

A Study on Performance of Personal Data by Meta Platform: Privacy Concern and Legal Challenges

K. Sanjana, II B.C.A., LL. B(Hons.), School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Chennai-600113, sanjanaadv26@gmail.com

Dr. M. D. Chinnu, Assistant Professor, Department of Economics, School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Chennai- 600113, chinnusoel@gmail.com

Abstract:

This study examines the performance and use of personal data by Meta Platforms and the resulting privacy concerns and legal challenges. Meta's data-driven business model relies heavily on the collection, processing, and monetization of user information across its platforms. The research analyses how such data practices affect user privacy and informational autonomy. It also evaluates Meta's compliance with major data protection laws such as the GDPR, CCPA, and India's Digital Personal Data Protection Act. Using doctrinal legal analysis and secondary data sources, the study identifies key gaps in regulatory enforcement. The paper highlights issues related to consent, data transparency, and algorithmic profiling. It further explores notable legal disputes and regulatory actions against Meta. The study concludes by suggesting stronger regulatory oversight and enhanced user-centric data governance mechanisms.

Keywords:

Data Misuse, User Awareness, CCPA- California Consumer Privacy Act, GDPR- General Data Protection Regulation, Data Privacy, Personal Data, Data Security, Right to Privacy, Digital Rights, Data Sharing.

1.Introduction

In the contemporary digital ecosystem, personal data has emerged as a critical economic and social asset, often described by scholars as the foundation of the information society. With the expansion of social media platforms such as Meta (formerly Facebook), encompassing Facebook, Instagram and WhatsApp, the collection and processing of vast quantities of personal information have become an integral part of business operations. Personal data includes any information that can identify an individual directly or indirectly, such as name, contact details, online identifiers, location data, and behavioural patterns.¹

The concept of privacy has long been recognized as essential to human dignity and individual autonomy. Alan Westin defines privacy as the claim of individuals to control when, how and to what extent information about them is communicated to others.² Similarly, Daniel J. Solove explains that privacy is closely connected with protection against surveillance, misuse of personal information, and loss of control over one's identity in the digital space.³ With the growing dependence on digital platforms,

¹ Ian J. Lloyd, *Information Technology Law*, 8th edn., Oxford University Press, 2016, p. 12.

² Alan F. Westin, *Privacy and Freedom*, Atheneum, New York, 1967, p. 7.

³ Daniel J. Solove, *Understanding Privacy*, Harvard University Press, 2008, p. 1.

concerns regarding consent, profiling, data breaches and commercial exploitation of user data have significantly increased.

In India, the constitutional importance of privacy was firmly established in Justice K.S. Puttaswamy v. Union of India (2017), where the Supreme Court declared the right to privacy as an intrinsic part of Article 21 of the Constitution.⁴ This judicial recognition has strengthened the legal discourse surrounding data protection. Globally, regulatory frameworks such as the General Data Protection Regulation (GDPR) of the European Union and, domestically, the Digital Personal Data Protection Act, 2023 seek to regulate the functioning of digital platforms like Meta. Therefore, a study on the performance of personal data practices by Meta platforms, along with the privacy concerns and legal challenges involved, becomes crucial in understanding the balance between technological advancement and protection of fundamental rights.

2.Statement of the Problem

The rapid growth of digital platforms such as Meta (Facebook, Instagram, and WhatsApp) has resulted in collecting, processing, and monetization of users' personal data. While these platforms offer significant social and economic benefits, their data practices regarding privacy, informed consent, surveillance, profiling, data breaches, and unauthorized sharing of personal information. The recognition of the right to privacy as a fundamental right in India and the enactment of data protection frameworks such as the Digital Personal Data Protection Act, 2023, practical challenges persist in regulating the activities of multinational digital corporations like Meta. Issues such as lack of transparency, weak enforcement mechanisms, cross-border data transfer, algorithmic decision-making, and corporate accountability effective protection of personal data. The core problem addressed in this study is whether the current practices of Meta platforms adequately protect users' personal data or not.

3.Review of Literature

Alan F. Westin – Privacy and Freedom (1967) states that privacy is the right of individuals to control the collection and use of their personal information. Westin explains that privacy is essential for dignity, autonomy, and democratic participation. His theory of informational self-determination directly applies to social media platforms like Meta, where users often lack control over their data. He highlights consent as a key element of privacy protection. However, in digital platforms, consent is often illusory due to complex policies. His work supports the argument that Meta's data practices should be transparent. The author also warns that excessive data collection leads to surveillance. Alan Westin's work is considered the foundation of modern privacy theory. This work provides philosophical support for data protection laws. It is highly relevant for analysing privacy concerns.⁵

Daniel J. Solove – Understanding Privacy (2008) examines privacy in the context of modern technology and digital surveillance. He argues that privacy harm is not only about secrecy but also about loss of control over personal data. He identifies issues such as data aggregation, profiling, and secondary use of data. These problems are clearly visible in Meta's business model. Solove criticizes traditional legal frameworks for being outdated in addressing digital threats. He stresses that users are often unaware of how their data is exploited. His work explains why informed consent is weak in social media platforms.

⁴Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

⁵ Alan F. Westin, Privacy and Freedom (Atheneum, New York, 1967).

He advocates for stronger legal accountability for corporations. This book is useful in understanding Meta's privacy risks. It strengthens the legal critique of big tech platforms.⁶

Ian J. Lloyd – Information Technology Law (2016) discusses the legal responsibilities of technology companies in protecting user data. He explains how online intermediaries collect large volumes of personal data for commercial purposes. The author highlights conflicts between business interests and privacy protection. He observes that corporations often prioritize profit over user rights. His analysis helps in evaluating Meta's role as a data controller. Lloyd also discusses regulatory challenges faced by governments in controlling multinational corporations. He emphasizes the need for stronger compliance mechanisms. His work is important for understanding platform accountability. It supports the argument that self-regulation by companies is insufficient. The book provides a legal framework to assess Meta's obligations.⁷

B.N. Srikrishna Committee Report (2018) states that privacy is intrinsic to dignity and liberty. The report introduces the concept of data fiduciaries and places responsibility on platforms like Meta. It highlights problems such as misuse of consent and lack of transparency. The committee recommends stronger user rights, including the right to access and erase data. It also discusses the dangers of surveillance capitalism. The report criticizes unchecked data Protection Act. The Justice B.N. Srikrishna Committee Report is a key document in Indian data protection law. This report is highly relevant to Indian users of Meta platforms. It provides an authoritative legal perspective on privacy concerns.⁸

Justice K.S. Puttaswamy v. Union of India (2017) This landmark Supreme Court judgment recognized the right to privacy as a fundamental right. The Court emphasized informational privacy in the digital age. It warned against both State and corporate surveillance. The judgment acknowledged that personal data misuse can seriously affect individual freedom. The Court highlighted that individuals must have control over their personal information. This decision strengthened constitutional protection against data exploitation. It is directly applicable to platforms like Meta that process large-scale data. The judgment also stressed the need for data protection legislation. It serves as a constitutional basis for regulating social media companies. This case is central to any study on privacy and data protection in India.⁹

4. Research Gap of the Study

Although several studies, reports, and legal writings have examined data protection and privacy in the digital age, there remains a significant gap in research specifically focusing on the practical data practices of Meta platforms in the Indian context. Most existing literature discusses privacy and data protection laws in a general manner but does not sufficiently analyse how global social media corporations like Meta collect, process, and utilize user data in everyday practice. Further, there is limited academic work evaluating the effectiveness of the Digital Personal Data Protection Act, 2023 in addressing the real-world challenges posed by Meta's data practices. Many studies focus on foreign legal frameworks such as the GDPR, while comparatively little attention is given to how Indian law can respond to cross-border data flows, algorithmic profiling, and corporate accountability of Big Tech companies. This study

⁶ Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).

⁷ Ian J. Lloyd, *Information Technology Law* (Oxford University Press, 6th edn., 2016).

⁸ Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Report of the Committee of Experts on Data Protection Framework for India, Ministry of Electronics and Information Technology, Government of India, 2018).

⁹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

attempts to bridge that gap by critically examining Meta's data practices through the lens of Indian data protection law and emerging legal standards.

5.Objectives of the Study

- (I) To find out the level of awareness among users about personal data privacy on digital platforms.
- (II) To analyse the impact of Meta platforms (Facebook, Instagram, WhatsApp) on the performance and use of personal data.
- (III) To examine the legal challenges related to data protection and privacy in the digital environment.
- (IV) To evaluate the effectiveness of existing data protection laws in safeguarding users' personal information.
- (V) To understand the concerns and perceptions of users regarding privacy and data security.
- (VI) To suggest suitable measures and policy recommendations to improve personal data protection and privacy practices.

6.Methodology

This research is based on both doctrinal and non-doctrinal research. The source of data collected from different Newspapers, Journals, Magazines, all India Reports and e-resources. This research uses some of the statistical tools such as percentage method and average method. The sample size of the respondents is 107. The duration of the research is three months.

7.Significance of the Study

This study is significant because it highlights the growing importance of personal data protection in the digital era. With the increasing use of Meta platforms such as Facebook, Instagram, and WhatsApp, users are sharing vast amounts of personal information online. The study helps in understanding how personal data is collected, processed, and used by these platforms. It creates awareness among users about privacy risks and data misuse. The study is useful for students and researchers who wish to understand digital privacy issues in depth. It also helps policymakers to recognize gaps in existing data protection laws. The research contributes to legal awareness by explaining users' rights related to data protection. It supports the need for stronger regulations to protect individuals from cyber exploitation. The study also promotes digital literacy and awareness. Overall, it plays a crucial role in strengthening privacy protection in the modern digital society.

8.Hypothesis

Hypothesis No.1: Protecting users' data on Meta Platforms is the responsibility of the Government, Meta Platforms & User themselves.

Hypothesis No.2: Meta Platforms such as Instagram, Facebook, Twitter, WhatsApp are misusing our personal data.

9. Limitation of the Study

This study is primarily based on doctrinal research using secondary sources such as books, journal articles, reports, websites, and newspaper materials. Therefore, the findings depend on the accuracy and availability of existing literature rather than on primary empirical data. No field survey or interviews with users or officials have been conducted, which limits the practical insight into real user experiences. The scope of the study is also limited to the legal aspects of data protection and privacy, with specific focus on Meta platforms and the Indian legal framework. Technical aspects of data processing and algorithmic systems have not been examined in detail. Additionally, as data protection laws and digital technologies are continuously evolving, some developments may occur after the completion of this study.

10. Result and discussion

PART - I Doctrinal Research

Legal frameworks across the world are evolving to address these concerns. India has introduced the Digital Personal Data Protection Act, 2023 to regulate the processing of personal data and to ensure accountability of data fiduciaries.¹⁰ Nevertheless, several scholars argue that enforcement mechanisms remain weak and that users continue to face risks of data misuse.¹¹ In this context, a doctrinal study becomes significant to analyse existing literature, legal provisions, and judicial interpretations relating to personal data protection and privacy challenges posed by Meta platforms.

Personal Data has been defined under the Digital Personal Data Protection Act, 2023 as any data about an individual who is identifiable by or in relation to such data.¹² Legal scholars explain that personal data includes not only basic information such as name and address, but also online identifiers, browsing behaviour, and digital footprints.¹³

Privacy has been described by Alan Westin as the right of individuals to determine when, how, and to what extent information about them is communicated to others.¹⁴ The Supreme Court of India, in Justice K.S. Puttaswamy v. Union of India, recognized privacy as a fundamental right arising from Article 21 of the Constitution.¹⁵

Data Protection refers to the legal and institutional mechanisms that safeguard individuals against the misuse of their personal information. According to Prashant Mali, data protection laws aim to regulate the collection, storage, processing, and sharing of personal data to prevent abuse and ensure accountability.¹⁶

User Privacy as a Legal Right

User privacy has emerged as one of the most significant legal rights in the contemporary digital age. Traditionally, privacy was understood as a personal and moral concept, but with the advancement of technology and digital communication, it has acquired the status of a legally protected right. Alan Westin,

¹⁰ Digital Personal Data Protection Act, 2023 (India)

¹¹ Prashant Mali, *Cyber Law and Information Technology* (Snow White Publications, 2020).

¹² Digital Personal Data Protection Act, 2023 (India), s.2(t).

¹³ Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).

¹⁴ Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967).

¹⁵ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁶ Prashant Mali, *Cyber Law and Information Technology* (Snow White Publications, 2020).

in his seminal work *Privacy and Freedom*, defines privacy as the right of individuals to control when, how, and to what extent information about them is communicated to others.¹⁷ This understanding forms the theoretical foundation of modern privacy law.

In India, the constitutional recognition of privacy as a legal right was firmly established in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where the Supreme Court held that the right to privacy is a fundamental right under Article 21 of the Constitution.¹⁸ The Court observed that informational privacy is an essential aspect of individual liberty in the digital age. This judgment transformed privacy from a moral claim into an enforceable constitutional right.

Internationally, privacy is recognized as a human right under Article 12 of the Universal Declaration of Human Rights and is strongly protected under legal frameworks such as the European Union's General Data Protection Regulation (GDPR).¹⁹ Legal journals have consistently emphasized that without strong privacy protection, individuals become vulnerable to surveillance, manipulation, and exploitation by both states and corporations.²⁰

Digital platforms have intensified debates on user privacy. Newspapers and magazines frequently report concerns about data breaches, surveillance capitalism, and misuse of user information by big technology companies.²¹ Scholars argue that the commodification of personal data threatens democratic values and calls for stronger legal accountability of technology corporations.²²

Legal Standards for Lawful Use of Personal Data

The lawful use of personal data is governed by certain well-established legal standards developed through legislation, judicial interpretation, and scholarly discourse. These standards are intended to ensure that personal data is collected and processed in a manner that respects individual autonomy, dignity, and privacy. One of the most fundamental principles is that personal data must be processed lawfully, fairly, and transparently. The General Data Protection Regulation (GDPR) of the European Union clearly states that personal data should be collected for specified, explicit, and legitimate purposes and should not be further processed in a manner incompatible with those purposes.²³

A key legal standard for lawful data use is informed consent. Alan Westin emphasizes that individuals must have meaningful control over how their personal information is collected and used.²⁴ Consent must be free, specific, informed, and unambiguous. Similarly, the Digital Personal Data Protection Act, 2023 of India requires that personal data can be processed only for a lawful purpose and with the consent of the data principal, except in certain legally recognized situations.²⁵

¹⁷ Alan F. Westin, *Privacy and Freedom* (Atheneum, New York 1967).

¹⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

¹⁹ European Union, General Data Protection Regulation (GDPR), Official Website of the European Commission, <https://commission.europa.eu>.

²⁰ Bert-Jaap Koops et al., 'A Typology of Privacy' (2017) 38(2) *University of Pennsylvania Journal of International Law*.

²¹ *The Hindu*, 'Data Privacy and the Rise of Surveillance Capitalism', Newspaper Article, 12 August 2022.

²² Shoshana Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019).

²³ European Union, General Data Protection Regulation (Regulation (EU) 2016/679), Article 5, Official EU Website.

²⁴ Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967).

²⁵ Digital Personal Data Protection Act, 2023 (India), ss. 4–6.

Meta's Data Collection Practices: A Legal Overview

In India, the Digital Personal Data Protection Act, 2023 governs the lawful collection and processing of personal data.²⁶ According to the Act, any collection of user data by platforms like Meta must be for a lawful purpose, with explicit consent, and in compliance with principles of transparency and proportionality. Courts in India, particularly in *Justice K.S. Puttaswamy v. Union of India*, have reinforced that privacy is a fundamental right under Article 21 of the Constitution, making any excessive or non-consensual data collection potentially unconstitutional.²⁷

Legal commentators have noted that Meta's data collection practices present challenges regarding cross-border data transfer, third-party sharing, and user consent management.²⁸ Newspapers and magazines have frequently reported incidents of data breaches, misuse, and opaque privacy policies, further emphasizing the need for robust legal oversight.²⁹ As such, a doctrinal study of Meta's data practices highlights both the technological mechanisms and the evolving legal standards required to safeguard user privacy.

Misuse of Personal Data: Concept under law

The misuse of personal data refers to the unlawful, unauthorized, or unethical collection, processing, sharing, or exploitation of an individual's personal information in violation of legal standards and privacy rights. Daniel J. Solove explains that data misuse threatens individual autonomy because it allows organizations to manipulate, control, or exploit individuals based on their personal information.³⁰ From a legal perspective, the concept of misuse is closely linked with the principles of consent, purpose limitation, and fair processing. Where these principles are violated, the use of personal data becomes legally questionable. Alan Westin also emphasized that privacy is compromised when individuals lose control over how their data is disseminated and used.³¹

Indian law recognizes misuse of personal data as a serious legal concern. The Digital Personal Data Protection Act, 2023 provides that personal data must be processed only for lawful purposes and in accordance with the consent of the data principal.³² Any unauthorized processing or disclosure can attract penalties and liability. Furthermore, in *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court held that informational privacy is an essential part of the fundamental right to life and personal liberty, and that arbitrary misuse of personal data violates constitutional guarantees.³³

International legal frameworks also condemn misuse of personal data. The General Data Protection Regulation (GDPR) treats unlawful processing, excessive data collection, and unauthorized sharing as violations of data protection principles.³⁴ Legal journals note that misuse is increasingly facilitated by big technology companies through opaque algorithms and surveillance-based business models.³⁵

²⁶Digital Personal Data Protection Act, 2023 (India), ss. 4–6.

²⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

²⁸ Graham Greenleaf, 'Global Data Privacy Laws 2021' (2021) 169 *Privacy Laws & Business International Report*.

²⁹ The Hindu, 'Data Privacy and the Rise of Surveillance Capitalism', Newspaper Article, 12 August 2022.

³⁰ Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).

³¹ Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967).

³² Digital Personal Data Protection Act, 2023 (India), ss. 4–8.

³³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

³⁴ European Union, General Data Protection Regulation (Regulation (EU) 2016/679), Article 5.

³⁵ Bert-Jaap Koops et al., 'A Typology of Privacy' (2017) 38(2) *University of Pennsylvania Journal of International Law*.

Newspapers and magazines frequently report incidents such as data breaches, unauthorized third-party sharing, and political profiling, highlighting how misuse of data has become a global legal challenge.³⁶

Surveillance, Profiling and Violation of Privacy Rights

In the digital age, surveillance and profiling have become significant threats to the right to privacy. Surveillance refers to the continuous monitoring of individuals' activities, communications, and behaviour through technological means, while profiling involves the automated processing of personal data to evaluate, analyse, or predict an individual's preferences, behaviour, or characteristics. Legal scholars argue that such practices undermine personal autonomy and human dignity when conducted without informed consent.³⁷

From a legal perspective, unchecked surveillance and profiling amount to a serious violation of privacy rights. The Supreme Court of India in *Justice K.S. Puttaswamy v. Union of India* (2017) clearly held that privacy includes the right to control the dissemination of personal information and protects individuals against intrusive state or corporate surveillance.³⁸ The Court emphasized that any restriction on privacy must satisfy the tests of legality, necessity, and proportionality. International legal instruments also condemn excessive surveillance. The General Data Protection Regulation (GDPR) restricts automated decision-making and profiling without explicit consent and grants individuals the right not to be subjected to decisions based solely on automated processing.³⁹ Academic journals have argued that profiling threatens democratic freedoms by enabling behavioural manipulation and eroding freedom of thought.⁴⁰

Meta's Compliance with Data Protection Laws

Under the European Union's General Data Protection Regulation (GDPR), Meta is obligated to obtain valid consent from users, clearly disclose how data is processed, and ensure that users can exercise rights such as access, correction, and deletion of their personal data.⁴¹

In the Indian context, Meta's operations are now governed by the Digital Personal Data Protection Act, 2023. The Act requires data fiduciaries such as Meta to process personal data only for lawful purposes, provide clear privacy notices, implement reasonable security safeguards, and establish grievance redressal mechanisms.⁴² Any failure to comply with these obligations can attract substantial financial penalties. This reflects the growing expectation that technology companies must be legally accountable for their data practices. Courts have also played an important role in shaping compliance standards. In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court emphasized that informational privacy is a fundamental right and that both State and non-State actors must respect this right while dealing with personal data.⁴³ This constitutional principle indirectly imposes higher compliance obligations on private corporations like Meta.

³⁶ The Indian Express, 'Data Breaches and the Growing Threat to Privacy', Newspaper Article, 18 October 2023.

³⁷ Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).

³⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

³⁹ European Union, General Data Protection Regulation (Regulation (EU) 2016/679), Article 22.

⁴⁰ Luciano Floridi, 'On the Intrinsic Value of Information Objects and the Infosphere' (2014) *Ethics and Information Technology Journal*.

⁴¹ European Union, General Data Protection Regulation (Regulation (EU) 2016/679), Articles 5–15, Official EU Website.

⁴² Digital Personal Data Protection Act, 2023 (India), ss. 4–10.

⁴³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Newspapers and technology law commentaries have frequently reported that despite Meta's public claims of compliance, the company continues to face investigations and fines for data protection violations across different jurisdictions.⁴⁴ Magazines and academic journals further observe that compliance is often treated by large technology companies as a formal requirement rather than as a genuine commitment to user rights.⁴⁵

GDPR Violations and Legal Actions against Meta

The enforcement of the General Data Protection Regulation (GDPR) has resulted in several significant legal actions against Meta Platforms Inc. for alleged violations of data protection principles. GDPR imposes strict obligations on data controllers, including lawfulness of processing, transparency, purpose limitation, data minimization, and protection of users' rights.⁴⁶ Meta, as a global technology company handling large volumes of personal data, has frequently been scrutinized by European data protection authorities for non-compliance with these standards.

One of the most notable legal actions involved the issue of forced consent. Regulatory authorities held that Meta could not rely on "contractual necessity" to justify extensive data collection for targeted advertising purposes.⁴⁷ Scholars argue that this practice undermines the GDPR requirement of freely given consent and weakens user autonomy.⁴⁸ This interpretation reinforced the principle that commercial convenience cannot override fundamental privacy rights. Meta has also faced legal consequences for unlawful cross-border data transfers. European regulators have repeatedly questioned the transfer of European users' data to the United States due to concerns about surveillance laws and inadequate protections.⁴⁹ In response, data protection authorities imposed substantial fines and ordered restrictions on certain data transfer practices. These actions demonstrate the seriousness with which GDPR treats international data protection compliance.

Digital Personal Data Protection Act, 2023 and Meta

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant development in India's legal framework for regulating the processing of personal data. For global technology corporations such as Meta Platforms Inc., which operates Facebook, Instagram, and WhatsApp in India, the DPDP Act creates new statutory obligations and heightened legal accountability.⁵⁰ Under the DPDP Act, Meta qualifies as a "Data Fiduciary", meaning it determines the purpose and means of processing personal data of Indian users.⁵¹ As a data fiduciary, Meta is legally bound to process personal data only for a lawful purpose and based on free, informed, specific, and unambiguous consent of the data principal.⁵²

The DPDP Act also grants enforceable rights to users, including the right to access information, the right to correction and erasure of personal data, and the right to grievance redressal.⁵³ These rights

⁴⁴ The Indian Express, 'Meta Faces Scrutiny Over Data Protection Compliance', Newspaper Report, 10 October 2023.

⁴⁵ Time Magazine, 'Why Big Tech's Privacy Promises Often Fall Short', Magazine Article, 2022.

⁴⁶ European Union, General Data Protection Regulation (Regulation (EU) 2016/679), Article 5.

⁴⁷ Court of Justice of the European Union, *Bundeskartellamt v Meta Platforms Inc.* (2023).

⁴⁸ Orla Lynskey, 'Deconstructing Data Protection: The Role of Consent under the GDPR' (2018) 40(2) *Oxford Journal of Legal Studies*.

⁴⁹ European Data Protection Board, 'Statement on Cross-Border Data Transfers and Meta', Official Website, 2022.

⁵⁰ Apar Gupta, *Digital India and the Law* (Oxford University Press, 2022).

⁵¹ Digital Personal Data Protection Act, 2023 (India), s. 2(i).

⁵² DPDP Act, 2023, ss. 4–6.

⁵³ DPDP Act, 2023, Chapter III (Rights and Duties of Data Principal).

empower Indian users of Meta platforms to exercise greater control over their personal information. Newspapers and legal commentaries have observed that this law could fundamentally alter the relationship between Indian users and global social media platforms by shifting power toward individuals.⁵⁴

Remedies Available to Victims of Data Misuse

One of the primary remedies available to victims is the right to complain to a regulatory authority. Under the Digital Personal Data Protection Act, 2023 (India), an aggrieved data principal may file a complaint with the Data Protection Board of India if a data fiduciary violates statutory obligations.⁵⁵ The Board has the power to inquire into complaints and impose significant monetary penalties on defaulting entities. This provides victims with an institutional mechanism for redress.

Victims of data misuse also have access to civil remedies, particularly the right to seek compensation for harm suffered. Legal scholars argue that monetary compensation is essential to recognize the real damage caused by privacy violations.⁵⁶ Internationally, strong remedial frameworks exist under laws such as the General Data Protection Regulation (GDPR). Article 82 of the GDPR expressly grants individuals the right to receive compensation for material and non-material damage resulting from data protection violations.⁵⁷ This provision reflects the growing global recognition that emotional distress and loss of dignity caused by data misuse are legally cognizable harms.

Case laws

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

This landmark case arose from a challenge to the Aadhaar scheme, where the petitioner argued that compulsory collection of biometric and personal data violated individual liberty. The main issue before the Supreme Court was whether the right to privacy is a fundamental right under the Indian Constitution. A nine-judge constitutional bench unanimously held that the right to privacy is an intrinsic part of Article 21 and flows from other fundamental rights such as Articles 14 and 19. The Court emphasized that privacy includes informational privacy, bodily autonomy, and decisional freedom. It recognized that in the digital age, protection of personal data is essential to preserve dignity and liberty. The judgment laid down the constitutional foundation for data protection laws in India. This case is now the backbone of all privacy and data protection jurisprudence. It directly supports legal challenges against misuse of personal data by the State and private corporations.⁵⁸

Govind v. State of Madhya Pradesh (1975) 2 SCC 148

In this case, the validity of police surveillance regulations was again challenged on the ground that they violated the right to privacy. The Supreme Court examined whether privacy could be considered a constitutional right. The Court held that although the right to privacy is not explicitly mentioned in the

⁵⁴ The Hindu, 'What the Digital Personal Data Protection Act Means for Social Media Users', Newspaper Article, 12 August 2023.

⁵⁵ Digital Personal Data Protection Act, 2023 (India), ss. 27–32 (Data Protection Board and grievance redressal).

⁵⁶ Daniel J. Solove & Danielle Keats Citron, 'Risk and Anxiety: A Theory of Data-Breach Harms' (2018) 96 Texas Law Review.

⁵⁷ European Union, General Data Protection Regulation (Regulation (EU) 2016/679), Article 82.

⁵⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 Supreme Court Cases 1 (Supreme Court of India).

Constitution, it is implicit in Article 21. The Court accepted that privacy is a protected right but clarified that it is not absolute and can be restricted in the interest of public order and security. The judgment balanced individual liberty with State interests. It marked an important development by explicitly recognizing privacy as part of fundamental rights. The Court's reasoning later influenced the Puttaswamy judgment. This case strengthened the legal protection against arbitrary surveillance.⁵⁹

People's Union for Civil Liberties (PUCL) v. Union of India (1997) 1 SCC 301

This case was filed against the practice of telephone tapping by government authorities. The issue before the Supreme Court was whether interception of telephone conversations violated the right to privacy. The Court held that telephone conversations are an important part of private life and are protected under Article 21. It ruled that phone tapping can only be done according to a fair, just, and reasonable procedure established by law. The Court laid down detailed safeguards to prevent arbitrary interception of communications. This judgment strengthened procedural protections for privacy in the context of technology. It recognized that technological surveillance poses serious threats to liberty. The case remains highly relevant in the digital communication era. It also supports arguments against unlawful digital surveillance and data interception.⁶⁰

Facebook Inc. v. Union of India (2020) SCC Online SC 932

This case arose from the Cambridge Analytica data scandal, where Facebook (Meta) was summoned by a Parliamentary Committee regarding misuse of user data. Facebook challenged the summons, arguing that it could not be compelled to disclose certain information. The Supreme Court rejected Facebook's attempt to avoid scrutiny and emphasized that social media platforms cannot escape accountability when public interest and user rights are involved. The Court observed that platforms like Facebook influence democracy, free speech, and privacy of millions of users. It recognized the serious implications of data misuse by Big Tech companies. The judgment highlighted the responsibility of digital platforms toward users. This case is important because it directly connects privacy rights with corporate accountability. It supports the argument that Meta must comply with Indian legal standards on data protection.⁶¹

Shreya Singhal v. Union of India (2015) 5 SCC 1

This case challenged the constitutional validity of Section 66A of the Information Technology Act, 2000, which criminalized certain online speech. The issue before the Supreme Court was whether this provision violated the right to freedom of speech and expression. The Court struck down Section 66A as unconstitutional for being vague and having a chilling effect on free speech. While the case focused on speech, the Court also made important observations about the internet, user rights, and the need to protect individuals from arbitrary state action online. The judgment emphasized that citizens' rights do not disappear in the digital space. It indirectly strengthened protection for digital autonomy and individual liberty. The case is often cited in discussions on digital rights and online freedoms. It highlights the judiciary's role in protecting individuals from excessive control over online platforms. This judgment remains crucial for understanding constitutional protections in cyberspace.⁶²

⁵⁹ Govind v. State of Madhya Pradesh, (1975) 2 Supreme Court Cases 148 (Supreme Court of India).

⁶⁰ People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 Supreme Court Cases 301 (Supreme Court of India).

⁶¹ Facebook Inc. v. Union of India, (2020) 7 Supreme Court Cases 162 (Supreme Court of India).

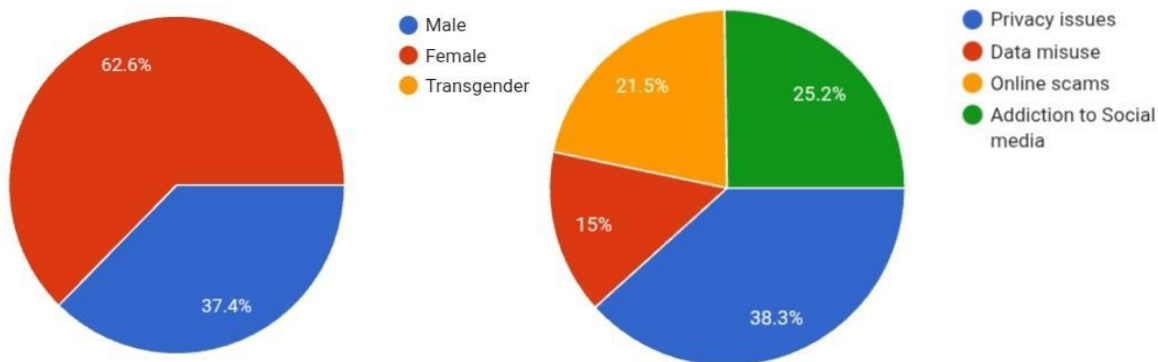
⁶² Shreya Singhal v. Union of India, (2015) 5 Supreme Court Cases 1 (Supreme Court of India).

Part- II Non-Doctrinal Research

Table No. 1 Gender of the Respondents and issues faced while using Meta Platforms

Particulars	Online Scams	Privacy Issues	Data Misuse	Addiction to social media	Total
Male	7 (6.54)	16 (14.95)	8 (7.48)	9 (8.41)	40 (37.4)
Female	16 (14.95)	25 (23.36)	8 (7.48)	18 (16.82)	48 (44.82)
Transgender	0 (0.00)	0 (0.00)	0 (0.00)	0 (0.00)	0 (0.00)
Total	23 (21.50)	41 (38.32)	16 (14.95)	27 (25.23)	107 (100.00)

Source: Primary data



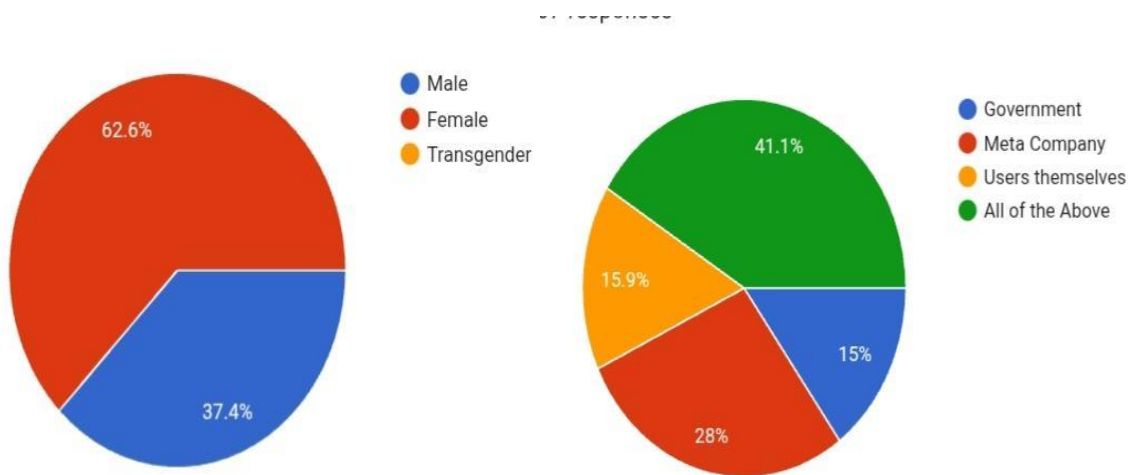
The above table depicts the gender-wise distribution of issues faced by respondents while using Meta platforms. Among the total 107 respondents, privacy issues were the most reported concern, affecting 41 respondents 38.32 percentage, followed by addiction to social media reported by 27 respondents 25.23 percentage. Online scams were experienced by 23 respondents 21.50 percentage, while data misuse was reported by 16 respondents 14.95percentage.

Among female respondents, privacy issues 25 respondents, 23.36 percentage and addiction to social media 16.82 percentage were the most significant concerns. Among male respondents, privacy issues 14.95 percentage were also the dominant issue, followed by addiction to social media 8.41 percentage. No transgender respondents were recorded in the study. Overall, the data indicates that privacy-related concerns are the most prominent issue across both genders.

Table No.2 Gender of the Respondents and responsibility of protecting users Personal Data on Meta Platform

Particulars	Meta Company	Government	Users Themselves	All of the Above	Total
Male	11 (10.28)	10 (9.35)	7 (6.54)	12 (11.21)	40 (37.4)
Female	19 (17.75)	6 (5.61)	10 (9.35)	32 (29.91)	67 (62.6)
Transgender	0 (0.00)	0 (0.00)	0 (0.00)	0 (0.00)	0 (0.00)
Total	30 (28.03)	16 (14.96)	17 (15.89)	44 (41.12)	107 (100.00)

Source: Primary data

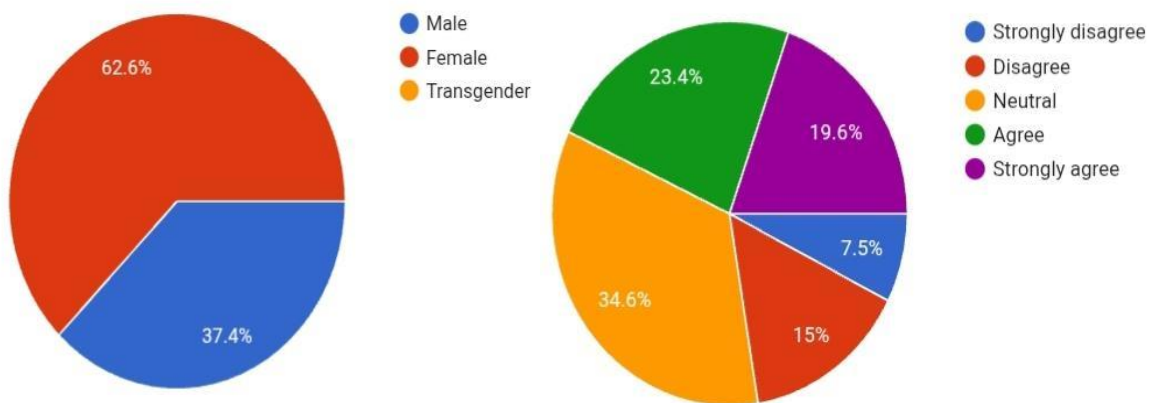


The above table shows the gender-wise opinion of respondents regarding responsibility for the protection of personal data on Meta platforms. Out of 107 respondents, the majority 44 respondents 41.12 percentage believed that all stakeholders, including the Meta company, government, and users themselves, are jointly responsible for protecting personal data. This view was more strongly supported by female respondents 29.91percentage compared to male respondents 11.21percentage. Further, 30 respondents 28.03 percentage felt that the Meta company alone bears responsibility for data protection, followed by 17 respondents 15.89percentage who believed that users themselves are responsible. Government responsibility was identified by 16 respondents 14.96percentage. No transgender respondents were recorded in the study. Overall, the findings indicate a strong perception that data protection is a shared responsibility among all stakeholders.

Table No.3 Gender of the Respondents and Opinion on the Statement Related to Data Privacy on Meta Platforms

Particulars	Strongly Disagree	Strongly Agree	Neutral	Agree	Disagree	Total
Male	5 (4.67)	4 (3.74)	15 (14.02)	6 (5.61)	10 (9.35)	40 (37.4)
Female	3 (2.80)	17 (15.89)	22 (20.56)	19 (17.75)	6 (5.61)	67 (62.6)
Transgender	0 (0.00)	0 (0.00)	0 (0.00)	0 (0.00)	0 (0.00)	0 (0.00)
Total	8 (7.47)	21 (19.63)	37 (34.58)	25 (23.36)	16 (14.96)	107 (100.00)

Source: Primary data



The above table presents the gender-wise opinion of respondents regarding the statement related to data privacy on Meta platforms. Out of 107 respondents, the highest number 37 respondents 34.58percentage expressed a neutral opinion, indicating uncertainty or lack of clear awareness regarding the issue. This was followed by agreement, expressed by 25 respondents 23.36 percentage, and strong agreement by 21 respondents 19.63 percentage. Among female respondents, a considerable proportion either strongly agreed 15.89 percentage or agreed 17.75percentage with the statement, reflecting a higher level of concern or awareness. Among male respondents, neutrality 14.02percentage and disagreement 9.35percentage were more prominent. Overall, the findings suggest a mixed level of awareness and perception, with a significant number of respondents remaining neutral on data privacy issues related to Meta platforms.

Testing of Hypothesis

Hypothesis H1:

Based on the analysis of table no.2, a majority of respondents 41.12 percentage opined that all stake holders Government, Meta Platforms, and user themselves are jointly responsible for protecting personal data. Hence, the null hypothesis (H_0) is accepted, and the alternative hypothesis (H_1) is rejected.

Hypothesis H2:

Based on the table no.3, a considerable proportion of respondents either agree or strongly agree with statements expressing concern over personal data misuse by Meta Platforms. This indicates a prevailing apprehension regarding data misuse. Hence, the alternative hypothesis (H₁₂) is accepted, and the null hypothesis (H₀₂) is rejected.

Conclusion

This study shows that the way Meta collects and uses personal data raises serious privacy concerns for users. Many people are not fully aware of how their data is tracked, stored, and used for profiling and targeted advertisements. This creates an imbalance between powerful digital platforms and ordinary users. Privacy is an important part of personal freedom and dignity, and its misuse can cause real harm to individuals. The law has started responding to these challenges. However, effective protection depends on proper enforcement of the law, responsible behaviour by companies like Meta, and greater awareness among users about their rights. Strong implementation of legal safeguards is essential to protect personal data in the digital age.

Suggestion

- 1.The government should strictly enforce data protection laws to stop misuse of personal data on Meta platforms.
- 2.Meta companies should clearly explain how they collect, use, and share users' personal data.
- 3.Users should be educated about privacy settings and safe use of social media through awareness programmes.
- 4.Meta platforms should provide easy complaint systems to report online scams and privacy problems.
- 5.The government should regularly check whether Meta platforms are following data protection rules.
- 6.Schools and colleges should teach students about safe and responsible use of social media.
- 7.Users should protect their own data by using strong passwords and not sharing personal information online.

Reference

1. Ian J. Lloyd, Information Technology Law, 8th edn., Oxford University Press, 2016.
- 2.Alan F. Westin, Privacy and Freedom, Atheneum, New York, 1967.
- 3.Daniel J. Solove, Understanding Privacy, Harvard University Press, 2008.
- 4.Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- 5.Shoshana Zuboff, The Age of Surveillance Capitalism (Public Affairs, 2019).
- 6.Don Tapscott, The Digital Economy (McGraw Hill, 1996).
- 7.Digital Personal Data Protection Act, 2023 (India).
- 8.Prashant Mali, Cyber Law and Information Technology (Snow White Publications, 2020).
- 9.Mark Andrejevic, 'Exploitation in the Data Mine' (2009) 4(2) Internet Studies Journal.
10. European Union, General Data Protection Regulation (GDPR), Official Website of the European Commission, <https://commission.europa.eu>.
11. Bert-Jaap Koops et al., 'A Typology of Privacy' (2017) 38(2) University of Pennsylvania Journal of International Law.

12. The Hindu, 'Data Privacy and the Rise of Surveillance Capitalism', Newspaper Article, 12 August 2022.
13. Graham Greenleaf, 'Global Data Privacy Laws 2021' (2021) 169 Privacy Laws & Business International Report.
14. The Indian Express, 'Data Breaches and the Growing Threat to Privacy', Newspaper Article, 18 October 2023.
15. Roger Clarke, 'Information Technology and Dataveillance' (1988) 31(5) Communications of the ACM.
16. Luciano Floridi, 'On the Intrinsic Value of Information Objects and the Infosphere' (2014) Ethics and Information Technology Journal.
17. The Guardian, 'How Big Tech Tracks and Profiles Users for Profit', Newspaper Report, 15 June 2021.
18. Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42(4) European Law Review.
19. The Indian Express, 'Meta Faces Scrutiny Over Data Protection Compliance', Newspaper Report, 10 October 2023.
20. Time Magazine, 'Why Big Tech's Privacy Promises Often Fall Short', Magazine Article, 2022.
21. Court of Justice of the European Union, *Bundeskartellamt v Meta Platforms Inc.* (2023).
22. Paul De Hert & Serge Gutwirth, 'Privacy, Data Protection and the Law' (2013) Computer Law & Security Review.
23. Apar Gupta, *Digital India and the Law* (Oxford University Press, 2022).
24. The Hindu, 'What the Digital Personal Data Protection Act Means for Social Media Users', Newspaper Article, 12 August 2023.
25. The Hindu, 'Data Breaches and the Struggle for Effective Remedies in India', Newspaper Article, 20 September 2023.