personal Data Protection Bill, 2023, https://prsindia.org/billtrack/prs-products/prs-legislative-brief-3399 (last visited Apr. 24, 2025).

promote foreign investments in the tech sector and improve India's standing as a reliable digital economy.

The committee's impact on the 2023 Digital Personal Data Protection (DPDP) Act was one of its most important results. The committee's suggestions had a significant impact on public opinion, sparked legislation, and increased awareness of data privacy. The DPDP Act, 2023, however, contained a number of changes, leniencies, and omissions, especially with regard to government exemptions, data localization, and regulatory authorities, even if it was based on the committee's recommendations.

5. CHANGES BROUGHT IN THE DPDP ACT, 2023 COMPARED TO THE COMMITTEE'S RECOMMENDATIONS

Though the Sri Krishna committee was the precursor to the DPDP Act, the act has incorporated some changes to it. Some key changes are:

1. Need for Data Localization

The Srikrishna Committee fervently supported mandatory data localization, mandating that sensitive and important personal data stay inside Indian borders and that at least one copy of all personal data be kept there. This suggestion sought to improve regulatory oversight, deter foreign spying, and fortify national security.

However, by permitting cross-border data transfers[42] to specific approved nations, the DPDP Act, 2023, greatly relaxed this barrier. This modification was introduced to lessen the burden of compliance on companies and to help India's aspirations for international digital trade. Although this facilitates data processing for global firms, it raises questions about India's capacity to adequately control and safeguard personal data.

2. Government Monitoring and Exemptions

The committee recommended that any surveillance operations be proportionate, transparent, and subject to monitoring, underscoring the necessity of stringent

[42] Digital Personal Data Protection Act, 2023, S. 16 (India).

limitations on government access to personal data. It made the case that government organizations shouldn't be granted complete exemptions from data protection laws. [43]

The DPDP Act of 2023, however, gives the government extensive exemptions that let it to process personal data without consent for research, law enforcement, and national security reasons. Furthermore, the act's weak control of government data processing raises questions about possible invasions of privacy and widespread surveillance.

3. The Data Protection Authority's (DPA) function and authority

The creation of an independent Data Protection Authority (DPA) with robust regulatory and enforcement capabilities was suggested by the Srikrishna Committee. This power was supposed to be in charge of looking into data breaches, making sure that compliance was maintained, and punishing offenders.[44]

By restricting the authority of the Data Protection Board of India (DPBI), which took the place of the originally envisaged DPA, the DPDP Act, 2023, on the other hand, erodes the regulatory framework. There are questions regarding the DPBI's independence and efficacy in implementing data protection rules because the government still has considerable control over the organization's makeup, operations, and decision-making procedures.

4. Mechanisms for Consent and User Rights

Strong user rights, such as the rights to access, correction, data portability, and forgetting, were highlighted by the committee. In order to gather and process data, it suggested that consent be explicit, informed, and revocable.

Although permission is still a key principle, the DPDP Act of 2023 gives government organizations more extensive exemptions that let them to process data without consent in some circumstances.[45] Furthermore, user's control over their personal information is

[43]Internet Freedom Foundation, Comparing the 2019 Personal Data Protection Bill with the 2022 Draft Bill, https://internetfreedom.in/comparing-pdpb/ (last visited Apr. 24, 2025).
[44] id
[45] Saikrishna & Associates, The Digital Personal Data Protection Act, 2023: India's Data Protection Law, https://www.saikrishnaassociates.com/the-digital-personal-data-protection-act-2023-indias-data-protection-law/?__cf_chl_tk=TeC_1jw88Lqf1fJ8LiATHJ8nQhGjTJS0KOsTcGw4szo-1745474669-1.0.1.1-aeomVjxA0YzkO4PIN8wJFULNY7auFHSHEtfAHjTbdfs (last visited Apr. 24, 2025).

limited by the DPDP Act's conspicuous lack of the Right to Data Portability and the limited scope of Right to be forgotten.

5. Tougher Repercussions for Data Violations

To guarantee strict enforcement and accountability, the Sri krishna Committee suggested severe sanctions for non-compliance, data breaches, and unauthorized data sharing. To discourage companies from treating personal data improperly, the penalties were made to be commensurate with the seriousness of the infraction.

Penalties for infractions are included in the DPDP Act, 2023, although enforcement is still unclear because of the Data Protection Board's limited authority. Concerns over how those impacted by data breaches can seek recourse are also raised by the lack of robust consumer compensation procedures.

6. Harmonizing Economic Growth, Innovation, and Privacy

By permitting companies to handle data responsibly and guaranteeing robust user rights, the committee sought to strike a balance between privacy protection and innovation. Additionally, it urged businesses to put strong data security frameworks in place and supported privacy-by-design principles.

Startups and international corporations will find it easier to comply with the DPDP Act, 2023, which adopts a more business-friendly approach. However, the act has come under fire for putting corporate interests before of individual privacy rights by easing data localization regulations and extending government exemptions

6. CONCLUSION

The evolution of data protection laws reflects the increasing need to safeguard personal data in an era of rapid technological advancements. From early privacy discussions in the 19th century to the enactment of comprehensive legal frameworks like GDPR, CCPA, and the DPDP Act, 2023, data protection has become a crucial aspect of modern governance. The transformation from fundamental privacy norms to intricate regulatory schemes reflects increased awareness of private rights, corporate accountability, and national security interests. As continued digitalization, AI, and international data flows accelerate, stronger and responsive data protection legislations will increasingly

become essential. Going forward, policymakers need to ensure that data protection laws balance innovation, economic development, and the inherent right to privacy, providing a secure and open digital environment for businesses and individuals.

CHAPTER 3

GLOBAL SCENARIO ON E-COMMERCE

3.1 INTRODUCTION

E commerce or electronic commerce is the conduct of business through the internet. There are many models which deals with the ecommerce transactions. E-commerce takes place through a range of different commercial relationships, involving any possible pairing of consumers (C), businesses (B) or governments (G). These include classical B2B transactions, which still account for the lion's share of turnover resulting from private sector e-commerce, as well as business-to-government (B2G) transactions like government procurements. E-commerce transactions increasingly involve consumers directly, most notably business-to-consumer (B2C) transactions. Additionally, emerging business models involve consumer-to-business (C2B) and peer to-peer relationships, which take place between two or more individuals.[46] In the retail industry, e-commerce has undoubtedly had a significant impact on demand supply chain, market structure and autonomy, and technology. The growth of e-commerce and its impacts on different retail industries have been extensively studied in the economics literature. No one will be surprised to learn that, with 79.6 percent of 2013 sales performed online, the music and video sector has the highest percentage of e-commerce in the data. On online retail platforms, books and magazines accounted for 44.2 percent of sales, while computer hardware and software accounted for 32.9 percent and games for 28.8 percent.[47]E commerce is not confined to buying and selling of physical goods but also include the goods and services of entertainment value and comfort.

3.2. EVOLUTION OF E COMMERCE

The term e commerce was coined by Robert Jacobson who was a principal consultant at the California State Assembly's Utilities & Commerce Committee.in the year 1984. Ecommerce is an umbrella term which includes buying selling, fund transfer etc. associated with a transaction's commerce has undergone significant transformation especially after the advent of the technology.

[46] OECD, *Unpacking E-Commerce: Business Models, Trends and Policies* (OECD Publishing 2019), https://doi.org/10.1787/23561431-en.
[47] Hortaçsu, Ali & Syverson, Chad, The Ongoing Evolution of US Retail: A Format Tug-of-War, 29 J. Econ. Persp. 89 (2015).

The concept of electronic transfer and transactions has emerged during the 1960s after the development of electronic data interchange. It was a method of data transfer across through electronic mode. It was primarily used by the business entities and was a revolutionary measure towards digitalising business transactions

The first ever technology was considered to be CompuServe which was founded in Columbus Byrd. John R. Goltz and Jeffrey Wilkins. It initially used electronic data interface technology for computer time sharing services and in 1979, it began providing technical support to the personal computers.

The EDI was not an e commerce as we see today but was precursor to the modern e commerce technology.

Online shopping, sometimes known as teleshopping, was created in 1979 by English inventor and businessman Michael Aldrich Offsite Link to facilitate online transactions between customers and companies or between companies. Aldrich's method, which was not commercially feasible until the Internet, was later dubbed e-commerce Offsite Link.[48]

Another major invention was the Boston computer exchange which was the first ecommerce platform developed in US.[49] The company aimed to make a fully automated trade system for the business transactions.

Later in 1992 Charles M. Stack founded Book Stacks Unlimited, which was an online bookstore. Later in 1994, it was transitioned to books.com. Later it was sold to another company due to financial crisis. Still it was a breakthrough invention preceding internet.

Netscape Navigator, the first commercial web browser, was introduced in 1994. It was developed at Netscape Communications Corporation by Marc Andreessen and his colleagues, building on the success of the previous browser, Mosaic, which Andreessen co-created. Netscape Navigator made technology accessible to non-technical users by introducing features like multimedia support and graphical user interfaces. It soon rose to prominence as one of the most widely used browsers at the time, greatly assisting in the early development of the World Wide Web.

---

[48] "The rise of ecommerce history of information" https://www.historyofinformation.com/detail.php?entryid=4528 (last visited Apr. 24, 2025).

[49] *The Evolution of E-Commerce: Analysis from Its Origins to Today*, https://www.42signals.com/blog/the-evolution-of-e-commerce-analysis-from-its-origins-to-today/ (last visited Apr. 24, 2025).

Then was the greatest invention in the history of ecommerce amazon by Jeff Bezos and e bay. Amazon was store as a book store alter expanded to trade in almost all essential things.

The ecommerce marketplace success stories include eBay, an online auction site that debuted in 1995, and Etsy, which launched in 2005 and by 2019 saw gross merchandise sales total $4.97 billion globally. [50]

3.3. KEY PROMOTERS AND TRENDS OF E COMMERCE

3.3.1 Internet

Internet was the breakthrough propagate of the ecommerce. Though ecommerce has been in practice years before it was confined only to business practices alone. It is after the internet is being invented the e commerce has entered a new phase. The number of network users exploded with the advent of the World Wide Web and later the expansion of multimedia content. The internet has in turn evolved even quicker than any other previous medium.[51]The expansion of the information and communication technology has catalysed ecommerce by promoting accessibility. It has also helped for the development of ecommerce models like B2C, business to customers and C2C customers to customers from the traditional business to business model (B2B)

3.3.2 Globalisation

Globalisation is said to have emerged during the 90s but the concept was in practice till the time immemorial. The Roman Empire, Silk route, Age of exploration, Rise of MNCs and colonial empires, World wars and the onset of covid 19 all have contributed to the advancement of globalisation. Globalisation has led to the development of the concept of global village where the goods and services that was not accessible easier was made accessible now. For example, Kerala was known for spices and had a large market in European countries. It was considered a symbol of prestige as these were not readily available to the geographical, transportation and accessibility constraints. Now with the concept of global market and global village, the countries began entering into trade contracts and negotiations which accelerated the e commerce technology.

[50]The History of E-Commerce: How Did It All Begin?, https://blog.miva.com/the-history-of-ecommerce-how-did-it-all-begin (last visited Apr. 24, 2025).
[51] Jain, Vipin, Malviya, Bindoo, & Arya, Satyendra, An Overview of Electronic Commerce (e-Commerce), 27 J. Contemp. Issues Bus. & Gov't 1 (2021), https://cibg.org.au/.

Therefore globalisation is one of the driving factor for the advancement of the ecommerce

3.3.3 Online payment gateway

Another factor that paced ecommerce is online payment facilities through debit cards credit cards etc. the advancement in the banking field helped the ecommerce transactions to flourish. Also the shift to digital currency or the digitalisation of currency has led to the increase in the number of ecommerce transactions

3.3.4 Social media platforms

One of the ways in which the ecommerce platforms sell their goods and services is through social media platforms in the form of advertisements, suggestions etc. The virtual platforms where people interact virtually was exploited by the ecommerce companies to make their products reach the target audience. Now the ecommerce has grown in a virtual world in such a way that here are social media accounts that sell their products and accounts that review the products. Hence, social media has now became the market for the retailers. More sales happens over social media than through the official websites nowadays.

3.3.5 Artificial intelligence

The features of the artificial intelligence like personalised shopping, Chabot assistants which provides the necessary guidelines and information , virtual and audio search feature etc. helps the customers to make their shopping experience memorable. Many experts believe that the foundation of the industry's growth is automation and the use of artificial intelligence-powered tools, systems, or algorithms to support operations.[52]

3.3.6 Advent of mobile phones

With the proliferation of mobile phones, the concept of mobile commerce has emerged. The advantage of the m commerce is that it is highly feasible and viable. It can be carried anywhere which means the sales can happen anywhere whether it be in office, home bus, car etc. Also the people can get all the services and goods in their fingertips. They don’t need to visit a showroom or shop a wide range of goods more than that

[52] Sulova, S., A Conceptual Framework for the Technological Advancement of E-Commerce Applications, Businesses 2023, 3, 220–230, https://doi.org/10.3390/businesses3010015.

available in the traditional brick and mortal retailor is available online. As there are a plenty of retailers online, the range of choices that the customers get is wide compared to the local retailer where the choices are limited to that shop alone.

A study finds that consumers perceive m-commerce as a complementary shopping potential than as a substitute for stationary devices and the reason could the experience that the consumers have with respect to m commerce and stationary devices and also the experience is a significant covariate with regard to the evaluation of e-channels.[53]

3.3.7 Personalisation

It is another feature which led to the growth of ecommerce in the recent years. By using cookies, the personalised ads and products reach the targeted audience which further helps people get their product of their choice and the ecommerce company lead their business. Personalisation happens through social mesial like Facebook, Instagram etc. however, the chances of exploitation is also posing a problem along with privacy concerns.by analysing customer behaviours, companies offer products that are well tailored to the customer requirements

3.3.8 e WTP (electronic world trade platform) Concept

The e WTP website established in 2016 and is a multistake holder, private sector-led platform that encourages public-private dialogue to share best practices, cultivate new trade regulations, and foster a more inclusive and integrated business environment and policy to promote global trade. The first hub was set up in Malaysia , kwala lumpur. The primary function of these eWTP e-hubs is to enable digital commerce. A strategically placed logistics centre that serves as a centralized location for customs clearance, warehousing, and fulfilment for the host nation and region and expedites import and export clearance is what distinguishes each hub.[54]

3.4. ADVANTAGES OF ECOMMERCE

3.4.1 Convenience

[53] Schramm-Klein, Hanna & Wagner Gerhard, Broadening the Perspective on E-Commerce: A Comparative Analysis of Mobile Shopping and Traditional Online Shopping, 36 *Marketing: ZFP - Journal of Research and Management* 119 (2014).
[54] Johnston, Lauren A., World Trade, E-Commerce, and COVID-19, 21 *China Review* 65 (2021).

One of the major reasons why people resort to ecommerce over the traditional method is convenience. It is convenient and can be accessed without much effort. Shopping can be done anywhere and at any time.

3.4.2 Market reach

This is advantageous to the ecommerce companies where they can reach a lot of people which is not possible in a traditional market where the reach is limited to the local place alone. The advertisements reach a large number of people and also the personalisation helps in providing a tailored products to people of their choice.

3.4.3 Reduced operational cost

Another important feature is the reduced operational cost where there is no need for a physical place where all the products is to be stored. The goods will be stored with the original seller and is shipping to the people as per their requirement. This reduces the operational cost to the entities.

3.4.4 Customer feedback

Most of the ecommerce entities have the facility of feedback where the customer can rate a particular vendor as well as the ecommerce platform. This helps them to improve in the areas where the customers felt necessary

3.4.5 Speedy transactions and time saving

The ecommerce reduces the time and effort required for the shopping. As the payment and shipping happens through the website, the customer can save his time and can enjoy a speedy transactions

3.4.6 Wide choice

Customers can enjoy a variety of choices as the platforms brings together many retailers across the globe. This gives the customers an opportunity to choose from the variety of alternatives available. This is also one of the prominent reason why the customers resort to e commerce.

3.5. CHALLENGES

3.5.1 Dominant online platforms

Some platforms have been there in the internet centuries before. These usually have an upper hand over the digital domain. In fact, the manner that powerful internet platforms now pose a threat to market distortion and competition is not wholly new. The issue stems from a basic difficulty presented by companies that take control of a vital distribution channel or network.[55] The court in a case held that the giants like Facebook, google and other online providers are serving as the "modern public square.[56] The dominant nature of these platforms harm the comparatively newer online platforms that emerged lately.

Another impact of dominant platforms is that it can favour or disfavour a merchant. Some sellers even worry about like discrimination. Some of the ways in which amazon can disfavour a seller is through suspending or shutting down accounts overnight, withholding merchant funds, changing page displays, and throttling or blocking favourable reviews.[57]

Facebook is also a dominant social network. As per the reports, about two-third of Americans use Facebook, among which three-quarters of them use it on a daily basis.[58]Today many other platforms like Instagram twitter etc has also emerged to the status of dominant platforms. These have a huge role in promoting ecommerce across the globe.

3.5.2 Logistics

The base of an ecommerce transaction is he logistics and shipping. Only if the supply chain is active, the transaction can be made effective. The duties freight charges etc. pose a problem of the entities

3.5.3 Payment issues

The issues related with payment portal and banking system soften cause inconvenience to the customers. Also fraudsters target payment portals for committing offences

3.5.4 Covid 19 pandemic

[55]Khan, Lina M., The Separation of Platforms and Commerce, 119 *Columbia L. Rev.* 973 (2019).
[56] Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).
[57] Supra note 51
[58]Smith, Aaron & Anderson, Monica, Pew Research Ctr., *Social Media Use in 2018*, at 2 (2018), https://www.pewinternet.org/wp-content/uploads/sites/9/2018/02/PI_2018.03.01_Social-Media_FINAL.pdf [https://perma.cc/J9EP-4TVZ].

Covid 19 had a significant impact on the ecommerce sector. In fact the world trade has lagged during that period. The inadequate digitization of the global commercial system is one reason why global trade has slowed throughout the pandemic. There were no relevant informational structures in place. It has been decades since international trade governance mechanisms were revised. The fundamental difficulty of coming to an agreement on the necessary reforms to the WTO's mission and scope is at the heart of that lag.[59]

3.5.5 Cybersecurity threats

According to the report prepared by McConnell International, cybercrimes are defines as, "harmful acts committed from or against a computer or network"[60] The various forms of cybercrimes includes identity theft, phishing, vising, smashing, job related frauds, cyber stalking, cyber bullying, sympathy fraud, banking frauds, hacking, virus attacks, spamming, romance fraud etc. The attackers aim at committing fraud at the customers either to get financial advantage or to get the data including personal and financial data of the customers.

3.5.6 Privacy concerns

One of the major concerns among the ecommerce entities is the privacy issues especially the data of the customers. There are many instance where the data of the customers got misused. There are instances where the data breach happened through e commerce sites. Cybercriminals, who can range from lone miscreants to highly skilled state-sponsored organizations, most frequently breach networks to obtain private information. In other situations, they may encrypt the data on a victim's computer and demand payment before the ransom is released and the victim regains access.[61]

In 2020, Tokopedia, one of Indonesia's largest e-commerce platforms, suffered a significant data breach in which the hackers accessed and sold the data of over 91 million users, including emails, hashed passwords, and names. This incident highlights how even large, established e-commerce sites are at risk and this breach severely

[59] Supra note 53
[60] Halder, Debarati & Karuppannan, Jaishankar, *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations* (2012)
[61] https://pmc.ncbi.nlm.nih.gov/articles/PMC6139979/#sec7

impacted user trust, which is crucial for e-commerce platforms, and likely led to financial losses, both directly and indirectly through the loss of customer trust[62]

A major data breach has affected Zivame, a well-known online retailer that sells a variety of women's clothing items. 1.5 million Zivame customers' personal information has been made available for purchase by threat actors. One of the organizations claiming to have the purported data and be willing to sell it for $500 in crypto currency was interviewed by the India Today Open Source Intelligence (OSINT) team.[63]

The e-commerce behemoth Amazon experienced yet another technical issue that impacted its vendors and sellers on its India page. According to the Seattle-based online retailer, on January 8, 2019, a website issue resulted in a data breach that revealed private financial data, including sales, category-by-category split, and inventory data of its vendors and sellers. Amazon, which has about 400,000 online retailers and suppliers nationwide, claimed that the problem was fixed in a few hours, although it is yet unknown how many members were impacted.[64]

In 2019, more than 15 billion data records were exposed, a 284% increase from the year prior.Then, in April 2020, Google reported blocking more than 18 million malware and phishing emails per day related to COVID-19.[65]. All these incidents shows the vulnerability of ecommerce platforms to data breaches and the need for a robust guidelines to regulate data collection nod processing by ecommerce sites so as to control data breaches.

3.5.7 Stringent laws

In the light of rising cybercrimes against the ecommerce websites, countries have made the laws more stringent making it hard for the ecommerce entities to conduct their business. Compliance with the laws which requires high operational cost pose additional cost to the ecommerce entities.

---

[62]Baek, Insights from Tokopedia, *Why Hackers Target E-Commerce*, https://www.linkedin.com/pulse/why-hackers-target-e-commerce-insights-from-tokopedia-baek--ddgoc.

[63]Zivame Data Breach: Leak of Personal Info of Indian Women, *India Today* (May 22, 2023), https://www.indiatoday.in/technology/story/zivame-data-breach-leak-personal-info-indian-women-2382614-2023-05-22.

[64]Amazon India Suffers Data Breach, Sellers' Financial Information Exposed, *CISO MAG*, https://cisomag.com/amazon-india-suffers-data-breach-sellers-financial-information-exposed/.

[65]Big Commerce, Ecommerce Data Breaches: Examples and Statistics, https://www.bigcommerce.com/articles/ecommerce/ecommerce-data breaches/#h2_ecommerce_data_breaches__examples_and_statistics (last visited Apr. 24, 2025)

3.6. LEGAL FRAME WORKS ON ECOMMERCE

3.6.1 UNCITRAL Model Law on Electronic Commerce (1996)

The UNCITRAL model was adopted on 12 June 1996. In order to remove legal barriers and improve legal predictability for electronic commerce, the Model Law on Electronic Commerce (MLEC) gives national legislators a set of internationally recognized guidelines. In addition to developing the legal concepts of non-discrimination, technological neutrality, and functional equivalency, the MLEC also creates guidelines for the creation and legality of contracts made electronically, as well as for the attribution of data messages, acknowledgment of receipt, and establishing the time and location of data message dispatch and receipt.[66]

3.6.2 Digital Services Act (DSA) & Digital Markets Act (DMA) (2022) of European Union

EU laws called the Digital Services Act (DSA)[67] and the Digital Markets Act (DMA)[68] (2022) are designed to make the internet a safer and more equitable place. By placing stringent regulations on very large platforms like Google and Facebook to prevent unlawful content and deceptive advertising, the DSA improves content moderation, consumer protection, and transparency for online platforms. By prohibiting self-preferencing, mandating interoperability such as WhatsApp-iMessage communication, and enabling third-party app stores, the DMA aims to combat monopolistic activities by targeting tech giants (gatekeepers) and promoting fair competition. Enforcement is scheduled to start on 2024, and noncompliance will result in fines of up to 10% of worldwide turnover.

3.6.3 Federal Trade Commission (FTC) Regulations of US

E-commerce in the United States is governed by Federal Trade Commission (FTC) regulations, which enforce data privacy, fair competition, and consumer protection. They maintain transparency in digital marketing while regulating unfair business practices, internet fraud, and deceptive advertising. Important legislation include COPPA, which protects children's online privacy, the CAN-SPAM Act, which regulates commercial emails, and data security rules for companies. The FTC enforces

[66] *UNCITRAL Model Law on Electronic Commerce*, United Nations Commission on International Trade Law, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.
[67] Regulation (EU) 2022/2065, 2022 O.J. (L 277) 1.
[68] Regulation (EU) 2022/1925, 2022 O.J. (L 265) 1.

severe penalties for non-compliance and keeps a close eye on social media advertisements, online marketplaces, and subscription services.

Also the nation controls the marketing and commercial emails by way of the CAN-SPAM act of 2003**.** Also for the protection of children's privacy online, US has adopted Children's Online Privacy Protection Act COPPA, in the year 1998. Therefore the laws of US in ecommerce are sectoral.

3.6.4 Information Technology (IT) Act, 2000, Consumer Protection Act, 2019 and Digital Personal Data Protection Act. 2023 of India

In India e commerce transactions and breaches are addressed by Consumer Protection (E-Commerce) Rules (2020) and consumer protection act 2019. Also the information Technology act, 2000 deals with the offences over computer networks. Recently in the year 2023, Digital Data Protection Act was enacted for the purpose of protection of personal data

3.6.5 Nigeria Data Protection Regulation, NDPR, 2019 of Nigeria

The Nigeria Data Protection Regulation (NDPR) (2019) establishes rules for data collection, processing, and storage in order to protect personal information. It gives people control over their data while requiring businesses to get user consent, protect data, and disclose breaches. It is modelled after the GDPR and applies to companies that handle the data of Nigerian people. Violations will result in sanctions. In Nigeria's digital economy, the National Information Technology Development Agency (NITDA) upholds accountability and privacy while enforcing compliance.

In spite of the above mentioned regulations, there are many laws existing in the nations, which regulates ecommerce transitions and privacy. By analysing the various laws across the globe, firstly, most of the laws on ecommerce are related to data protection and privacy, which is one of the major issue in connection with ecommerce transactions. Secondly, most of the legislations are sectoral and there is no law which deals with all the aspects of ecommerce under a single umbrella.

3.7. CONCLUSION

As online stores continue to grow, they collect masses of personal information, such as consumer habits, payment details, and browsing histories. This information is critical

for personalizing services, improving user experiences, and maximizing marketing efforts. However, the emergence of such data-driven business models has raised widespread alarms over privacy invasions, identity theft, and abuse of personal data. As such, there has been a growing need for sound legal regimes that safeguard consumers' privacy rights as well as their right to expect fair and open data handling processes.

Internationally, the urgency for harmonized data privacy laws has been identified. Nations are struggling to strike a balance between safeguarding individual data while advancing innovation and ensuring cross-border commerce. Whereas some places, like the European Union's General Data Protection Regulation (GDPR), have been proactive in adopting comprehensive data protection legislation, others are at various stages of formulating and enacting their own laws. This disparity of data protection legislations poses critical challenges to business entities that partake in cross-border e-commerce since they are faced with myriad regulatory environments.

The quick development of e-commerce, together with the increased attention to data protection and privacy, calls for an in-depth appreciation of the international standards that control the collection, processing, and transfer of personal data. Such standards are meant to find a balance between the protection of the privacy rights of individuals and facilitating the free flow of data, which is central to international trade and innovation. As we enter the next phase, it is crucial to review these global frameworks on protection and privacy of data, which have developed due to the increasing issues around personal data during the digital era. The examination of current legal frameworks like the EU's GDPR, California Consumer Privacy Act (CCPA) etc and how different regions are tackling the urgent matter of data privacy and what the effects of such regulations have on international e-commerce would help.

It is not only important for businesses to understand these frameworks but also for consumers, as it dictates the manner in which their personal data is protected and how cross-border e-commerce persists under changing legal regimes.

CHAPTER 4

INTERNATIONAL FRAMEWORKS ON DATA PRIVACY AND SECURITY

4.1 INTRODUCTION

In the digital age, data security and privacy have emerged as key concerns for both individuals and businesses. Due to the rapid growth of social media, cloud-based services, and e-commerce, vast amounts of personal data, including names, addresses, financial information, and browsing patterns, are collected, processed, and stored online. It is essential to ensure that this data is handled safely and ethically in order to protect users from identity theft, financial fraud, and unlawful monitoring. As technology and data processing play a greater role in the life of the individual and society, they gain increasing significance in the shaping of the social environment. This potentially makes them an inevitable policy battleground. Accordingly, in a democratic society, participation should play a role in each policy approach, initiative or decision.[69] Public understanding of the legal framework was taken as a solid starting point for consideration of the complex and fluid issues of data protection and privacy.[70]Therefore, it is necessary to know the frameworks related to data privacy and security.

4.2 DATA BREACH AND E COMMERCE

The e-commerce market has undergone significant change due to new business models and rapid digital innovation. Increased Internet and mobile connectivity and the emergence of online marketplaces are important conduits for online transactions between consumers and businesses. Customers in both developed and emerging markets now have access to anything at any time, from any location, including across borders due to these advancements. Consumers have become active market participants driving innovation, competition and economic and social growth. The data is now a valuable and significant economic asset that powers a variety of new business models, technology, and a greater range of cutting-edge products and services that are

[69] Hallinan, Dara, Friedewald, Michael & McCarthy, Paul, Citizens' Perceptions of Data Protection and Privacy in Europe, 28 *Computer L. & Sec. Rev.* 263 (2012).
[70] ibid

reasonably priced.[71]As data is now a valuable asset, the chances of it being stolen or exploited are also high. Ecommerce platforms are one such way in which data breaches are taking place. The perpetrators aim the personal data of the consumers and use them to achieve their profits.

More generally, national and occasionally regional consumer protection laws are put to the test by cross-border e-commerce. International cooperation on consumer enforcement, particularly with regard to product safety and recalls, becomes increasingly crucial.[72]Legal and regulatory ambiguities may arise for businesses engaged in cross-border e-commerce due to the blurring of the lines between goods and services under current bilateral and multilateral trade agreements that rely on regulations based on the conventional differentiation between these two product categories.[73] Lack of a comprehensive framework on data privacy and security and business transactions make the situation vulnerable.

Also the use of internet for purchase and sale increased at a surprising rate. The means by which various businesses and nations use the internet to offer goods and services differs. On average, more than 33% of all firms in OECD nations with ten or more workers use the internet for purchases, and over 17% do the same for sales.[74] In Australia, Canada, Germany, Ireland, New Zealand, and Switzerland, more than half of all firms make purchases online. In Australia, New Zealand, and the UK, about one-third of all firms sell products or services online.[75]Therefore, it is clear that the recent years have witnessed an increase in the e commerce rates not only in a single nation but on a global level.

As data is a significant component of e commerce businesses, the entities store large amount of data for their working. However, if not stored properly, the chances of getting breached are also high. As per the report of Global Cybersecurity Index 2024, on average, legal measures remain a nation's strongest pillar. From data protection to unlawful online activity, more nations have enacted laws identifying and elucidating cybersecurity-related issues. At least in terms of nomenclature, there is indication that

---

[71] *Report on the Implementation of the OECD Recommendation on Consumer Protection in E-commerce 2022*, https://www.oecd.org/legal/oecd-legal-0422-implementation-report-2022.pdf.

[72] OECD, *Unpacking E-Commerce: Business Models, Trends and Policies* (OECD Publishing 2019), https://doi.org/10.1787/23561431-en.

[73] id

[74] OECD, *Electronic Commerce*, in *OECD Science, Technology and Industry Scoreboard 2009* (OECD Publishing 2009), https://doi.org/10.1787/sti_scoreboard-2009-38-en.

[75] *Id.*

these rules and regulations are becoming more harmonized, such as by aligning with international cybercrime treaties or the GDPR. Additionally, many nations are revising or establishing laws that are phrased in language that is neutral to technology, allowing for greater interpretation, flexibility and bringing online and offline obligations and offenses into line.[76] Hence the recent trends shows that the nations are necessarily aware about the impact of data breaches and began to come up with legislative enactments for the protection of the data. But the question arises as to how effective are these laws in curbing data breaches or how these laws are equipped to deal with the dynamic technological advancements?

4.3 IMPACT OF DATA BREACH ON ECOMMERCE

There were many data breach cases reported across the globe. Ecommerce giants like amazon, ebay, alibaba etc were subjected to such breaches. Now think of the potential impact it leave on the ecommerce entities and the years the entities take to recover the goodwill. some of the impacts are:

1. Loss of customer trust

Customers are the strength of an ecommerce platforms. If a data breach happens, the immediate effect is seen on the customer trust. According to a study's findings, businesses that prolong disclosing a data breach are more likely to see a decline in customer trust than those who do so straight away. According to the post-hoc analysis, businesses that reveal a breach as soon as it is discovered may find it simpler to restore pre-breach levels of trust. Withholding information could be viewed as untrustworthy by consumers.[77]

2. Reluctance to use online platforms

29% of the younger and 24% of the senior citizens subjects had shopped at a website that at least once faced a hacking incident. Among the younger subjects, 13% had fallen victim to Internet scams in general and 14% were victims of some form of identity theft. The numbers on the senior citizens side were a little on the higher side i.e19% and 17%, respectively. [78]This would result in reluctance to use the online platforms out of fear or

[76] *Global Cybersecurity Index 2024, 5th Edition*, International Telecommunication Union, ITU Publications.

[77] Muzatko, Steven & Bansal, Gaurav, *Timing of Data Breach Announcement and E-Commerce Trust* (2018), in *MWAIS 2018 Proceedings* 7, http://aisel.aisnet.org/mwais2018/7.

[78] Chakraborty, Rajarshi, Lee, Jaeung, Bagchi-Sen, Sharmistha, Upadhyaya, Shambhu & Rao, H. Raghav, Online Shopping Intention in the Context of Data Breach in Online Retail Stores: An Examination of Older and Younger Adults, 83 *Decision Support Sys.* 47 (2016).

previous experience. Hesitation to use online platforms are also a result of loss of customer trust.

3. Negative response towards the entity

First, consumers react unfavourably to business's gathering and use of their data because they feel harmed. This customer-centric perspective demonstrates how individuals see possible harm as a result of businesses' data management initiatives. Therefore, compared to broad privacy concerns or financial losses, this vulnerability provides a more accurate framework for understanding how customers react to businesses' use of their information.[79]

4. Change in customer behaviour patterns

The concern that their financial and personal information has been stolen, maybe resulting in identity theft and fraudulent actions, is what is causing this lack of confidence. When a breach occurs, consumers may adjust their behaviour right away, cutting back on or stopping their online purchases from the impacted merchants.

This loss of confidence is driven by the fear that their personal and financial information has been compromised, potentially leading to fraudulent activities and identity theft. Consumers may immediately change their behaviour in response to a breach, such as reducing or halting their online shopping activities with the affected retailers. E-commerce consumer trust is the degree to which customers have faith in the security, dependability, and honesty of online transactions as well as the organizations that make them possible. Because it affects consumers' propensity to buy online, divulge personal information, and make transactions, trust is a critical component of e-commerce[80].

5. Customer loyalty

Longitudinal studies suggest that the impact of a data breach extends far beyond the immediate aftermath, with lasting effects on consumer trust and loyalty. Consumers who experience a breach may develop a heightened sense of scepticism and caution when engaging with the affected e-commerce platform, often resulting in a sustained decline in transaction volumes and customer retention rates.[81]

6. Reputational damage

---

[79] Kelly D., Borah, Abhishek & Palmatier, Robert W., Data Privacy: Effects on Customer and Firm Performance, 81 *J. Marketing* 36 (2017), https://doi.org/10.1509/jm.15.0497.

[80] id

[81] Kumari, Mamta, Sinha, Pallav Chandra & Priya, Sannu, The Impact of Data Breaches on Consumer Trust in E-Commerce, 4 *Int'l J. Current Sci.* (IJCSPUB) 1 (2014), available at www.ijcspub.org.

Additionally, the breach may lead to a broader reputational damage that affects not only existing customers but also potential new customers who may be deterred by the negative publicity surrounding the breach. Long-term trust erosion can also manifest in a shift in consumer attitudes towards data security and privacy, with customers becoming more selective and demanding higher security assurances from e-commerce platforms.[82]

4.4 DATA PROTECTION LAWS ACROSS THE GLOBE

The need of privacy and data protection is becoming more widely acknowledged as more and more social and commercial activities take place online. The gathering, use, and disclosure of personal data to third parties without customer's knowledge or consent is equally concerning. Out of 194 nations, 137 have laws in place to provide data and privacy protection. With 61 and 57 percent of countries having implemented such laws, Africa and Asia exhibit varying levels of acceptance. Just 48% of the population lives in the least developed nations.[83] The UNCTAD report shows that 71 % of the countries across the globe has legislations on data protection and privacy, 9% has draft legislations and 15% has no legislation at all. For another 5% the data is not available[84]the results of the studies implies that most of the nations have its own legislations to deal with data security and privacy but still the alarming rise in the number of online frauds and breaches is also raising concern at the same time.

4.4.1. GDPR

The European Data Protection Directive (95/46/EU) has been removed and replaced by the EU General Data Protection Regulation (the "GDPR") (2016/679). It was enacted on May 25, 2018, with the dual goals of modernizing European data protection legislation and achieving greater levels of uniformity throughout the continent as a regulation as opposed to the directive. [85]The scope of GDPR is vast. The wide territorial scope and expanded definitions of personal data ensure that the GDPR will have a

[82] id
[83] *Data Protection and Privacy Legislation Worldwide*, United Nations Conference on Trade and Development (UNCTAD), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
[84] id
[85] Taylor, Mark J. & Paterson, Jeannie Marie, Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection, 16 *Indian J. L. & Tech.* 1 (2020), available at https://repository.nls.ac.in/ijlt/vol16/iss1/4.

significant impact.[86] Businesses and organisations that target the subjects of EU in any of the following forms comes under the purview of GDPR

- Provide goods or services that are accessible to EU citizens, even in the absence of a financial transaction.
- Keeps a watch on EU citizens online conduct

The above would mean that the entities and businesses outside the EU territory would also fall under its jurisdiction if it has any of the above transactions with EU.

Privacy regulations of GDPR apply to any service and company collecting or processing personal data in Europe. Many companies had to adjust their data handling processes, consent forms, and privacy policies to comply with the GDPR's transparency requirements. [87]Instead of Member States having to transpose each and every provision to national law with wide discretion, the GDPR regulates almost all of the questions directly and only leaves exceptional and limited specification powers to member States which then have to always justify any divergence from the aim of a fully harmonised legal frame.[88]For analysing the GDPR provisions with the Indian definitions, it is essential to know the fundamental definitions made by the GDPR for the basic terms like personal data, consent etc. Under GDPR, personal data is defined as "Any information relating to a natural person who can be identified or identified (a "data subject") is called "personal data." A natural person is considered identifiable if they can be identified directly or indirectly, especially by using an identifier like their name, identification number, location, or online identifier, or by one or more characteristics specific to their physical, physiological, genetic, mental, economic, cultural, or social identity."[89]

Any freely provided, explicit, informed, and unambiguous expression of the data subject's desires by which he or she expresses assent to the processing of personal data

[86] Jan Philipp Albrecht, How the GDPR Will Change the World, 2 EUR. DATA PROT. L. REV. 287 (2016).
[87] Degeling, Martin, Utz, Christine, Lentzsch, Christopher, Hosseini, Henry, Schaub, Florian & Holz, Thorsten, We Value Your Privacy... Now Take Some Cookies, 42 *Informatik Spektrum* 345 (2019).
[88] Supra note 85
[89] Art. 4(1), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

about them through a statement or a definite affirmative action is known as the data subject's consent.[90]

A security lapse that causes the unintended or unlawful destruction, loss, alteration, unauthorized disclosure, or access of personal data that has been sent, stored, or otherwise processed is known as a personal data breach.[91]

Principles of GDPR

Article 5 of the GDPR, enshrines the core principles for the purpose of personal data collection, storage, and use:

- Lawfulness, fairness and transparency[92]

Since the GDPR is user-centric, transparency in its context entails a shift from legal tick-box compliance to a customized, reflective, and dynamic approach. Individuals must be given a wealth of information, including information about recipients, retention periods, and the scope of their individual rights, such as access and portability, all of which must be presented in an easily understandable language.[93]

- Purpose limitation[94]

The GDPR mandates that the data can be used only for the purpose in which it has been extracted. Using the data collected for a particular purpose to another purpose would mean the violation of lawful consent. However, safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[95] is exempted under Art 89. In general, the data collected shall not be used for any other purpose other than intended.

- Data minimisation[96]

As per this principle, only the adequate quantity if data shall be collected. In other words, the data collected should be proportional to the object it is intended to achieve. No data which is excess to what is required shall not be collected, processed or stored.

---

[90] 4(11), Regulation (EU) 2016/679.
[91] Art. 4(12), Regulation (EU) 2016/679.
[92] Art. 5(1)(a), Regulation (EU) 2016/679.
[93] Goddard, Michelle, The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact, 59 *Int'l J. Market Research* 2017.
[94] Art. 5(1) (b), *Regulation (EU) 2016/679*.
[95] Art 89, *Regulation (EU) 2016/679*.
[96] Art 5(1) c , *Regulation (EU) 2016/679*.

- Accuracy[97]

Accuracy requires to keep the data current and all possible measures must be made to guarantee that inaccurate personal data is promptly deleted or corrected, taking into account the purposes for which it is processed.

- Storage limitation[98]

This principle requires the business entities not to store the data for more than the period for which it was collected. This principle is also hit by Art 89 of the GDPR.

- Integrity and confidentiality[99]

The security of data provided is of utmost importance as far as a Peron is concerned. It also imposes a duty to the data processor to maintain confidentiality thereby securing the data. The de facto method of explaining how a business or organization, and especially its website, gathers, distributes, and uses personally identifiable information (PII) is through privacy policies. Posting privacy policies are required by numerous government organizations worldwide, including the Federal Trade Commission in the United States.[100]Hence, the privacy policies should be in such a way that which takes all reasonable responsibility to take due care of the data collected.

- Accountability[101]

In order to be held accountable, organizations must implement the proper organizational and technical procedures and be able to prove their actions and efficacy upon request. For high-risk processes, this can also entail using privacy impact evaluations. An obligatory data breach notification system is also introduced by GDPR.[102]

4.4.2. The United State's Sectoral and State-Level Approaches

As opposed to the EU's comprehensive approach, the United States has a sectoral and decentralized approach to data privacy regulation. There isn't any single, inclusive federal legislation in the US that governs the gathering and use of personal data. Rather than addressing privacy and security, the government has created overlapping and

[97] Art 5(1) d , *Regulation (EU) 2016/679*.
[98] Art 5(1) e, *Regulation (EU) 2016/679*.
[99] Art 5(1) f, *Regulation (EU) 2016/679*
[100] Zaeem, Razieh Nokhbeh & Barber, K. Suzanne, The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise, 1 *ACM Trans. Manag. Inform. Syst.* 1 (2020), https://doi.org/10.1145/3389685.
[101] Art 5(2), R*egulation (EU) 2016/679*.
[102]Supra note 92

competing regulations by regulating just specific industries and categories of sensitive data such as financial and health[103].

Some of the main federal laws are the Health Insurance Portability and Accountability Act (HIPAA) for healthcare information, the Gramm-Leach-Bliley Act (GLBA) for financial information, and the Children's Online Privacy Protection Act (COPPA) for information about children. At the state level, the California Consumer Privacy Act (CCPA) and its follow-up, the California Privacy Rights Act (CPRA), have enacted more robust rights for consumers, including the right to know, erase, and opt-out of the sale of personal information. These pieces of legislation represent a growing trend toward GDPR-style protections at the subnational level. The U.S. also has a strong emphasis on cybersecurity, with frameworks like the NIST Cybersecurity Framework providing voluntary guidelines for managing cyber risk. However, the lack of harmonization across states and sectors poses challenges for compliance and international data transfers.

4.4.3. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework

The APEC Privacy Framework, established in 2005, represents a regional effort to promote cross-border data flows while safeguarding privacy rights across the Asia-Pacific region. Unlike the GDPR, it is non-binding and operates through voluntary implementation by member economies. The structure provides important privacy principles like notice, choice, integrity, security, and access, and enforces mechanisms like the Cross-Border Privacy Rules (CBPR) System, which allows data controllers in certified economies to prove compliance with APEC principles. The CBPR system promotes interoperability and fosters trust in cross-border data flows, especially among economies with different legal traditions. Despite their limited enforceability, the APEC model has been a workable template for promoting cooperation and regulatory convergence across a heterogeneous region.

4.4.4. The African Union Convention on Cybersecurity and Personal Data Protection

[103] Reforming the U.S. Approach to Data Protection and Privacy Author(s): Nuala O'Connor Council on Foreign Relations (2018)

The African Union (AU) endorsed the Convention on Cybersecurity and Personal Data Protection in 2014, or the Malabo Convention. This tool attempts to create a harmonized cyberlaw framework concerning cybersecurity and the protection of data in AU member states. It imposes national legislation on the protection of personal data, creates autonomous data protection authorities, and adopts technical and organizational measures for data protection. But ratification and implementation have been tardy, with only a few countries adopting fully the Convention at the national level. The Malabo Convention is nevertheless an important move towards continent-wide acceptance of data rights and data protection responsibilities. Supply chains have been made easier by the recent change and growth in e-commerce in Africa, and entrepreneurs have been exposed to a new business model that they can now implement going forward since they have acquired new clients. Introducing digital solutions has not been simple for all businesses, some smaller ones have struggled and need specialized assistance.[104]This growth of ecommerce necessitated for a regulation on data flows and privacy.

4.4.5. The OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data

The reason for bringing this comprehensive regulation is due to the risk that differences in national laws will impede the free movement of personal information across borders, which has significantly expanded in recent years and will only continue to do so as new computer and communications technologies become more widely used. Important economic sectors like banking and insurance might be severely disrupted by restrictions on these flows.[105]Issued first in 1980 and revised in 2013, the OECD Guidelines constitute a core international reference for data privacy, setting out principles akin to those in the GDPR such as collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability though in a less structured, non-binding manner. As a soft law tool, the OECD Guidelines have shaped national laws and ensured policy coordination between member and non-member states. They also assist trans-border data flows by fostering

[104] Michelle Chivunga & Alistair Tempest, *Digital Disruption in Africa: Mapping Innovations for the AFCFTA in Post-COVID Times*, South African Inst. of Int'l Aff. (2021).
[105]OECD, *Federal Information Processing Standards (FIPS)*, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf (last visited Apr. 24, 2025).

mutual understanding and equivalence among diverse privacy regimes, which makes them most effective in multilateral negotiations and trade talks.

4.6.UNITED NATIONS GUIDELINES AND THE ROLE OF INTERNATIONAL LAW

The United Nations has made contributions to data protection discussion mainly in the form of declarations and resolutions. Significantly, the UN General Assembly Resolution 68/167 (2013) reaffirmed the right to privacy in the digital era and urged states and businesses to protect personal data. Although not legally binding, such resolutions are a manifestation of international consensus and have an impact on domestic policymaking. In addition, the International Covenant on Civil and Political Rights (ICCPR), specifically Article 17, sets the right to privacy as a universal human right, serving as the foundation for legal interpretation and judicial activism in most jurisdictions. The 2030 Agenda states that "to ensure that no one is left behind and to assist with the measurement of progress (SGDs), quality, accessible, timely, and reliable disaggregated data will be needed." Such information is essential for making decisions.[106] Article 12[107]of the Universal Declaration of Human Rights Article 17[108] of the International Covenant on Civil and Political Rights, Article 16[109] of the Convention on the Rights of the Child; Article 14[110] of the International Convention on the Protection of All Migrant Workers and Members of Their Families; Article 8[111] of the European Convention on Human Rights; and Article 11[112] of the American Convention on Human Rights enshrine the right to privacy. The UN's campaign has also driven the creation of global digital cooperation mechanisms and promoted a human rights-based approach to data governance.

[106]United Nations Development Group, *Big Data for Development: Challenges & Opportunities*, https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf (last visited Apr. 24, 2025).
[107] G.A. Res. 217 A (III), Universal Declaration of Human Rights, U.N. GAOR, 3d Sess., Supp. No. 13, U.N. Doc. A/810, at 71 (Dec. 10, 1948).
[108]International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171.
[109]Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.
[110] International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Dec. 18, 1990, 2220 U.N.T.S. 3.
[111] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.
[112] American Convention on Human Rights, Nov. 22, 1969, 1144 U.N.T.S. 123.

4.7. EMERGING FRAMEWORKS AND GLOBAL INTEROPERABILITY INITIATIVES

In the past few years, there has been a joint effort towards establishing interoperability across varied data protection regimes. Examples include the Global Privacy Assembly (GPA) and the G7 Data Protection and Privacy Authorities Roundtable initiatives that aim at harmonizing principles and promoting cross-border cooperation on enforcement. Also, newer systems such as the Global Cross Border Privacy Rules (CBPR) Forum, which came into being in 2022, seek to take the APEC CBPR framework beyond its founding membership. Such moves show a rising acknowledgment that data regulation has to be collaborative and responsive to global digital realities.

4.8. CONCLUSION

To conclude, the global data privacy and security environment is characterized by a dynamic interplay of regional instruments, national legislations, and multilateral initiatives. The absence of a single, binding international data protection treaty highlights the significance of soft law tools and interoperability initiatives. While data will continue to drive economic growth, innovation, and social change, the development of these frameworks will remain at the heart of the debate around digital sovereignty, human rights, and global governance. While data flows across borders and cyber-attacks become increasingly sophisticated, the necessity for overarching global standards has never been greater.

The GDPR is a landmark legislation that has raised the bar for data protection, focusing on essential principles like transparency, accountability, data minimization, and data subjects' rights. Its extraterritorial application and strict enforcement tools have prompted other jurisdictions to enact their own privacy legislations, frequently copying GDPR's fundamental principles but modifying them to suit local legal, cultural, and economic environments. Such frameworks as the California Consumer Privacy Act (CCPA) in the United States, and China's Personal Information Protection Law (PIPL) represent an overall international shift in elevating persons to a higher level of control over their personal data and setting stricter standards on organizations that accumulate, process, and transfer such data.

Along with privacy regulations, cybersecurity models like the EU's NIS2 Directive and the U.S. Cybersecurity Maturity Model Certification (CMMC) augment privacy legislation by emphasizing the security of critical infrastructure and organizational resilience to cyberattacks. This alignment of privacy and security regulations underlines

the increasing awareness that safeguarding data privacy cannot be divorced from ensuring data security.

International institutions like the OECD, the Council of Europe, and the United Nations have played significant roles in advancing shared principles and stimulating dialogue between countries. In summary, the global guidelines on data security and privacy are a developing and dynamic area of practice where the safeguarding of individual rights is weighed against the needs of innovation and international business. Organizations need to be proactive and alert in adjusting to emerging rules, developing a culture of security and privacy, and contributing to the development of future frameworks by interacting with policymakers. Finally, realizing a harmonized and effective global data privacy and security regime will depend on sustained cooperation between governments, industry actors, and civil society to foster trust and resilience in the digital ecosystem. To know the regional effects and implications of the data protection laws it is necessary to analyse the domestic legislations also.

CHAPTER 5

INDIAN LEGISLATIVE FRAMEWORK ON DATA PROTECTION AND PRIVACY

5.1. INTRODUCTION

In the 21st century the flow of personal information from one digital space to another become as natural to life as a common phenomenon. In this changing digital landscape, personal data has become a new kind of virtual capital, but extremely powerful. It feeds algorithms, fuels innovation, and defines user experience. Yet, this increasing reliance on digital technologies has also raised growing concerns about the misuse, commodification, and unauthorized surveillance of personal data. Information about individuals should not be automatically made available to other people and organizations in order to protect privacy and data. Each individual must have significant control over the data and how it is used. Data protection is a legal measure to stop the improper use of personal information on computers and other media.[113] Herein, the right to privacy and the constitutional framework of data protection have been at the nexus of both legal argumentation and policy-making in India.

Even though the concept of privacy is commonly accepted, Indian law has given it a particularly complex and dynamic path. In contrast with certain jurisdictions where privacy is expressly enshrined in constitutional or statutory laws, Indian recognition of the right of privacy has been fashioned predominantly through the courts. Indian courts have gone back and forth between strict and broad interpretations of personal liberty for many decades, usually viewing privacy as a peripheral matter. It was not until 2017, in the historic Justice K.S. Puttaswamy (Retd.) v. Union of India[114] ruling, that the Supreme Court firmly held that privacy is a fundamental right inherent in the right to life and personal liberty guaranteed under Article 21 of the Indian Constitution. This ruling did not just confirm privacy as a legal right; it triggered a fundamental change in how data management would now be addressed in the nation.

[113] Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, 53 J. Indian L. Inst. 663 (2011).
[114] Justice K.S. Puttaswamy (Retd.) v. Union of India, A.I.R. 2017 S.C. 4161 (India).

After this constitutional landmark, the Indian state was charged with developing a strong legal framework that would translate the right to privacy in the era of digital data. While such existing legislation like the Information Technology Act, 2000 and its subordinate regulations provided minimal protections for data security, these fell short of the all-around protection contemplated in the Puttaswamy ruling. In order to address this legislative gap, the Indian government established the Justice B.N. Srikrishna Committee in 2017 as part of a process of policy and legal reform. This ultimately led to the creation of the Personal Data Protection Bill, 2019which is a draft law that was modified to take into account Indian sociopolitical circumstances while drawing at least some inspiration from the General Data Protection Regulation (GDPR) of the European Union. However, this law was dropped in 2022 after receiving criticism for granting excessive state exemptions.

As a result, India's first comprehensive law committed exclusively to preserving personal data, the Digital Personal Data Protection Act, 2023, went into force. The law aims to strike a delicate balance between the legitimate interests of the state and private parties in data processing for national security, innovation, and governance, and the individual's right to information privacy. It brings in concepts like consent-based data processing, fiduciary duties, rights of the user, and the creation of a regulatory authority named the Data Protection Board of India. In spite of its progressive aim, the legislation has come under criticism for the extent of government exemptions and the restricted autonomy of its enforcement apparatus. In most Asian and international cities, privacy is now considered a luxury, despite the European Union having robust legislative protections for the privacy of personal information and explicit legislation governing the collection, storage, and reuse of data.[115]

This chapter provides a critical analysis of the Indian legislative environment on data protection and privacy. It follows the constitutional development of the right to privacy, examines the sufficiency of current and pending statutory regimes, and reviews the implications of the 2023 Act in light of global best practices.

5.2. JUDICIAL DEVELOPMENT OF THE RIGHT TO PRIVACY IN INDIA

[115] Cybersecurity and Privacy Issues Facing Smart Cities, in Cyber Infrastructure Protection Volume III (Strategic Studies Inst., U.S. Army War Coll. 2017).

The history of protecting privacy in India, especially about personal data, has been defined by judicial contemplation, legislative change, and developing societal issues. The development of privacy as a constitutional right in India is not only a legal but also a deeply interconnected journey with India's socio-political and technological advancements. Information privacy, often known as data privacy, is the connection between society's perception of privacy, the legal and political challenges surrounding data technology, and its collection and distribution.[116]

5.2.1 Pre-Constitutional and Early Post-Constitutional Framework

In pre-independence India, privacy was not legally conceived as a specific concept. In British colonial law, state control was more prevalent and individual privacy less so. The idea of personal privacy hence remained mostly undiscussed under the legal mechanism, which considered state surveillance and control more pertinent and the regulation of public order more important.

Following India's independence in 1947, the drafters of the Indian Constitution were keenly conscious of the necessity to safeguard individual liberties from state encroachment. Yet, the Constitution itself did not have any explicit provision that ensured the right to privacy. The basic rights under Part III of the Indian Constitution, such as the right to life and personal liberty (Article 21), were enunciated widely, but they did not specially enjoin privacy as an individual right. Privacy, in a constitutional sense, was never regarded as an independent right but as a dimension of overall personal liberties.

5.2.2 The Kharak Singh Case (1963)[117]

The first important judicial encounter with the right to privacy in India was in 1963, when the Supreme Court decided the case of Kharak Singh v. State of Uttar Pradesh. The case was a challenge to police surveillance in the form of domiciliary visits to suspected criminals, which was authorized under UP Police Regulations. Kharak Singh argued that such surveillance intruded into his fundamental right of personal liberty. The Court held that although there was no direct "right to privacy" stated in the Constitution, the right of personal liberty under Article 21 of the Constitution encompassed some elements of privacy. The Court did not declare privacy as a

[116] Supra note 113
[117] Kharak Singh v. State of U.P., A.I.R. 1963 S.C. 1295 (India).

fundamental right in its entirety. Rather, it held that privacy could be restricted by law for reasons such as national security or public order[118]. In spite of all this, Kharak Singh set the groundwork for subsequent reasoning regarding the role of state action in relation to individual liberty.

5.2.3 The Post-Kharak Singh Era: Wider Concept of Privacy

After Kharak Singh, privacy was an infant concern in Indian law for a few decades. There was little judicial attention to the growing issues of surveillance, data collection, and state surveillance that were becoming more and more pertinent in the post-Internet era, and legal debate of privacy was occasional. Even while privacy cases persisted, they were typically viewed in light of other rights, such as personal liberty or freedom of speech and expression.

One of the most important cases of this time was R. Rajagopal v. State of Tamil Nadu (1994),[119] in which the Supreme Court held that the right to privacy was inherent in the right to life and liberty under Article 21. The case was not really about the right of an individual to safeguard his/her image and reputation from being published without permission, but not about the wider aspects of privacy or data protection.

5.2.4 The Puttaswamy Judgment (2017)[120]

The seminal judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India[121] in 2017 was a paradigm shift in India's judicial strategy on privacy. In this judgment, the Supreme Court at last held that the right to privacy is an integral aspect of the right to life and personal liberty under Article 21 of the Indian Constitution. This decision was a landmark in Indian constitutional law, as it established the right to privacy as a fundamental right that extends to all areas of a person's life including physical, digital, or informational.

The judgment, handed down by a nine-judge bench, categorically declared that privacy is an integral part of human dignity, autonomy, and personal liberty. The judgment recognized that privacy is not only a shield against physical invasion but also includes the safeguarding of personal information, bodily integrity, and informational privacy in

[118] id
[119] R. Rajagopal v. State of Tamil Nadu, A.I.R. 1995 S.C. 264 (India).
[120] A.I.R. 2017 S.C. 4161 (India).
[121] id

the age of the internet.[122] Justice Chandrachud specifically emphasized that privacy also involves a person's control over their personal information and the right to determine how it is disseminated and to whom.

Notably, the Court also underscored the principle of informed consent, pointing out that individuals should have complete knowledge and voluntary control over the collection and use of their personal information. This was a significant lead-up to the conceptualization of data protection legislation in India. The judgment laid down the constitutional basis for legislation governing data privacy and security and sparked the drive for legislative changes to safeguard personal data from abuse.

5.2.5 The Need for Legislation

Although the Puttaswamy case was a milestone in affirming privacy as a fundamental right, it also highlighted the need for a strong legislative framework to enforce such rights in the digital era. The decision emphasized that the right to privacy might be curtailed on specified grounds such as protection of national security or public order but any restriction thereof had to satisfy the constitutional test of necessity, proportionality, and lawfulness. Privacy is both a societal and personal value.[123] The Court also emphasized the necessity of a full-fledged law on data protection, since the nation was fast becoming a world hub for digital transactions and data creation.

This resulted in the formation of the Justice B.N. Srikrishna Committee in 2017 to formulate a full-fledged data protection law for India. The recommendations of the committee finally led to the Personal Data Protection Bill, 2019, which aimed to regulate the collection, processing, and transfer of personal data in a way that would be in harmony with the basic right to privacy. While the Bill ran into several challenges and was finally substituted by the Digital Personal Data Protection Act, 2023, the legal principles enunciated in Puttaswamy continued to remain at the heart of the development of India's data protection landscape. It's crucial to recognize that different countries have different laws, perspectives, interests, and attitudes when it comes to privacy problems. When it comes to designing and developing smart cities, a "one size fits all" strategy might be foolish and unlikely to satisfy the privacy requirements of

[122] Justice K.S. Puttaswamy (Retd.) v. Union of India, A.I.R. 2017 S.C. 4161 (India).
[123] R. Revathi, Pervasive Technology, Invasive Privacy and Lucrative Piracy – A Critique, 51 J. Indian L. Inst. 368 (2009).

various demographic groups.[124]This notion is applicable not only in the case of smart cities but also in all fields. Sector specific legislations tailored to meet the peculiar conditions is what required.

5.2.6 The Right to Privacy as a Dynamic Legal Concept

The development of the right to privacy in India is a demonstration of the dynamic character of legal principles in reaction to technological innovation and social change. Since its early inception in Kharak Singh up to the constitutional validation in Puttaswamy, the Indian judiciary has steadily enlarged the purview of privacy, particularly that of digital privacy and protection of personal data. But as India struggles with balancing privacy rights with the relative needs of state security, economic development, and technological advancements, the privacy law of the future will ride on the efficacy of its legislative framework and the watchfulness of its courts in protecting individual rights. In order to develop the novel framework for data treatment, Indian regulatory bodies appear to be working toward a similarly complicated and broad set of goals. This include safeguarding the privacy of Indian citizens, defending people and institutions from local or international cyberattacks, facilitating the growth of Indian digital businesses, and enhancing law enforcement through the use of digital tools and legal authorities. All of these goals are quite acceptable provided they are pursued with careful policymaking. It should not be expected, nevertheless that they can all be readily balanced and made to work together.[125]

5.3. LEGISLATIVE TOOLS CONTROLLING DATA PROTECTION IN INDIA

Although earlier legislation tended to focus more on cybersecurity and digital data privacy, India only began to address the pressing issues of data privacy in a comprehensive manner in the twenty-first century. The legislative tools that regulate data protection in India presently are the Information Technology Act, 2000 (IT Act), the Sensitive Personal Data or Information Rules, 2011, the Personal Data Protection Bill, 2019, and the Digital Personal Data Protection Act, 2023. These tools, as much as

[124] Cybersecurity and Privacy Issues Facing Smart Cities, in Cyber Infrastructure Protection Volume III (Strategic Studies Inst., U.S. Army War Coll. 2017).
[125] Mark Linscott & Anand Raghuraman, *Aligning India's Data Governance Frameworks* (Atlantic Council 2020).

they define a legal regime for the protection of personal data, also bring out a number of gaps and challenges that still frame India's data privacy agenda.

5.3.1 The Information Technology Act, 2000 (IT ACT, 2000)

The Information Technology Act, 2000 (IT Act) was India's first serious effort towards giving a legal framework for handling cybercrimes and electronic commerce. Both specific data protection regulations and freedom of information legislation give people the right to know what kinds of information an organization is keeping about them. This component of information freedom is especially important in India, where the Right to Information Act advances the goal of data protection laws despite the lack of a specific data protection law. [126]Although the IT Act dealt mainly with concerns like online fraud, digital signatures, and regulation of e-commerce, it also established some provisions regarding the safeguarding of personal data, but in a limited sense. It is a law that determines legal recognition for transactions conducted through electronic data interchange and other electronic communication channels. This type of activity is commonly known as "electronic commerce" and involves using alternatives to paper-based communication and information storage methods to enable electronic document filing with government agencies.[127]

The IT Act was a necessary beginning in India's journey into the digital world. Yet, provisions related to data protection were not stringent enough to respond to increasing worries over private lives in the digital world. The IT Act provided the idea of "reasonable security practices,"[128] which eventually became the foundation for data protection practices in India. But it should be noted that the IT Act did not clearly define what constitutes reasonable security practices, and businesses and entities had to interpret the requirement in a way that could result in inconsistency in the degree of protection given to personal data.

5.3.1.1 Section 43A – Compensation for Failure to Protect Data

One of the significant provisions of the IT Act is Section 43A, whereby a company or an entity that processes sensitive personal data or information has to implement

[126] Atul Singh, *Data Protection*, 59 J. Indian L. Inst. 78, 78–101 (2017).
[127] Vivek Kumar Tyagi, Legal Offshoring Industry and Data Privacy: Global Perspectives (With Special Reference to India), 74 Indian J. Pol. Sci. 517, 517–532 (2013)

[128] Information Technology Act, 2000, S. 43A (India).

"reasonable security practices and procedures" to protect such data. In case of any data breach and consequent damage or loss to a person, the organization has to compensate the aggrieved party[129]. This stipulation was an attempt to engender a perception of responsibility within organizations that are dealing with individual data. This was an early recognition that computer security was more than a technological issue but was also a matter of law.

But the lack of a specific definition of "reasonable security practices" has made enforcement difficult. What is "reasonable" may be different, and without definite guidelines or particular regulatory requirements, organizations function with minimal compliance, exposing personal data to risk.

5.3.1.2 Section 72A – Punishment for Disclosure of Information

Another important provision in the IT Act is Section 72A, which criminalizes the unauthorized release of personal information by any person or company having access to it through their professional or contractual relationship. This is a provision that attracts a penalty of up to ₹5,00,000 or imprisonment for three years, or both, for any individual or entity that releases personal data without permission beyond the scope for which it was gathered.[130]

Although Section 72A acts as a deterrent in cases of violation of trust, its applicability is restricted. The provision is applicable only to persons or entities entering into a contractual or professional relationship with the data subject. This leaves a huge lacuna in data protection, particularly in cases involving third parties or governmental organizations. It also fails to deal with general issues like data abuse by private entities, which might not come under the jurisdiction of a contract but still deal with huge amounts of personal data.

5.3.1.3 Limitations of the IT Act in Data Protection

Even though the IT Act introduced concepts that established the cornerstones of India's data protection system, its rules fall short in addressing the complexities of modern data privacy. Data protection takes a backseat under the IT Act, which is more focused on cybersecurity and digital transactions. Enforcement gaps have been caused by the lack

[129] IT Act, S. 43 A
[130] IT Act, S. 72 A

of explicit consent procedures, the ambiguity around "reasonable security practices," and the absence of a dedicated regulatory body for data protection. In general, although while the IT Act served as the original foundation, it is now thought to fall short of what the modern digital world requires, especially in terms of complete security of personal data.

5.3.2 The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

In 2011, the government brought out the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, which are popularly known as the SPDI Rules. The SPDI Rules were intended to be an add-on to the IT Act, providing more specific provisions regarding the processing of sensitive personal data. The SPDI Rules acknowledged that some categories of data like passwords, financial data, health-related information, and biometric data need stricter safeguards because they are sensitive in nature.

5.3.2.1 Definition of Sensitive Personal Data or Information (SPDI)

The SPDI Rules classified some personal data as "sensitive," which had to be treated with greater safeguards. These include financial information, health information, sexual orientation, and biometric information. In defining sensitive information, the SPDI Rules sought to bring clarity to the kinds of information that needed special treatment.[131] These regulations also required that organizations gathering such information do so with the express permission of the data subject and that the data be kept securely to avoid unauthorized access or disclosure.

The placing of biometric information and health records within the sensitive data category was especially significant. It was an indication of increasing recognition of the risks involved in the gathering of highly intimate information, especially in the modern digital era. In Mr. X v. Hospital Z,[132] the Supreme Court ruled that although a doctor-patient relationship is essentially commercial, it is a matter of professional confidence, and as such, doctors have an ethical and moral need to maintain confidentiality.

[131] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 3 (India).
[132] Mr. X v. Hospital Z, A.I.R. 1999 S.C. 495 (India).

5.3.2.2 Key Provisions and Requirements

The SPDI Rules required organizations handling sensitive personal data to implement "reasonable security practices and procedures." Such procedures encompass actions like encryption, firewalls, and access controls to avoid unauthorized access to information. Organizations must also obtain the express consent of the data subject prior to the collection of sensitive personal data and inform the individual of the purpose for which the data is being collected.

The regulations also mandated that organizations restrain the retention of personal information. Data should not be held beyond what is needed to serve the purpose for which it was collected, and once this purpose is served, the data must be destroyed securely.

5.3.2.3 Criticisms

Despite the SPDI Rules being a step ahead in safeguarding sensitive information, their application was still restricted. These regulations pertain specifically to body corporates, thereby exempting government institutions and other non-private organizations from direct applicability of these provisions. The definition of "reasonable security practices" remains still too ambiguous and therefore results in varied implementation and enforcement across industries. Finally, the lack of a specialized regulatory agency to monitor and enforce these rules makes compliance optional and leaves no enforcement mechanism in place to impose significant fines for breaches.

5.3.3 The Digital Personal Data Protection Act, 2023 (DPDP ACT)

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark development in India's efforts to implement end-to-end data protection legislation. The DPDP Act was brought after the Personal Data Protection Bill, 2019 (PDPB) was withdrawn and aims to simplify and make provisions for personal data protection more streamlined along with remedying some of the grievances expressed by stakeholders during the review process of the PDPB.

The DPDP Act is a step toward a more comprehensive data protection regime that emphasizes giving people greater control over their own personal information while holding data processing companies accountable for their actions. This Act is a

continuation of India's broader efforts to solve particular problems specific to the country's socioeconomic and political situation and to harmonize Indian data privacy regulations with international norms, such as the General Data Protection Regulation (GDPR) of the European Union.

5.3.3.1 Important Provisions of the DPDP Act

1.Data Protection Principles

The DPDP Act stipulates a number of key fundamentals that form the basis of the entire scheme of data protection in India. The principles guide how personal data is to be treated by parties and rights accorded to people whose data is being processed. The Act requires the following:

- Lawfulness, Fairness, and Transparency[133]: Processing of personal data should be done in a legal and ethical way, and individuals should be informed of the reasons why their data is being processed and collected.
- Purpose Limitation[134]: Personal data should only be collected for legitimate, particular purposes, and should not be further processed in a way incompatible with those purposes.
- Data Minimization[135]: Personal data should only be collected and processed to the extent that is necessary for the purpose.
- Accuracy[136]: Personal data should be accurate and updated. Inaccurate data should be corrected or deleted as soon as possible.
- Storage Limitation[137]: Data should not be stored longer than is necessary for the purposes for which it was collected, and it should be securely deleted when no longer needed.
- Accountability[138]: Organizations that handle personal data, or data fiduciaries, are responsible for adhering to the terms of the Act. They are held accountable for the privacy and security of the data they handle.

2. Rights of Data Principals (Individuals)

---

133 Digital Personal Data Protection Act, 2023, S. 6(1), (3) (India).
134 DPDP Act, S. 7(1), 5(2) (i).
135 DPDP Act, S. 5(2)(i), (ii).
136 DPDP Act, S. 5(2), 12(1).
137 DPDP Act, S. 5(2) (b).
138 DPDP Act, S. 8, 9.

One of the most important features of the DPDP Act is the list of rights it provides to individuals (data principals) whose data is being processed. These rights are intended to provide people with greater control over their personal data. The most important rights under the DPDP Act are:

- Right to Access[139]: Data principals are entitled to access the personal data that a data fiduciary maintains on them, including information regarding the purpose for which their data is being processed.
- Right to Correction/Rectification[140]: In case any of the data maintained by the data fiduciary is erroneous or incomplete, data principals have the right to correct it.
- Right to Erasure: The data principals may exercise the right to have their data erased in specific situations, for example, where the data is no longer required for the purpose for which it was collected or where the consent is revoked.
- Right to Grievance Redressal[141]: Each Data Principal is entitled to an accessible grievance redressal system on the part of the Data Fiduciary. In the event of dissatisfaction, they can approach the Data Protection Board of India for resolution and enforcement.
- Right to Nominate[142]: The Act also gives Data Principals the option of nominating some other person to exercise data protection rights in the case of death or incapacitation. This ensures continuity of control over personal data even where the principal himself is not able to act anymore.
- Right to Withdraw Consent[143]: Individuals have the right to withdraw their consent at any time, with the process being as easy as granting it. Once withdrawn, the data fiduciary must cease processing the personal data unless otherwise required by law.

These rights empower and allow individuals to be in charge of their personal data, establishing a legal system that fosters accountability and transparency.

3 Data Fiduciaries and Data Protection Obligations

[139] Digital Personal Data Protection Act, 2023 S. 11(1) (a)(India).
[140] DPDP Act, S. 12(1) (a), (b).
[141] DPDP Act, S. 11(1) (c).
[142] DPDP Act, S. 14.
[143] DPDP Act, S. 6(5).

The DPDP Act also brings the concept of data fiduciary, which can be defined as any government or private entity which decides the purpose and means for processing personal data. Such data fiduciaries are required to ensure that personal data processed by them is processed in accordance with the principles provided in the Act.

Some major obligations of data fiduciaries are:

Consent Management[144]: Data fiduciaries are required to secure explicit, informed consent of individuals prior to processing their personal data. This consent should be clear, specific, and reversible at any time.

Data Security[145]: Data fiduciaries shall take adequate technical and organizational measures to guarantee the security of personal data and protect it against breaches, unauthorized access, and abuse.

Data Impact Assessment[146]: Data fiduciaries must carry out regular Data Protection Impact Assessments (DPIAs) to assess the risks associated with their data processing operations. The latter is especially crucial in the processing of sensitive personal data.

Notification of Data Breaches[147]: In the case of a data breach, data fiduciaries must notify the Data Protection Board and individuals affected within a prescribed period (e.g., within 72 hours of their becoming aware of the breach).

5.3.3.2 Data Protection Board (DPB)[148]

The DPDP Act envisages the creation of an independent regulator by the name of the Data Protection Board (DPB). The DPB shall be responsible for ensuring compliance with the provisions of the Act, investigating breaches of data, and hearing complaints from individuals whose privacy rights under the data have been infringed.

The DPB will have some major functions, such as

- Monitoring Compliance[149]: The DPB will oversee whether data fiduciaries are complying with the data protection principles and meeting their obligations under the Act.

[144] Digital Personal Data Protection Act, 2023, S. 6(1)–(5) (India).
[145] DPDP Act, S. 8(5).
[146] DPDP Act, S. 10(1) (b) (for Significant Data Fiduciaries)
[147] DPDP Act, S. 8(6).
[148] DPDP Act, S. 18–32.
[149] DPDPAct, S. 28(1) (b)

- Enforcement and penalities[150]: The DPB will be empowered to issue orders, fines, and penalties against non-compliant parties. It can also take action against parties breaching the data privacy rights of individuals.
- Public Awareness[151]: The DPB will work to create awareness and educate the general public and companies regarding data protection and privacy rights.
- Adjudication of Complaints[152]: The DPB shall receive and settle disputes from data principals who believe that their data privacy rights have been violated.

5.3.3.3 Cross-Border Data Transfers and Localization[153]

One of the most important features of the DPDP Act is how it handles cross-border data flows. Although the Act does not put in place a complete ban on taking personal data out of India, it creates certain conditions for such transfers to take place. These involve having a guarantee that the recipient country delivers an equal level of protection, just like that within India.

The Act also proposes provisions of data localization, specifically for sensitive personal data, which can possibly be stored within India. The data fiduciaries are to ensure that the sensitive data stay in India subject to terms set by the Data Protection Authority. Yet, the ambit of localization requirements is less onerous in comparison with other global regimes such as the GDPR, which imposes more robust data localization procedures. In addition to increasing compliance costs for businesses operating in India, stringent data localization regulations may set a precedent for other nations to follow, restricting Indian businesses' capacity to cater to international clients. India should therefore approach data localization carefully and precisely while also establishing flexible, reciprocal pathways and mechanisms that permit the cross-border processing and storage of Indian data in nations that adhere to particular privacy protection and law enforcement cooperation standards.[154]

5.3.3.4 Exemptions and Governmental Powers[155]

[150] Digital Personal Data Protection Act, S. 28(1) (d), (e), S. 33 (India).
[151] DPDP Act, S. 28(1) (f).
[152] DPDP Act, S. 28(1) (c), S. 13.
[153] DPDP Act, S. 16, 17.
[154] Mark Linscott & Anand Raghuraman, *Aligning India's Data Governance Frameworks* (Atlantic Council 2020)
[155]DPDP Act, S. 18–21

The DPDP Act also grants a number of exemptions to government use of personal data. For instance, data processing by government agencies on grounds of national security, public order, or law and order may be exempted from some provisions of the Act. Privacy groups have expressed concern about these exemptions, believing they will encourage excessive government monitoring and undermine citizens' right to privacy.

Furthermore, in order to maintain public order or national security, the government may derogate certain provisions of the law by declaring exemptions for specific industries. Due to concerns that it will be used for unrestricted surveillance and data exploitation, this expansive exemption given to the state has long been the focus of intense criticism.

5.3.4 CRITICISMS AND CHALLENGES OF THE DPDP ACT

Although the Digital Personal Data Protection Act, 2023 (DPDP Act) is a critical legislative framework for personal data protection in India, its provisions have generated massive criticism on several fronts. Critics of the Act point out that it does not contain enough protection against overreach by the government, its enforcement provisions are inadequate, and its strategy for cross-border data flows may stifle international business operations. Following are the major criticisms and issues for the DPDP Act:

1. Wide Exemptions for Government Agencies

Perhaps the most controversial part of the DPDP Act is the wide exemptions it grants to government agencies, particularly on grounds of national security, public order, and law enforcement. The Act permits the government to override a number of important provisions of the law when it processes personal data for these reasons. A number of sections are up for Central Government decision-making, which raises concerns about unrestrained rule-making and possible regulatory gaps.[156]

2. National Security and Public Order Exemptions

Under the DPDP Act, the government may process personal data without resorting to the normal data protection principles (like data minimization, consent, and purpose

[156] Dr. Pradip Kumar Kashyap, Digital Personal Data Protection Act, 2023: A New Light into the Data Protection and Privacy Law in India, 2 ICREP J. Interdisc. Stud. (Prof. N.R. Madhava Menon ICREP, Cochin U. Sci. & Tech.) (2023).

limitation) if the processing of the data is found to be necessary for national security or public order. These exceptions are very sweeping in nature, and critics say that these may pave the way for unfettered surveillance by the government. The legislation is additionally criticized for weakening the RTI Act by restricting the disclosure of public officials' personal information. One area of worry among the public was the Act's significant impact on the RTI Act.[157] Although RTI has made it possible for anybody to inquire about government programs, social benefits, corruption, and rights, departments can now easily suppress inquiries by claiming that personal data cannot be disclosed.[158]

For instance, state agencies may gather, process, and store individuals' data under the pretext of national security or fighting terrorism, without being subject to accountability regarding ensuring that data is processed within the terms of privacy rights. Uncertainty in defining "national security" and "public order" may give rise to indiscriminate and unjustified processing of data.

3. Individual Privacy Impact

Many privacy advocates believe that these exemptions undermine the DPDP Act's fundamental purpose of protecting people's privacy. The broad scope of the exemptions would enable government agencies to escape data protection laws, reducing transparency and compromising citizens' fundamental right to privacy in the process.

This have led to proposals to limit these exemptions and implement stronger oversight tools to guarantee that government organizations handle data in an accountable and transparent manner. To ensure that data processing for national security is subject to sufficient checks and balance judicial monitoring or a distinct review body could be established as a solution.

4. Weak Enforcement Mechanisms and the Role of the Data Protection Authority

Although the DPDP Act sets out to create the Data Protection Authority (DPA), whose role it is to oversee compliance and enforce the law, the critics say that the DPA might

[157] id
[158] Patial, Tushar & Gupta, Aashi, Balancing Privacy and Accountability: A Closer Look at India's DPDP Act of 2023, 6 Indian J. L. & Legal Research 6709 (2023).

lack the necessary power, resources, or autonomy to be able to regulate such a complicated regulatory landscape effectively.

5. Independence of the DPB

The independence of the DPB is essential so that it is not subject to external interference, especially from the government. However, there are concerns that the proposed structure of the DPB may not be independent enough. The government's involvement in appointing the leadership of the DPB could potentially undermine its autonomy and credibility. The DPB is portrayed less as a proactive regulator and more as an adjudicatory body. This arrangement casts doubt on its capacity to enforce the Act and hold influential people and organizations responsible.[159] The entire effectiveness of the data protection system is compromised in the absence of a strong, independent DPB. As DPB is not constituted yet, its efficiency and effectiveness are still to be known.

6. Large Tech Company's Accountability

International tech behemoths like Facebook, Google, and Amazon, which are present in India, handle massive amounts of individual data. Most critics believe the DPDP Act is not equipped with sufficient enforcers to punish such corporations for violation or misuse of data privacy. The arrangement of DPB raises doubt on the capacity to enforce the Act and hold prominent individuals and organizations responsible.[160] The Act emphasizes making data fiduciaries comply, but little is made clear as to how the DPB will be able to enforce large companies to comply, particularly when these companies are international in scope and might be regulated by various privacy regimes in various jurisdictions.

7. Unclear and Ambiguous Provisions in Data Fiduciary Obligations

While the DPDP Act imposes a significant burden of responsibility on data fiduciaries to provide personal data protection, there remain areas of ambiguity in some provisions, especially with regards to data security and data breach notifications.

---

[159] Sreevalli Seetharamu, Lakshmi C.N., Anisha Bhattacharya & Dr. B.T., *Digital Data Protection Laws: A Review*, 11 Int'l J. Sci. Res. Sci. Eng'g & Tech. 64 (2024), https://doi.org/10.32628/IJSRSET2411416.
[160] id

8. Lack of Clear Data Security Requirements

The DPDP Act requires data fiduciaries to adopt "appropriate" technical and organizational measures for securing personal data, but the Act does not give a definitive definition of "appropriate" measures for security. The lack of a clear definition or specific guidelines for data security may lead to inconsistencies in business and organizational treatment of data protection.

Without standardized measures for data protection, businesses may implement differing levels of security, creating gaps in data protection practices across industries. This may create possible openings for the system to be vulnerable, and it would be hard to avoid cyber-attacks, data breaches, or abuse of personal data.

9. Lack of classification of sensitive personal data

Unlike the GDPR, which classifies personal information revealing racial or ethnic origin, political opinion, religion or philosophy, sexual orientation, etc. as "special categories of Personal Data," the DPDP Act does not categorize personal information. These sensitive data are given extra protection.[161] The act fails to classify data into sensitive personal data. The classification is there in the Information Technology act and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 but the legislation that aims to protect personal data lacks such classification raises concerns as to which king of data the act intends to protect.

10. Cross-Border Data Transfers and Data Localization Requirements

Another major concern raised by critics is the cross-border data transfer and data localization provisions of the DPDP Act. The Act permits data to be transferred to foreign countries only if the destination country ensures data protection levels equivalent to those required within India. The Bill's flaw is that it doesn't expressly restrict cross-border data transfers or outline specific compliance requirements that must be fulfilled when transferring personal information outside of India (such completing transfer impact evaluations or following standard contractual agreements).

[161] Kumar Abhishek, Deep Prabhat, Raghuvanshi Shivam & Kumar Vivek, India’s New Data Frontier: A Critical Legal Insight of the Personal Data Protection Act, 2023, 44 Library Progress Int'l 3 (2024).

[162]But this provision has raised eyebrows over its implications on international data flows and trade especially ecommerce.

11. Data Localization and Its Economic Impact

The DPDP Act introduces data localization requirements for sensitive personal data that has to be stored in India. While data localization can strengthen data protection by keeping sensitive data within India's legal realm, it may also create serious difficulties for businesses that are dependent on the free flow of data across borders. Sectoral norms are necessary, though, in addition to the fundamental values, duties, and rights. As a result, the DPDP Act 2023 can be described as a horizontal law that generally affects every industry[163]. However, because some industries, like e-commerce, have unique needs, the DPDP Act 2023 has to be enhanced with vertical rules and regulations. However, in the digital kaleidoscope, this law can be a harmonious symphony to re-engineer India's data privacy system provided it is complemented with the appropriate e-commerce norms and regulations.[164]

Several international businesses can also be required to invest in local data storage systems to meet such provisions, which can add to operational expenses. For globally operating multinational firms, this can make it difficult to handle the data across regions, which can translate to inefficiencies and clashes with such international regulations as the GDPR, which has varying demands for data transfers.

12. Global Trade and Compliance Concerns

The DPDP Act's policy towards cross-border data transfers may also influence India's position in the international digital economy. Nations with more open data transfer policies, like the United States or the European Union, might consider India's localization norms as a trade barrier. The effect of these policies on foreign investment in India's technology industry is unclear. Since India is becoming more influential as a source of global digital services and start-ups, strict data localization regulations would

[162] Mohd Abdul Sabur Khan, *Personal Data and Consumer Protection in E-Commerce: Examining Laws and Issues*, 6 Int'l J. L. Mgmt. & Hum. 2023 (2023).
[163] Amrita Jha, The DPDP Act 2023: Critical Insights into Its Legal Framework and Practical Impact, 43B Bull. Pure & Applied Sci.: Zool. (Animal Sci.) (Supp. No. 2) 466 (July–Dec. 2024).
[164] id

compromise its position as a player in the international market, and it would become less desirable for multinational companies.

13. Exclusion of Right to data portability

This right, which allows individuals to retrieve and recycle their own data from one service to another, is necessary to preserve consumer choice and competition in the digital economy. Its absence diminishes user's ability to change their service providers and manage their digital footprint. A specific clause pertaining to portability would encourage the data ecosystem to assume responsibility for preserving the data in a machine-readable, structured, and widely-used manner.[165]

14. Right to be forgotten (RTBF)

Similar to the clauses proposed by the Joint Committee of Parliament in clause 20 of the D.P. Bill, 2021 and the Committee of Experts in clause 27 of the PDP Bill, 2018, a specific provision on "the right to be forgotten" be included in the DPD Act, 2023. The emphasis would remain on the temporary nature of the personal data if the right were included as a special provision. Right to Be Forgotten (RTBF) enables one to request the erasure or removal of personal data where no strong rationale exists for its further processing. It is best known under Article 17 of the EU General Data Protection Regulation (GDPR). Right to erasure is mentioned under the DPDP act but the scope is limited.

The Court in the case Subhranshu Rout @ Subhranshu Goyal v. State of Odisha[166] identified the idea of the "Right to Be Forgotten" as a part of the general right to privacy. The Court highlighted legal provisions that will give individuals the power to demand erasure of their sensitive and personal information from public areas like social media sites, search engines, and websites.

But the court did not come out with a binding judgment accepting RTBF as an enforceable right, but instead suggested that this field needs legislative intervention and protection within the Indian legal system. It noted that the digital persistence of intimate

[165] A. Kumar Bisht & N. Shanmuka Sreenivasulu, *Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023*, IntechOpen (2024), https://doi.org/10.5772/intechopen.1007353.
[166] Subhranshu Rout @ Subhranshu Goyal v. State of Odisha, 2020 SCC OnLine Ori 878.

or defamatory data can infringe upon the right of a person to live with dignity, particularly victims of sexual violence or harassment crimes.[167]

An important turning point in India's data protection history was the Digital Personal Data Protection Act, 2023 (DPDP Act). However, it also faces significant challenges, just like any ambitious law. The effectiveness of the law may be undermined by the broad government exemptions, poor enforcement practices, ambiguities surrounding data fiduciary duties, problems with cross-border data flows, and the high costs of data localization. These will need to be addressed in the future through modifications and the creation of a strong, transparent enforcement system in order for the DPDP Act to successfully safeguard people's privacy while encouraging innovation and development.

5.4 CONCLUSION

India's attempts to balance personal privacy with digital innovation are currently at a turning point. As the nation's digital economy develops, it has begun to create regulatory frameworks that are based on human rights and constitutional principles in addition to controlling data flows. From industry-specific rules and the Information Technology Act to the newly passed Digital Personal Data Protection Act, 2023, the legislation under examination depicts a country fighting with the urgency and complexity of data governance in a networked society.

This legislative history reveals a patchwork that reflects both developmental pains and advancements. Although the first legal responses were technological and compliance-based, later frameworks have tried to firmly establish data protection within a rights paradigm. However, there are still structural, interpretative, and institutionally established problems that are not related to legislation. In the overlapping domains of national security, health, telecom, and finance, the lack of legislative coherence creates uncertainties that make enforcement and compliance difficult. Furthermore, the executive branch's discretionary freedom granted by recent laws raises questions about accountability, transparency, and the options open to individuals in the event of misuse.

[167] id

Importantly, the subject of data protection in India is increasingly found in courtrooms, corporate boardrooms, public forums, and civil society conversations rather than just in legal books. It suggests that wider public engagement with technology and rights would shape India's privacy landscape rather than just lawmakers and judges. The ability of India's legislative system to function will be the true test, not its existence. Technological readiness, procedural justice, and administrative autonomy must be combined with legal certainty. Only then can data protection laws serve as tools of dignity and trust in a digital society, rather than as surveillance tools or administrative barriers.

As a result, the current framework cannot be seen as a final destination, but rather as a place to start a moral, legal, and constitutional basis upon which a more equitable and safe digital future will be built. The Indian privacy law should keep evolving in a dynamic, responsive, and participatory way so that people's rights grow in the light of data rather than shrinking within it. For that adopting international best practices into Indian tailored version would be helpful.

CHAPTER 6

ANALYSIS OF THE INDIAN LEGISLATION IN THE LIGHT OF INTERNATIONAL REGIME

6.1. INTRODUCTION

Personal data is now the new oil driving the development of e-commerce and business models as digital transactions take centre stage. However, the privacy and protection of personal data present an immense barrier in modern data economy. Today, governments everywhere have the dual responsibility of passing laws that protect individual privacy while permitting the unrestricted growth of online commerce. Two legislations, India's Digital Personal Data Protection (DPDP) Act, 2023, and the European Union's General Data Protection Regulation (GDPR), 2016, represent different methods of meeting this challenge. Although GDPR has long been regarded as the gold standard of data protection legislations around the world, DPDP Act mirrors a more business-oriented, adapting legal paradigm to serve India's growing digital economy.

6.2. LEGISLATIVE GOALS

The GDPR was enacted with the main objective of harmonizing the data protection legislation throughout the European Union to ensure a high level of protection for personal data as a right under the EU Charter. It aims at empowering individuals through giving them end-to-end rights on their personal data and imposing strict obligations upon data controllers and processors. Yet another critical aim of the GDPR is to ensure that data moves easily within the EU to support one digital market, as long as such transfers comply with privacy protection. The original goal of the Data Protection Directive[168] was to establish a uniformly high standard for data protection that would provide a consistent set of rights throughout the Union[169]. The original goal of the GDPR regulation was to establish a harmonized framework by eliminating the need for national implementation laws.[170]

[168] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.
[169] Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle?, 2 EUR. DATA PROT. L. REV. 290 (2016).
[170] id

On the other hand, the Indian DPDP Act seeks to develop an equilibrium legal environment that values both the right of privacy and the necessity to process personal data for the purpose of lawful processing, particularly in a country with a fast-digitizing economy. It focuses on facilitating lawful data processing for innovation and governance while protecting the rights of the people with a well-designed consent structure. The DPDP Act seems more so in line with the Indian situation, where digital adoption is still ramping up and companies need regulatory clarity and ease of compliance.

6.3. SCOPE AND JURISDICTION

The GDPR has broad territorial scope. It not only applies to those established within the EU but also to those outside the EU if they provide goods or services to, or observe the conduct of, individuals within the EU. This extraterritorial application entails that any business in the world that handles EU citizen data must fulfil GDPR requirements regardless of location. Clarity about processing requirements outside the EU territory has now been established, which is a crucial component of the Regulation. Organizations that handle a variety of personal data are now required to adhere to data security and protection regulations as though they were established in Europe.[171] This international coverage has established GDPR as a de facto worldwide standard but at the same time poses huge compliance challenges to foreign enterprises.

In comparison, the DPDP Act has a narrower ambit. It covers the processing of digital personal data in India and reaches foreign entities only if they provide goods or services to data principals in India. It specifically excludes non-automated offline data processing and is less restrictive regarding extraterritorial application. This reduced scope facilitates compliance for Indian startups and small digital businesses but can also create concerns regarding data protection adequacy in cross-border situations.

The extraterritorial application of the GDPR is one of its most characteristic elements, extending to any organization handling the personal data of EU residents, irrespective of the physical location of the entity. Likewise, the California Consumer Privacy Act (CCPA) also preempts its jurisdiction over businesses accumulating information from residents of California, subject to certain parameters like revenue or data of consumers

[171] Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle?, 2 EUR. DATA PROT. L. REV. 290 (2016).

processed. The DPDP Act follows the same pattern by pre-empting its applicability to processing outside India when related to providing goods or services to data subjects in India. This represents a major improvement on the IT Act, which has no extraterritorial operation, reducing its efficacy in the digital global economy.

6.4 DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITIQUE THROUGH THE LENS OF E-COMMERCE AND INTERNATIONAL BEST PRACTICES

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a significant legislative milestone in India. But, as measured against the international benchmark established by the General Data Protection Regulation (GDPR), its provisions disclose several weaknesses in responding to the needs of the e-commerce industry. The GDPR strikes a better balance between privacy protection and economic innovation.

6.4.1. Over-Reliance on Consent without Alternative Legal Grounds

In DPDP Act Data fiduciaries, organizations processing personal data, can process personal data only if the data principal (the individual) provides free, specific, informed, unconditional, and unambiguous consent[172]. The consent has to be with reference to a particular purpose and has to be clear, affirmative, and ascertainable. Furthermore, data fiduciaries are required to furnish a notice to the data principal prior to or at the time of obtaining consent, specifying the nature and purpose of the data being collected.[173]

In contrast, the General Data Protection Regulation (GDPR) offers a more pluralistic and flexible system for legal processing of personal data. In Article 6(1), the GDPR sets out six legal grounds for processing personal data, one of which is "legitimate interests"[174]. This provision allows data controllers to process personal data without consent where the processing is required for the legitimate interests of the controller or a third party, as long as such interests are not overridden by the data subject's fundamental rights and freedoms[175].

[172] Digital Personal Data Protection Act, No. 22 of 2023, § 6(1) (India).
[173] Id S 6(3)
[174] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 6(1)(f), 2016 O.J. (L 119) 1.
[175] id

The legitimate interest of GDPR has been construed widely by supervisory bodies and courts to encompass a range of commercial activities including fraud prevention, direct marketing, network security, and enhancing customer experience these activities are justified through regulatory guidance such as the European Data Protection Board (EDPB) Guidelines on Article 6(1) (f)[176] and national data protection authority rulings. Significantly, the GDPR places a balancing test, under which the controller must consider whether their legitimate interests outweigh the data subject's interests or rights and freedoms enshrined in Article 6(1) (f) explicitly. The three tests namely purpose test[177], necessity test[178] and balancing test[179] are laid down in determining the legitimate interest.

This method grants more flexibility in operation to digital businesses and e-commerce sites so they can engage in some forms of processing without the drawbacks of seeking express consent each time (Article 6(1) (f)), yet upholding the privacy rights of the individual through measures like transparency,[180] opt-out particularly for direct marketing[181] and data subject rights, most notably the right to object to processing for purposes of legitimate interests, as stated in Article 21(1).

1. Deemed Consent: A Partial Parallel

Section 7 of the DPDP Act introduces "deemed consent", which encompasses situations like:

- Performance of any function under law [182]
- Compliance with judicial orders[183]
- Attending to medical emergencies or disasters[184]

[176] Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC*, WP 217 (Apr. 9, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[177] Id
[178] Id at 27
[179] Id at 35-38
[180]GDPR, art. 5(1)(a), Regulation 2016/679, 2016 O.J. (L 119) 1.
[181] GDPR, recital 70 & art. 21(2), Regulation 2016/679, 2016 O.J. (L 119) 1.
[182] Digital Personal Data Protection Act, No. 22 of 2023, § 7(a) (India).
[183] Id at Section 7(b)
[184] Id at S, 7 (d)

- Employment purposes[185]

These are limited and listed exceptions, and do not grant the open-ended discretion that "legitimate interest" does under the GDPR.

2. Implications for E-Commerce and Innovation

The lack of legitimate interest in the DPDP Act could limit companies, particularly in e-commerce, ad-tech, and AI-driven personalization, where processing might occur in absence of direct consent but under business need. Most of these use cases under GDPR are permissible under Article 6(1) (f), as long as they do not prejudice individual rights.

In India, such processing would generally not be lawful unless it is in the specified limited categories under Section 7 or the user gives explicit consent under Section 6.

Although the DPDP Act is consent-centric, the GDPR provides numerous legal grounds, such as contract, legal obligation, vital interest, public interest, and legitimate interest which would help to protect the privacy as well as the functioning of the ecommerce platforms.

6.4.2. Shortage of a Framework for Legitimate Profiling and Personalization

The DPDP Act is silent on profiling, automated decision-making, or AI-based personalization. While GDPR Article 22 strictly regulates automated individual decision-making, including profiling, providing users with the right not to be subject to decisions based only on automation. 1. DPDP Act on Profiling and Automation

The Digital Personal Data Protection Act, 2023 (DPDP Act) does not set out profiling or automated decision-making, such as those based on Artificial Intelligence (AI), machine learning, or other algorithmic systems, particularly. The Act mainly deals with general principles regarding consent, notice, and duties of data processing but does not establish a dedicated regulatory regime regarding automated processing or profiling that touches the rights of individuals.

There is also no specific mention of automated decision-making in Section 6 (Consent), Section 7 (Deemed Consent), or Section 9 (Data Fiduciary Obligations). Consequently, the Act seems to be technology-neutral in its approach, but this lack of speech can lead to regulatory uncertainty, especially for industries such as e-commerce, fintech, and

[185] Id at S. 7 (h)

digital marketing, in which algorithmic profiling underlies operations. This lacuna is especially important considering the increasing use of AI systems that make or take decisions regarding individuals, such as credit scoring, dynamic pricing, targeted advertising, or tailored recommendations often without human oversight. Without such provisions, there is a danger that individuals can be exposed to significant automated decisions without effective transparency, redress, or supervision.

2. GDPR's Strong Regulation under Article 22

Conversely, the GDPR offers a detailed and rights-based approach to profiling and automated decision-making in particular through Article 22. According to Article 22(1), the GDPR stipulates that a data subject has the right not to be subject to an automated decision, including profiling, which creates legal effects pertaining to them or has a similarly significant effect on them.

This provision limits fully automated decisions, those involving no human involvement of substance, that have legal or similarly significant effects, like denial of credit, insurance, or job opportunities. Article 22(2) permits such decisions only in narrow situations:

- When necessary for the performance of a contract[186]
- When mandated by Union or Member State law [187]
- When founded on the data subject's express consent[188]

Even where such decisions are permissible, Article 22(3) requires the data controller to put in place appropriate measures to protect the data subject's rights, freedoms, and legitimate interests, including the right to obtain human intervention, to be heard and to challenge the decision. This provides a vital level of accountability and guarantees transparency in automated settings.

The GDPR also complements this with Recital 71, which speaks to the nature of the safeguards, mandating that individuals be informed of the logic behind, as well as of the importance and the intended effects of such processing.

3. Consequences for E-Commerce and Autonomy of Users

[186] GDPR, art. 22(2)(a), Regulation 2016/679, 2016 O.J. (L 119) 1.
[187] GDPR, art. 22(2)(b), Regulation 2016/679, 2016 O.J. (L 119) 1.
[188] GDPR, art. 22(2)(c), Regulation 2016/679, 2016 O.J. (L 119) 1.

The lack of such a regulatory mechanism in India's DPDP Act could be of concern to digital consumers and e-commerce players, particularly as more businesses use AI-based tools for user profiling, price automation, or personalized advertisements. In the absence of such a provision as GDPR's Article 22, Indian users would not be protected from discriminatory or black-box algorithmic practices.

E-commerce is highly dependent on algorithms for dynamic user experiences. The GDPR permits such profiling but requires transparency, safeguards, and the possibility of human review promoting both innovation and accountability. The lack of such mechanisms in DPDP provides regulatory opacity to Indian platforms

6.4.3. Lack of Data Portability and Competitive Enablement

DPDP Act makes no reference to data portability rights. GDPR Article 20 codifies the Right to Data Portability, whereby individuals can receive their personal data and transfer it to another service provider.

1. Lack of Data Portability in the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) lacks the provision for the right to data portability. Across the Act, including Section 6, which addresses the lawful basis for data processing on the basis of consent, Section 7 (assumed consent), and Section 9 (obligations of data fiduciaries), there is no provision or wording that authorizes data principals to ask for a copy of their personal data in a machine-readable form or to port that data to another data fiduciary.

This lack is considerable, especially when viewed through the prism of contemporary digital economies in which control over user data by individuals is instrumental to market competition, consumer choice, and innovation in technology. Due to the expansion of the digital economy, domestic data laws, such as those pertaining to data localization and internet filtering, could pose serious challenges to free commerce[189]. Without a legal framework for portability, customers suffer the risk of becoming locked onto specific platforms due to the inconvenience or inutility of transferring their historical data, whether from social media, cloud, or e-commerce.

[189] Drysdale & Samuel Hardwick, *China and the Global Trading System: Then and Now*, in China's 40 Years of Reform and Development: 1978–2018 431 (Ross Garnaut, Ligang Song & Cai Fang eds., ANU Press 2018).

2. GDPR Codification of the Right to Data Portability: Article 20

However, the General Data Protection Regulation (GDPR) provides a strong right to data portability in Article 20. Article 20(1) states that a data subject is entitled to obtain the personal data relating to them, which they have submitted to a controller, in a structured, commonly used, and machine-readable format.[190] Additionally, they are allowed to send those data to another controller free from interference by the initial controller.

Moreover, this right enables the data subject to ask for the direct transfer of personal data from one controller to another if it is technically possible[191]. The exercise of this right, however, is only applicable in cases where:

- The processing is pursuant to consent under Article 6(1)(a), or
- The processing is required for the performance of a contract under Article 6(1)(b),
- And processing is done through automated means (Article 20(1) (a)–(b)).

3. Competitive and Operating Consequences

The GDPR way promotes more interoperability among services and user portability without the threat of losing access to their data. This is especially vital in promoting level competition for digital service providers and lessening the likelihood of data monopolies. By giving power to users to own their data, GDPR allows market forces to act more freely and smaller, privacy-oriented platforms to compete with giants.

But the DPDP Act's exclusion of a data portability clause undermines the legal framework necessary to enable consumer-led data ecosystems. Without portability, there is less pressure on service providers to compete on data privacy, user experience, or ethical AI behaviours. This harms consumer liberty but also decelerates innovation in digital services.

India's DPDP Act is missing this element now, but sectoral rules or amendments in the future can bring about a right of data portability either through a rule-making process delegated to the Government or through special guidelines by the Data Protection Board of India. Having this inclusion will bring India's system in line with international best

[190] GDPR, art. 20(1), Regulation 2016/679, 2016 O.J. (L 119) 1.
[191]General Data Protection Regulation, Art 20(2)

practices and bolster consumer rights within the fast-growing e-commerce and digital services environment.

6.4.4. Unclear Mechanism for Cross-Border Data Transfers

GDPR only allows cross-border transfers of data to jurisdictions with suitable data protection regimes or through measures such as Standard Contractual Clauses (SCCs)[192] or Binding Corporate Rules (BCRs)[193]. This keeps the personal data of EU residents from being exported to jurisdictions that have lower protections, thus retaining a high standard of protection even in cross-border situations. Nonetheless, these prohibitions can establish legal and operational bottlenecks for international e-commerce platforms.

DPDP Act takes a more permissive approach. It permits the export of personal data outside India except if the central government notifies a particular nation as being restricted[194]. This default favouring can help ease cross-border digital trade and cloud services. Although this stance diminishes regulatory resistance for internationally operating e-commerce parties, it can undermine India's hold on the usage and preservation of Indian citizens' data abroad, particularly in places where there is weak data protection regulation. Section 16 permits cross-border data transfers, upon government notification, without defining the criteria or mechanisms.

GDPR Chapter V (Articles 44–50) provides well-defined rules for cross-border data transfers, including adequacy decisions, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs).

1. Permissive but Ambiguous Framework under the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 takes a relatively permissive approach to cross-border data transfers. As per Section 16(1) of the Act, the Central Government, by notification, can prohibit the transfer of personal data by a data fiduciary to certain countries or territories if it finds such a transfer prejudicial to the interests of the data principal or to the sovereignty and integrity of India.[195] This means that in the absence of such a notification, data can freely travel across borders.

[192] General Data Protection Regulation, art. 46(2) (c)–(d), 2016 O.J. (L 119) 1.
[193]General Data Protection Regulation, art. 47, 2016 O.J. (L 119) 1.
[194] Digital Personal Data Protection Act, No. 22 of 2023, s. 16
[195]Id S. 16(1)

Yet, the Act does not set objective criteria or assessing factors for determining "safe" or "unsafe" jurisdictions. Nor does it have legal tools such as contractual protection, adequacy findings, or binding company rules to validate transfers. The lack of rule-based arrangements brings an important aspect of regulatory uncertainty, especially for internet market places facilitating cross-border processing of consumer's data. Where there is no guidance under statute, the risk of ad-hoc executive action can impinge upon business continuity and consumer confidence.

2. Organized and Rights-Based Regime under the GDPR

The General Data Protection Regulation (GDPR) has a systemic and integrated regime under Chapter V (Articles 44 to 50). As provided under Article 44, any transfer of personal data to a third country shall ensure that the level of protection is not diminished.[196]

Article 45 states that the European Commission can find that a third country provides an adequate level of protection, under which personal data may be transferred with no other protection.[197] Where there is no adequacy decision, Article 46 makes transfers permitted based on suitable safeguards, e.g, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or codes of conduct that provide effective rights and accessible legal remedies.[198]

Article 49 enumerates precise derogations, including the clear consent of the data subject, transfers required by performance of the contract, or for reasons of significant public interest. These provisions taken together provide a multi-tiered, transparent, and accountable process to enable international data flows and ensure continuity of protection to the data subjects.

3. Practical Impact on E-Commerce and Cross-Border Trade

The GDPR's hierarchical framework offers certainty and legal predictability, enabling e-commerce websites, cloud service providers, and online advertisers to conduct business with more assurance across borders. By giving rise to both legal tools and

[196] GDPR, art. 44, Regulation 2016/679, 2016 O.J. (L 119) 1.
[197] Id. art. 45.
[198] Id. art. 46.

procedural protection, the GDPR framework ensures that personal data maintains its protective armour even when it is sent abroad.

On the other hand, the DPDP Act's dependence on sweeping executive powers lacking statutory guidelines may discourage international digital service providers from setting up data operations in India or catering to Indian consumers. Uncertainty might also lead to decreased foreign investment and interoperability issues, particularly in sectors depending on international data infrastructure.

To align its data transfer regime with international best practices, India might consider including adequacy determinations comparable to Article 45 GDPR, Facilitating transfers on the basis of contractual or organisational controls, such as Article 46 GDPR, Providing for narrowly targeted derogations according to Article 49 GDPR and establishing transparency requirements for the executive in imposing transfer restrictions.

This would harmonize with international best practices, minimize compliance costs, and enhance international confidence and cooperation in digital trade, without sacrificing sovereignty over sensitive data flows.

The absence of specificity under the DPDP Act creates doubt for multinational platforms. On the contrary, GDPR's comprehensive structure guarantees legal certainty, which is essential for e-commerce companies leveraging international infrastructure

6.4.5. Limited Recognition of Consumer Rights and Objection Mechanisms

DPDP Act gives the right of consent withdrawal (Section 6(5)) but does not have provisions for objecting to the processing of data or restricting its use.

GDPR Articles 18 and 21 entitle users to the right to restrict processing and object to processing, particularly direct marketing.

The Digital Personal Data Protection Act, 2023 (DPDP Act) only grants a limited extent of user control over continuous processing of data. Under Section 6(5) of the DPDP Act, a data principal i.e the person may withdraw consent at any time, after which the data fiduciary is required to stop further processing of personal data.[199] Yet, the withdrawal does not impair the legality of the processing that has been done prior to

[199] Digital Personal Data Protection Act, No. 22 of 2023, § 6(5) (India).

such withdrawal. Although this provision recognizes the dynamic control of the individual over their consent, the Act is not bestowing a general right to object to processing that does not have consent as its basis such as statutory processing or public interest processing. It also does not have the right to limit processing, where users cannot ask for a temporary restriction or limitation of the use of their data in certain situations.

As compared to the General Data Protection Regulation (GDPR), the latter has a wider and more sophisticated basis for user control of personal data processing. Under Article 18, data subjects have the right to restriction of processing, which enables individuals to suspend temporarily the processing of their data while the data's accuracy is disputed or a valid objection is being considered. More importantly, [200]GDPR creates the right to object to processing, including the right to object at any time to processing for purposes like direct marketing. Where objection is expressed, the data controller is under an obligation to stop processing unless it is able to show compelling legitimate grounds which prevail over the interests, rights, and freedoms of the individual.

This multi-layered design in the GDPR enables users to have control over the processing of their personal data, enhancing the norms of user autonomy and proportionality. The lack of such rights in the DPDP Act can come in the way of exercising informational self-determination effectively, especially in areas of targeted advertising, algorithmic recommendation, and profiling, which are core to digital and e-commerce platforms.

6.4.7. Lack of Incentives for Innovation and Ethical Processing

DPDP Act passes reference to data minimization (Section 8(1) (b) but has no directives on privacy by design or default.

While Article 25 of GDPR imposes privacy by design and by default, inviting organizations to integrate privacy into product design.

1.Lack of Incentives to Innovate and Ethical Processing

The Digital Personal Data Protection Act, 2023 (DPDP Act) shows only a partial commitment to encouraging ethical innovation or to instilling privacy-respecting values

[200] GDPR, art. 21, Regulation 2016/679, 2016 O.J. (L 119) 1.

in the design of digital technologies. Although Section 8(1)(b) of the Act cursorily mentions the principle of data minimization, that a data fiduciary must ensure the personal data processed is restricted to such data which is required for the stated purpose[201], it falls short of even identifying any affirmative obligation to construct systems or processes with privacy in mind as a default setting. There are no specific provisions that support or require "privacy by design" or "privacy by default" approaches, and there lies an absence of proactive regulatory measures that can encourage ethical data governance. In order to facilitate societal change, policymakers have also acknowledged the potential importance of data-driven innovations utilizing big data and open data. Policymakers in Europe have combined their agendas on open data, big data, and open access in the hopes of generating important innovations and competitive advantages[202].

In reality, this lack means that Indian data fiduciaries, such as digital companies and e-commerce sites, can technically meet the law's letter with reactive steps like consent or recording, but not be incentivized or mandated to incorporate privacy measures structurally in the design of their systems. This can undermine the long-term growth of trust-based innovations like privacy-enhancing technologies, fairness-checked AI, or products permitting user-controlled specification of data-sharing levels.

On the other hand, the General Data Protection Regulation (GDPR) establishes a specific and enforceable commitment to combining privacy and ethics in technology and system design. Under Article 25, it is a statutory obligation of controllers to apply data protection by design and by default. Therefore, privacy is to be woven into every product and service design, not be used as add-ons. Suitable technical and organisational measures such as pseudonymization, data minimisation and encryption are supposed to be utilized by organisations when planning and while operating the process of data treatment.

Most importantly, the "by default" provision under Article 25(2) mandates that, by default, only necessary personal data for every given purpose is processed and that such data is not made available to an unspecified number of people without the individual's

[201] Digital Personal Data Protection Act, No. 22 of 2023, § 8(1)(b) (India).
[202] Bridgette Wessels et al., *Big Data, Open Data and the Commercial Sector*, **in** Open Data and the Knowledge Society (Amsterdam Univ. Press 2017).

action.[203] This regulation guarantees that user privacy is maintained even when users do not intervene actively in modifying privacy settings thus instilling a legal context that supports ethical design, user dignity, and data economy efficiency.

By so providing, the GDPR establishes a regulatory incentive regime that supports innovation for privacy-oriented values and competition on data responsibility grounds. This not only bolsters consumer confidence in digital systems but also promotes sustainable e-commerce development by instilling privacy as a competitive advantage.

Such principles in GDPR establish a pro-innovation approach that incentivizes ethical processing and technological savvy. Their omission in DPDP foregoes the chance to bring India's privacy framework on par with international best practices in ethical digital innovation

6.4.8. Absence of Right to Object

The DPDP Act doesn't have any specific provision wherein users can object to the data processing. Withdrawing consent[204] is recognized, but it goes no further in granting an unconditional right to object or limit usage of data. While Article 21 of GDPR provides the Right to Object, which enables individuals to object to data processing on specific grounds, mainly direct marketing. Article 18 also offers the Right to Restrict Processing, where users can restrict the processing of their data under specific circumstances.

1.Limited Mechanisms for Objection and Restriction of Data Processing

The Digital Personal Data Protection Act, 2023 (DPDP Act) offers limited means for data principals to object to data processing. The only main right granted in the DPDP Act is the right to withdraw consent under Section 6(5). While this enables individuals to prevent further processing of their personal data, it does not establish a more unconditional right to object to the processing of their data, nor does it offer mechanisms to limit or restrict data usage. The Act does not have specific provisions similar to the Right to Object or Right to Restrict Processing of the GDPR. This absence of strong objection mechanisms places individuals with minimal control over processing of their personal data after consent has been provided, and limits their ability

[203] GDPR, art. 25(2), Regulation 2016/679, 2016 O.J. (L 119) 1.
[204] Digital Personal Data Protection Act, No. 22 of 2023, § 6(5) (India).

to object to processing in instances where data is processed for purposes other than consent for compliance with legal obligations or public interest.

However, the General Data Protection Regulation offers a better framework for users to exert control over their data. People can object to the processing of their personal data for certain purposes. The existence of such a particular circumstance needs to be investigated case-by-case.[205] In Article 21, the GDPR gives individuals the Right to Object to the processing of their data on various grounds, most significantly when data is being processed for direct marketing. This enables users to halt the processing of their data if they are opposed to its use for commercial or promotional purposes, so that people are not exposed to unwanted solicitations or profiling without their permission. Notably, the GDPR grants individuals the right to object at any moment to data processing for direct marketing purposes, which allows users to more easily retain control over the use of their personal data in commercial situations. This right also applies to other forms of processing, such as profiling, subject to specified conditions. The data subject must provide "compelling legitimate grounds" for their objection and the processing need only stop if the objection is valid.[206]

Additionally, the GDPR also provides the Right to Restrict Processing[207], which enables individuals to suspend data processing temporarily under certain conditions. For instance, if the accuracy of personal data is in question, the individual can request a restriction on processing until the matter is resolved. Alternatively, if processing is illegal but the person doesn't wish to have the data deleted, then they can request a processing restriction instead. This added protection within the GDPR gives people greater levels of control over their data through mechanisms to freeze or limit usage, particularly where users are in doubt about the accuracy of the data or over the grounds on which it will be processed.

In the context of e-commerce, the Right to object is critical to users, particularly in direct marketing or commercial profiling scenarios. It provides consumers with more control over their personal data and deters unwanted data exploitation. The DPDP Act's

[205] European Commission, What Happens if Someone Objects to My Company Processing Their Personal Data?, EUR.COMM'N,https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/dealing-citizens/what-happens-if-someone-objects-my-company-processing-their-personal-data_en.
[206]Bird & Bird, *Guide to the GDPR: Rights to Object*, https://www.twobirds.com/-/media/pdfs/gdpr-pdfs/33--guide-to-the-gdpr--rights-to-object.pdf?la=en
[207] GDPR, art. 18, Regulation 2016/679, 2016 O.J. (L 119) 1.

exclusion of this right exposes users to repetitive marketing and other type of unwanted data processing. This lack also results in regulatory ambiguity for online businesses, as the equilibrium between consumer privacy and commercial interests cannot be defined. On the other hand, the explicit provisions of the GDPR increase consumer confidence and promote more transparent business operations.

6.4.9. Scope of the Right to be forgotten

The Right to be forgotten is addressed in the DPDP Act, with under s. 12 as right to erasure but not having strong provisions that specifically empower individuals to have their data deleted on demand. Article 17 of the GDPR formulates the Right to be forgotten, as it permits data subjects to seek erasure of their personal data when it is no longer needed for the purpose it was collected or when the consent is withdrawn.

1.Right to be Forgotten and Deletion of Data

The necessity of forgetting and the balance between memory and recall have changed. The pendulum of memory and recording concepts has swung in favour of digital technology.[208] The Digital Personal Data Protection Act, 2023 (DPDP Act) is a limited recognition of the Right to be Forgotten, commonly invoked in terms of data erasure or the right to request that personal data be erased. As compared to the GDPR, which extends across all personal data irrespective of the legal basis for processing, the DPDPA limits this right mainly to personal data that has been obtained with consent and not data that has been processed on other grounds of law. The DPDPA also applies only to electronic data, excluding non-electronic records, as opposed to the GDPR, which covers all types of personal data. The DPDPA does not have specific timelines for acting on erasure requests, which may lead to delays, whereas the GDPR requires a quick response within one month. In addition, the DPDPA permits data fiduciaries to hold data if needed for the original purpose or legal requirements, with wider exceptions than the GDPR's more limited grounds. Unlike the GDPR, the DPDPA does not have an express requirement to notify third parties to delete data that was shared, thus curbing the efficacy of erasure requests. Enforcement means under the DPDPA continue to mature and are less effective than the existing regulatory framework of the GDPR and

[208] Binoy Kampmark, *To Find or Be Forgotten: Global Tensions on the Right to Erasure and Internet Governance*, 2 J. Global Faultlines 1 (2015).

hefty penalties. In general, the DPDPA's right to be forgotten is less in scope, less clear, and more difficult to enforce

By comparison, the General Data Protection Regulation (GDPR) is far more comprehensive and robust in its approach to data erasure in Article 17, referred to as the Right to Erasure, or the Right to be forgotten. The data subjects have the right to obtain the erasure of their personal data when it is no longer required for the purposes for which it was originally processed or where the individual withdraws the consent, subject to the condition that the processing is based on consent.[209] This provides people with the right to ask for their data to be deleted in a range of circumstances, including where they no longer want their data to be processed, or where it has been processed illegally. The European Court of Justice (ECJ) ruled that Google, as a search engine operator, must remove any links to personal websites from the list of search results if the information is irrelevant to the reasons the data was gathered or processed and given the passage of time.[210] To put it briefly, the ECJ demanded that the fundamental rights of the data subject be balanced with the legitimate interest in information access.[211]

Moreover, GDPR's Article 17(1) contains some exceptions where the right to erasure does not hold, such as where the processing is necessary for compliance with a legal obligation or for the purposes of establishment, exercise, or defence of legal claims. In spite of these exceptions, the GDPR guarantees that the right to be forgotten is an evident, enforceable right that may be exercised in various contexts and gives individuals control over their right to privacy.

This right to erasure is a key feature of the GDPR's user-centric privacy framework, ensuring that individuals can regain control over their personal data when they no longer wish it to be retained, especially in an age where personal data is widely shared across various platforms. The lack of such a scope in the DPDP Act dilutes the possibility for Indians to have control over their own personal information and privacy as consumers in the EU have.

[209] GDPR, art. 17(1), Regulation 2016/679, 2016 O.J. (L 119) 1.
[210] Google v. Agencia Española de Protección de Datos, Case C-131/12, [2014] E.C.R. I-0000.
[211] Bill Hannay, *The Long Arm of the Law*, in *Roll with the Times, or the Times Roll Over You: Charleston Conference Proceedings, 2016* 50 (Beth R. Bernhardt, Leah H. Hinds & Katina P. Strauch eds., Purdue Univ. Press 2017).

The Right to be forgotten is essential in the e-commerce sector, as it provides a mechanism for people to have their information erased from websites that do not need it anymore. The right helps maintain the privacy of users and enables digital rights of citizens, allowing them to erase their personal data that can be utilized to discriminate against or cause harm to them in the future. The DPDP Act's limited scope of such a right is diametrically opposite to the GDPR, which provides a clear mechanism for erasure of data. Companies may lose business reputations if consumers are unable to control their data, leading to loss of consumer confidence and trust in Indian e-commerce sites.

6.4.10. Regulatory Bodies and Enforcement

The GDPR is enforced by independent supervisory authorities established in each EU member state. These authorities have far-reaching investigative and corrective powers, including the power to levy substantial administrative fines of up to €20 million or 4% of worldwide annual turnover. This strong enforcement apparatus enforces solid accountability and deterrent.

In comparison, the DPDP Act sets up a central Data Protection Board of India (DPBI) that will process complaints, give directions, and impose fines. The DPBI is likely to adopt a more consultative and curative style. While this might lower apprehension of stringent penalties and facilitate compliance through education and advice, its centralization and possible executive control could give rise to doubts about independence and impartiality. The DPA may find it difficult to develop internal capacity due to its cross-sectoral mandate, which could result in either excessive or insufficient regulation. While the DPA would impose needless difficulties on compliant enterprises, the low regulatory capacity would undermine the purpose of the bill.[212] Moreover, delay in enforcement can weaken the overall effectiveness of the regime.

6.4.11. Provisions in DPDP That Could Slow Down E-Commerce

[212] Anirudh Burman, *The Growth of Privacy Regulation and the Bill*, in *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?* (Carnegie Endowment for Int'l Peace 2020), http://www.jstor.com/stable/resrep2429.

Though business-friendly in its design, some provisions under the DPDP Act could end up slowing down e-commerce by default. The imprecise language regarding "deemed consent" could cause inconsistent interpretations and legal ambiguity, particularly in the areas of customer profiling and targeted advertising. The removal of "legitimate interest" as a legal ground also limits companies from justifying processing without consent, which is vital for activities such as fraud detection and analytics. In addition, the absence of data portability hinders interoperability across platforms, thus diminishing user mobility and constraining competition in the e-commerce environment.

6.5. HOW GDPR MAINTAINS BALANCE BETWEEN PRIVACY AND E-COMMERCE

The GDPR strikes a delicate balance between data protection and commercial innovation by blending flexibility into a robust legal framework. The inclusion of "legitimate interest" permits companies to process information without subject consent under specific safeguards, enabling functions like marketing, user behaviour analysis, and optimizing services. Additionally, GDPR's proportionate approach to risk guarantees that compliance obligations are in line with the size and nature of data processing activities. Small and medium-sized businesses (SMEs) enjoy exemptions in cases like record-keeping and DPIAs, depending on the risk. Through the imposition of harmonized standards and contractual arrangements for cross-border transfers, GDPR provides legal certainty and trust, both of which are essential to the success of e-commerce.

6.6. COMPARATIVE ANALYSIS OF DPDP ACT WITH GDPR

	DPDP Act, 2023 (India)	GDPR (EU)
Scope	Applies to digital personal data in India, including processing outside India if in connection with goods/services	Applies to all personal data processed by controllers/processors in the EU or targeting EU individuals

Legal Basis for Processing	Consent and legitimate uses (broader and includes deemed consent)	Consent, contract, legal obligation, vital interests, public task, legitimate interests
Data Subject Rights	Access, correction, erasure, grievance redressal	Access, rectification, erasure, restriction, portability, objection, not to be profiled
Right to Be Forgotten	Yes (limited)	Yes (comprehensive)
Data Portability	Not explicitly provided	Explicitly provided
Profiling and Automated Decision-Making	Not clearly restricted	Right to object to automated decisions, including profiling
Data Protection Authority	Data Protection Board of India (government-appointed, not independent)	Independent Supervisory Authorities in each EU member state
Cross-border Data Transfer	To be regulated by notified countries (not yet defined)	Requires adequacy decisions or appropriate safeguards
Penalties	Up to Rs.250 crore	Up to EUR20 million or 4% of global turnover
Exemptions	Broad exemptions for government (national security, research etc.)	Limited exemptions, subject to necessity and proportionality
Data Breach Notification	Mandatory, but specifics to be notified	Mandatory within 72 hours to authority, affected subjects if high risk

6.7 CONCLUSION

Despite its best efforts, the DPDP Act of 2023 falls short of providing the innovative, business-friendly structure that the e-commerce sector requires. It favours a constricted consent-based approach to a balanced rights-and-risk-based system such as the GDPR.

As a consequence, Indian platforms might struggle with international interoperability, customer trust, and compliance transparency. With the adoption of provisions such as legitimate interest, right to object, data portability, and independent oversight, India can consolidate consumer rights and digital market growth.

The omission of major provisions such as the Right to Data Portability, the Right to Object, and the Right to be forgotten in the DPDP Act also makes it increasingly difficult for India to conduct e-commerce. Though these rights are integrated into the GDPR, balancing consumer privacy against business interests fairly, the lack of such under the DPDP Act threatens to curtail consumer agency and marketplace competition in India's expanding e-commerce market. Additionally, such exclusions diminish Indian businesses' capacity to compete according to best international practices and hamper interoperability on the global stage. To safeguard both consumer welfare and industry growth, India should consider incorporating these rights into its framework, ensuring a more holistic and future-proof data protection environment.

CHAPTER 7

FINDINGS, SUGGESTIONS AND CONCLUSION

The comparative study shows that the GDPR provides a more prescriptive and precautionary legal regime, best suited for sophisticated digital economies with developed regulatory architectures. Most importantly, the GDPR maintains a better balance in terms of flexible legal foundations, proportionate duties, and institutional resilience but DPDP Act lacks that balance. The absence of data portability provisions, robust objection mechanisms, and privacy by design may undermine the development of an innovative and privacy-aware e-commerce environment in India. Moreover, the Act's emphasis on consent as the data-processing basis and its poor data-transfer framework across borders can be a source of friction for companies, especially in today's globalized e-commerce environment. By incorporating more robust privacy rights, regulatory incentives for businesses to ethically innovate, and cross-border data flow mechanisms, the DPDP Act would be able to align more closely with international privacy standards and create an e-commerce environment that balances consumer confidence with business development.

7.1 FINDINGS

On a comparison of the provisions of the Digital Personal Data Protection Act, 2023 (DPDP Act) with the General Data Protection Regulation (GDPR), the following conclusions can be drawn about their likely effect on e-commerce in India:

1. Limited Consumer Control and Objection Mechanisms:

Although the DPDP Act acknowledges the significance of consent withdrawal (Section 6(5)), it is not well-equipped with provisions to enable users to object to data processing or limit its use. In contrast to the GDPR, which provides extensive rights to object and limit processing, the DPDP Act grants limited relief for people to contest the processing of personal data. This limits user’s control over how they can protect their privacy, particularly in online shopping environments where shoppers can be subjected to direct marketing or data profiling.

2. Data Portability Gap:

The Right to Data Portability under Article 20 of the GDPR allows users to port their data between service providers, making consumers more mobile and promoting market

competition. The DPDP Act, however, lacks such a provision, which may impede competition in the e-commerce market and trap consumers in sites where data portability is not easy. The absence of portability of data can lower new e-commerce platform's competition power since new platforms are unable to easily bring customers who are already rooted in current platforms.

3. Privacy by Design and Default:

The GDPR insists on privacy by design and default under Article 25, and it demands that organizations build in privacy protections at the development stage. This promotes moral data behaviour and facilitates long-term business-consumer trust. But the DPDP Act does not contain provisions that mandate similar principles, which might slow down the growth of privacy-respecting technologies in India. This lack might result in a lack of incentives for e-commerce businesses to innovate with privacy as a consideration, which might lead to data practices that are more focused on business convenience than consumer privacy.

4. Right to Be Forgotten:

The Right to Be Forgotten, entrenched in Article 17 of the GDPR, provides users with the right to have their personal information removed when no longer required or where consent has been revoked. The DPDP Act has a similar provision but the scope is limited. This curtails the power of data subjects to request the erasure of their personal data, which might be detrimental to consumers who want to exert control over their personal information in the online environment, such as in e-commerce websites where data retention may result in privacy threats.

5. Regulatory Gaps and Innovation:

Although the DPDP Act sets up a regulatory environment for data protection, it does not extend to the same level as the GDPR in encouraging innovation in privacy-friendly e-commerce solutions. The emphasis of the GDPR on privacy by design and the Right to Data Portability promotes the creation of ethical and competitive business models in e-commerce, which is not explicitly promoted by the DPDP Act. The lack of such provisions may restrict the scope of Indian e-commerce company's ability to be at the forefront of privacy innovation and gain the trust of consumers.

6. Consent Mechanism:

The DPDP Act highlights the significance of informed consent (Section 6) with the provision that data processing shall be subject to clear, specific, and unambiguous consent. Though this is consistent with the GDPR focus on explicit consent (Article 6), the Act fails to provide adequate flexibility in situations where legitimate interests or other legal grounds for processing, such as those under the GDPR, may be applicable. Such over-reliance on consent as the fundamental legal basis may unduly weigh on e-commerce enterprises, especially in situations of run-of-the-mill business operations or data processing for administrative purposes. E-commerce sites could struggle to obtain repeated consents for everyday activities from users, which may adversely affect the speed of user experiences or the efficiency of operations.

7. Cross-Border Data Transfers:

The DPDP Act does cover cross-border data flows, mandating that personal data can only be transferred to states that offer an adequate standard of protection of data (Section 15). But, it does not specify a specific mechanism for compliance or offer an effective safeguards framework similar to the GDPR's standard contractual clauses or Binding Corporate Rules (BCRs) for cross-border data transfers. This would potentially create important challenges for globally operating e-commerce companies, particularly those engaged in global customer data transfer or cross-jurisdictional operations. Companies could be subject to more legal and regulatory complexities when moving data across borders, which could cause delays in operations or higher compliance expenses.

7.2 RECOMMENDATIONS

Some recommendations are as follows:

1. Including Stronger Objection and Restriction Provisions:

The DPDP Act can be improved by including provisions like the GDPR's Right to Object and the Right of Restriction of Processing. These mechanisms would give people greater control over how their data is handled, particularly where direct marketing and profiling are concerned, which are of most importance in e-commerce. By giving users the right to object to processing or ask data usage to be restricted, the Act would be more in line with international privacy standards and give consumers greater control over their data.

2. Introduction of Data Portability:

Introducing a Right to Data Portability would greatly increase the competitiveness of the Indian e-commerce industry. Permitting consumers to port their data smoothly between service providers would not only facilitate transparency but also attract new market entrants. It would make the ecosystem more competitive by allowing customers to change platforms without any loss of data, thereby motivating businesses to improve their services and serve consumer requirements better.

3. Incorporating Privacy by Design and Default:

The DPDP Act may include provisions similar to Article 25 of the GDPR, which requires privacy by design and privacy by default. This would motivate e-commerce companies to incorporate privacy features into their systems at the outset, minimizing the need for remedial measures later. Additionally, by integrating privacy at the very fabric of digital products, Indian companies would be better equipped to take advantage of increasing global demand for privacy-oriented services.

4. Enhancing the Right to Be Forgotten:

A clearer Right to Erasure, akin to the GDPR's Right to Be Forgotten (Article 17), should be included in the DPDP Act. This would empower individuals more with respect to their personal data, enabling them to ask for its deletion when it is no longer required or on withdrawal of consent. This provision would enhance privacy safeguards and ensure that online commerce sites do not store data unnecessarily, thereby strengthening consumer confidence in electronic transactions.

5. Innovation in Privacy-Friendly E-Commerce Paradigms:

The DPDP Act ought to encourage companies to innovate privacy-friendly technologies by making privacy a competitive advantage. This can be done through tax incentives, regulatory accolades, or certification schemes for companies that practice privacy by design principles. Furthermore, the government may encourage the adoption of data protection-friendly technologies like encryption and anonymisation, so that Indian e-commerce websites are not only ahead in terms of privacy compliance aspect but also in terms of technological advancement.

6. Cross-Border Data Transfers:

The DPDP Act must clarify cross-border data transfer's framework, offering standard contractual clauses or BCRs, akin to those under the GDPR. This would ease smoother data exchanges between India and other jurisdictions, especially in the e-commerce space, where companies must process large amounts of customer data across borders. Clarity in guidelines would also enable Indian companies to position their practices according to global norms and mitigate the risk of non-compliance with international data protection regulations.

7. Equilibrating Consent with Legitimate Interests:

The DPDP Act may examine adding legitimate interest as a secondary legal basis for processing, following the GDPR's Article 6(1) (f). Businesses would be enabled to process personal data without the need for express consent, provided that their legitimate interests are predominant over the data subject's rights. This degree of flexibility would minimize operational onuses for e-commerce sites, particularly in the case of data processing that occurs routinely, and simplify business practices while ensuring robust consumer privacy measures.

7.3 CONCLUSION

In conclusion, although the Digital Personal Data Protection Act, 2023 (DPDP Act) does not in itself discourage the development of e-commerce in India, some provisions of the Act can pose operational difficulties for companies in the industry. The fundamental goals of the DPDP Act, including the preservation of consumer privacy and safeguarding personal data, are in line with international standards and are favourable to the establishment of a secure digital transaction environment. However, some specific aspects of the Act, such as the lack of data portability rights, the limited scope for objecting to data processing, and the absence of privacy by design provisions, could complicate the operational flexibility that e-commerce platforms require to withstand in an increasingly globalized market.

For example, the DPDP Act's insistence on express consent as the foremost ground for data processing may make processes for business cumbersome, especially in the handling of routine data operations. It may hinder the speed of transactions and impact user experience, which is essential for e-commerce. Likewise, the absence of measures related to cross-border data transfers and data portability can generate legal uncertainty

and impede the facility with which Indian companies can move globally, thus impacting their competitiveness in foreign markets.

On that note, they are not impossible to overcome. With some fine-tuning, including the addition of legitimate interest provisions, more precise guidelines for cross-border data flows, and enhanced privacy by design incentives, the DPDP Act can more effectively balance privacy protection with the operational requirements of e-commerce platforms. Thus, although the DPDP Act is a much-needed legislation for data protection, its existing provisions must be made more precise so that e-commerce companies can still develop and innovate without sacrificing consumer privacy.

In short, the DPDP Act does not directly inhibit e-commerce expansion, but some provisions might cause operational challenges that could supress its potential unless rectified through more adaptable and holistic data protection policies.

BIBLIOGRAPHY

BOOKS

1. Bygrave, Lee A., Data Privacy Law: An International Perspective (Oxford University Press 2014).
2. Kamath, Nandan, Law Relating to Computers, Internet & E-Commerce (Universal Law Publishing Co. Pvt. Ltd. 2007).
3. Sharma, S.R., Laws on E-Commerce (Anmol Publications Pvt. Ltd. 2004).
4. Ramappa, T., Legal Issues in Electronic Commerce (Macmillan India Ltd. 2003).

ARTICLES

1. Sasha Romanosky, Rahul Telang and Alessandro Acquisti, Data Breach Disclosure Laws Reduce Identity Theft?, JPAM, 30(2), 256-286,(2011)
2. W. Gregory Voss, Katherine Woodcock, David Dumont, Nicholas D. Wells, Jonathan I. Exor, João Luís Traça, Bernardo Embry and Fatima Khan, The International Lawyer,46(1), 97-112,(2012)
3. Patial, Tushar & Gupta, Aashi, Balancing Privacy and Accountability: A Closer Look at India's DPDP Act of 2023, 6 Indian J. L. & Legal Research 6709 (2023).
4. Kumar Abhishek, Deep Prabhat, Raghuvanshi Shivam & Kumar Vivek, India’s New Data Frontier: A Critical Legal Insight of the Personal Data Protection Act, 2023, 44 Library Progress Int'l 3 (2024).
5. CA Shagun Kabra and Ms. Khyati Lad, Advancement of Technology, Lack of Privacy: Pre-Requisite of the Digital Personal Data Protection Act, 2023.
6. Edwin Black, IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation (2001).
7. Marc Langheinrich, Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems, Distributed Systems Group, Institute of Information Systems, IFW Swiss Federal Institute of Technology, ETH Zurich, 8092 Zurich, Switzerland

8. Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z., The European Union General Data Protection Regulation: What It Is and What It Means, 28 Info. & Commc'ns Tech. L. 65 (2019)
9. Anirudh Burman, The Growth of Privacy Regulation and the Bill, in Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? (Carnegie Endowment for International Peace, 2020)
10. Hortaçsu, Ali & Syverson, Chad, The Ongoing Evolution of US Retail: A Format Tug-of-War, 29 J. Econ. Persp. 89 (2015).
11. Jain, Vipin, Malviya, Bindoo, & Arya, Satyendra, An Overview of Electronic Commerce (e-Commerce), 27 J. Contemp. Issues Bus. & Gov't 1 (2021), https://cibg.org.au/.
12. Schramm-Klein, Hanna & Wagner Gerhard, Broadening the Perspective on E-Commerce: A Comparative Analysis of Mobile Shopping and Traditional Online Shopping, 36 Marketing: ZFP - Journal of Research and Management 119 (2014).
13. Johnston, Lauren A., World Trade, E-Commerce, and COVID-19, 21 China Review 65 (2021).
14. Khan, Lina M., The Separation of Platforms and Commerce, 119 Columbia L. Rev. 973 (2019).
15. Halder, Debarati & Karuppannan, Jaishankar, Cyber Crime and the Victimization of Women: Laws, Rights and Regulations (2012)
16. Hallinan, Dara, Friedewald, Michael & McCarthy, Paul, Citizens' Perceptions of Data Protection and Privacy in Europe, 28 Computer L. & Sec. Rev. 263 (2012).
17. Chakraborty, Rajarshi, Lee, Jaeung, Bagchi-Sen, Sharmistha, Upadhyaya, Shambhu & Rao, H. Raghav, Online Shopping Intention in the Context of Data Breach in Online Retail Stores: An Examination of Older and Younger Adults, 83 Decision Support Sys. 47 (2016).
18. Kelly D., Borah, Abhishek & Palmatier, Robert W., Data Privacy: Effects on Customer and Firm Performance, 81 J. Marketing 36 (2017), https://doi.org/10.1509/jm.15.0497.

19. Kumari, Mamta, Sinha, Pallav Chandra & Priya, Sannu, The Impact of Data Breaches on Consumer Trust in E-Commerce, 4 Int'l J. Current Sci. (IJCSPUB) 1 (2014), available at www.ijcspub.org.
20. Taylor, Mark J. & Paterson, Jeannie Marie, Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection, 16 Indian J. L. & Tech. 1 (2020), available at https://repository.nls.ac.in/ijlt/vol16/iss1/4.
21. Jan Philipp Albrecht, How the GDPR Will Change the World, 2 EUR. DATA PROT. L. REV. 287 (2016).
22. Degeling, Martin, Utz, Christine, Lentzsch, Christopher, Hosseini, Henry, Schaub, Florian & Holz, Thorsten, We Value Your Privacy... Now Take Some Cookies, 42 Informatik Spektrum 345 (2019).
23. Michelle Chivunga & Alistair Tempest, Digital Disruption in Africa: Mapping Innovations for the AFCFTA in Post-COVID Times, South African Inst. of Int'l Aff. (2021).
24. Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, 53 J. Indian L. Inst. 663 (2011).
25. Cybersecurity and Privacy Issues Facing Smart Cities, in Cyber Infrastructure Protection Volume III (Strategic Studies Inst., U.S. Army War Coll. 2017).
26. Mark Linscott & Anand Raghuraman, Aligning India's Data Governance Frameworks (Atlantic Council 2020).
27. Atul Singh, Data Protection, 59 J. Indian L. Inst. 78, 78–101 (2017).
28. Simon Davies, The Data Protection Regulation: A Triumph of Pragmatism over Principle?, 2 EUR. DATA PROT. L. REV. 290 (2016).
29. Drysdale & Samuel Hardwick, China and the Global Trading System: Then and Now, in China's 40 Years of Reform and Development: 1978–2018 431 (Ross Garnaut, Ligang Song & Cai Fang eds., ANU Press 2018).
30. Bridgette Wessels et al., Big Data, Open Data and the Commercial Sector, in Open Data and the Knowledge Society (Amsterdam Univ. Press 2017).
31. Binoy Kampmark, To Find or Be Forgotten: Global Tensions on the Right to Erasure and Internet Governance, 2 J. Global Faultlines 1 (2015).

STATUTES

1. Universal Declaration of Human Rights, art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).

2. "Freedom of Information Act (FOIA)," U.S. Department of Justice, https://www.foia.gov/about.html (last visited Apr. 24, 2025).
3. OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, OECD (2013), https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.
4. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, Jan. 28, 1981.
5. UNCITRAL Model Law on Electronic Commerce, United Nations Commission on InternationalTradeLaw,https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.
6. Data Protection and Privacy Legislation Worldwide, United Nations Conference on Trade and Development (UNCTAD), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
7. International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171.
8. Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.
9. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Dec. 18, 1990, 2220 U.N.T.S. 3.
10. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.
11. American Convention on Human Rights, Nov. 22, 1969, 1144 U.N.T.S. 123.
12. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, (India)
13. Digital Personal Data Protection Act, 2023, (India).
14. Freedom of information act, (FOIA) 1967
15. OECD guidelines on data protection, 1980
16. Data protection convention (Treaty 108), 1981
17. European data protection directive
18. Sectoral legislations of US- HIPAA
19. Directive on privacy and electronic communications, 2002

20. EU electronic communications regulations, 2009
21. The General Data Protection Regulation (GDPR),2016
22. CCPA California Consumer Privacy Act), 2018
23. UNCITRAL Model Law on Electronic Commerce (1996)
24. Digital Services Act (DSA) & Digital Markets Act (DMA) (2022) of European Union
25. Federal Trade Commission (FTC) Regulations of US
26. Information Technology (IT) Act, 2000, Consumer Protection Act, 2019 and Digital Personal Data Protection Act. 2023 of India
27. Nigeria Data Protection Regulation, NDPR, 2019 of Nigeria
28. GDPR
29. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework

The National University of Advanced Legal Studies (NUALS)

CERTIFICATE OF PLAGIARISM CHECK

1.	Name of the Research Scholar	**JEMIMA B S**
2.	Title of Thesis /Dissertation	**BALANCING THE GROWTH OF E-COMMERCE WITH DATA SECURITY AND PRIVACY: AN ANALYSIS OF THE INDIAN LEGISLATIVE FRAMEWORK**
3.	Name of the Supervisor	**RAVEENDRAKUMAR D** **HARI S. NAYAR**
4.	Department/ Research Centre	**INTERNATIONAL TRADE LAW**
5.	Similar content (%) Identified	**8**
6.	Acceptable Maximum Limit	**10**
7.	Software Used	**Turnitin - iThenticate**
8.	Date of Verification	**26-05-2025**

** Report on plagiarism check, items with % of similarity is attached*

Checked by (with Name, Designation & Signature):

Name & Signature of the Researcher: **JEMIMA B S**

Name & Signature of the Supervisor: **RAVEENDRAKUMAR D**

HARI S. NAYAR