INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 9 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 9 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-10-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CRITICAL ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT IN RELATION TO SOCIAL MEDIA DATA AGGREGATION

AUTHOR -ROHITA BOSE* & ASST.PROF RAMAKANT TRIPATHI**

* STUDENT AT LAW COLLEGE DEHRADUN / UTTARANCHAL UNIVERSITY

** ASSISTANT PROFESSOR AT LAW COLLEGE DEHRADUN / UTTARANCHAL UNIVERSITY

BEST CITATION - ROHITA BOSE & ASST.PROF RAMAKANT TRIPATHI, CRITICAL ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT IN RELATION TO SOCIAL MEDIA DATA AGGREGATION, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (10) OF 2025, PG. 142-149, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

An unprecedented digital data boom and unrelenting technical innovation have made protecting personal data a top priority for people, businesses, and governments around the world. There has been discussion on how social media affects people's right to privacy. Due to global digitisation, especially in India, the significance of data protection has increased to previously unthinkable heights in recent decades.Since the dawn of human civilisation, the concept of "privacy" has existed. However, privacy could be difficult to comprehend.Scholars cannot agree on a single definition of "privacy" because the concept changes with society. The concept of the right to privacy has evolved over time to encompass rights that have arisen throughout human history, such as the right to anonymity or the right to privacy. This freedom must be safeguarded because digital media is so prevalent in today's society. The Digital Personal Data Protection Act, 2023, is significant because it empowers people and protects their rights by establishing guidelines for the appropriate handling of personal data. The main objective of the DPDP Act is to increase the standard of accountability and responsibility for companies that are subject to Indian law, such as internet service providers, mobile applications, and companies that gather, store, and alter personal data. By emphasising the preservation of the "Right to Privacy," this law seeks to guarantee that these organisations function transparently and are held responsible for how they use personal information, thus placing a high premium on individual rights to privacy and data security.Thus, examining the Digital Data Protection Act of 2023 from a privacy perspective is pertinent.

KEYWORDS- Data protection, privacy, social media, digital data

I. INTRODUCTION

The landmark Digital Personal Data Protection Act (DPDPA), 2023, passed by the Indian Parliament in August 2023, aims to balance the interests of governments and the rights of individuals and businesses by regulating the gathering, processing, and storage of digital personal data. This law reflects India's substantial efforts to protect people's rights over their personal information in the modern digital age, where personal data is regularly and openly exchanged. It adapts to India's particular circumstances while adhering to international data protection norms such as the General Data Protection Regulation (GDPR) of the European Union.[7]

The constant flow of digital information and the quickly evolving technical landscape have made protecting personal data a top priority for people, businesses, and governments everywhere. In addition to changing how we work, communicate, and live our lives, the quick

[7] Dhiraj R. Duraiswami, Privacy and Data Protection in India, 6 J.L. & CYBER WARFARE 166, 169-172(2017)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

growth of social media, e-commerce, and digital transactions has brought attention to the urgent need for strict privacy and data security regulations. An important turning point in data protection and privacy was reached in India with the passage of the Digital PersonalData Protection Act, 2023 (DPDP Act). The goal of this historic law is to create a new paradigm that properly balances the advantages of technological innovation with the need to protect people's right to privacy.[8]

The right to privacy is recognised as a fundamental human right by the 1948 Universal Declaration of Human Rights (UDHR), the 1976 International Covenant on Civil and Political Rights (ICCPR), the 2003 United Nations Convention on the Protection of the Child, the United Nations Convention on Migrant Workers, and other international agreements. Privacy has become a critical problem in the era of enormous data, and researchers and analysts are tackling privacy challenges to maintain security. People's views of privacy have changed as a result of the internet and effective data storage methods, raising worries about how third parties may collect, store, access, and safeguard information.[9]

Large databases are usually owned by enterprises and governments, including the Indian government, IT companies, and private organisations. These databases are used in social services, digital projects, and marketing. Public-private collaborations create concerns about data ownership and access control protocols, even though most big data projects incorporate privacy guidelines.

II. DATA PROTECTION AND THE RIGHT TO PRIVACY

The relationship between data protection regulations and the right to privacy is obvious. Even while these two abstract ideas are most likely logically separate, the rights to privacy and data protection are practically connected.[10] Recognising the right to privacy as a fundamental right is the foundation for the claim that data protection regulations have greatly improved. For the purposes of the Data Protection law, however, the right to privacy must be precisely and unambiguously stated. The term "right to privacy" is ambiguous because politicians in many countries differ over what exactly it means.[11]

- **Constitutional basis**

The Digital Personal Data Protection Act, 2023 was passed as a result of the Supreme Court's ruling in **Justice K.S. Puttaswamy vs. Union of India**[12] upholding the "Right to Privacy" as a necessary component of the fundamental right to "Right to Life," which is protected by Article 21 of the Indian Constitution. The Court also recommended that the Central Government enact legislation to safeguard personal information.

Many international human rights frameworks recognise the right to privacy as a fundamental human right. The primary interpretation of this right in relation to data protection is the ability of individuals to control the gathering, use, storage, and dissemination of their personal data. Privacy as a concept is not new. Ancient Greece was divided into two realms: Polis, or the public or political sphere, and Oikos, or the private or familial domain. But the idea of the "right" to privacy is rather recent. Even if the right to privacy can encompass both physical privacy and privacy related to information, the rise of newspapers, television, and the internet has caused the idea of privacy to shift to focus more on data privacy. The intrusive interference in private talks is one way that the assault on privacy manifests itself, as demonstrated by the Edward Snowden exposé and the present Pegasus episode. However, it's important to

[8] NANDAN KAMATH, *Law Relating To Computers, Internet, And E-Commerce: A Guide To Cyber LawsAnd The Information Technology Act*, 2000 121 (Kamal Law House, Calcutta,1st Ed. 2020).

[9] Jason Asbury, Maria McClelland, Kris Torgerson, India Vincent & Jennifer Boling, Law and BusinessTechnology: Cyber Security & Data Privacy Update, 20 *Transactions: TENN. J. BUS.* L. 1065, 1067-71(2019).

[10] Systems Thinking, Big Data, and Data Protection Law, 18 Eur. J.L. Reform 478 (2016)

[11] Orla Lynskey, "Deconstructing Data Protection: The Added-Value of a Right to Data Protection inthe EU Legal Order", 63 *INTL & COMP. L.Q.* 569, 577-81 (2014).

[12] AIR 2018 SC (SUPP) 1841

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 9 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

keep in mind that the right to privacy extends much beyond the ability to speak in confidence.

- **Essense of privacy and data protection**

A key idea in the protection of personal data is the right to privacy, which gives people, businesses, or organisations the freedom to choose how, when, and to what degree their information is disclosed. This right affects people profoundly and is essential to any democratic government. However, data security is necessary to safeguard people's privacy. The policies, practices, and legally binding laws that safeguard and guarantee control over personal data are referred to as data protection. It means being in charge of deciding whether to reveal certain information, as well as who must know it, for how long, and why. Generally speaking, "processing" is obtaining, preserving, using, and sharing information. The purpose of data protection laws is to safeguard the information of individuals and businesses alike.[13]

- **Data protection regulations in india**

India's data privacy regulations give informational sovereignty and self-determination a lot of weight in order to guarantee equity in the handling of personal data. Digitalisation has enhanced these regulations, which place a high focus on people's right to privacy. By safeguarding the distribution, collection, use, erasure, storage, and destruction of personal data, data protection laws provide a fair degree of equity in line with accepted standards.

New concepts for data protection are introduced in India by the Digital Personal Data Protection Act, 2023[14], such as the right to privacy, purpose limitation, equitable processing, and erasure. By establishing guidelines for data principals and data fiduciaries, this legal framework offers assurance about the safety of personal information.

III. DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL ANALYSIS

In India, the DPDP Act regulates how digital personal data is handled in two situations: when it is downloaded digitally from data principals and when it is first collected in a non-digital manner before being converted to digital form. The Act may be applied extraterritorially to processes of goods or services that are rendered to data principals in India outside of India's borders. Whether its rules extend to data processing from data principals located outside of India is not mentioned, though. The Act creates the phrase "Personal Data" and requires data fiduciaries to protect personal data and report breaches to the Board and affected data principals. According to the Act, processing personal data includes gathering, documenting, organising, storing, changing, retrieving, using, aligning, combining, indexing, sharing, and disclosing.[15]

- **Definition and consent**

The DPDP(Digital Personal Data Protection) Act expands the definition of a "data principal" to include parents, minors' legal guardians, and individuals with disabilities. A data fiduciary is somebody who decides on the purposes and methods for handling personal data. Consent must be freely given, explicit, informed, unconditional, and unambiguous, and only valid uses of data are allowed. Consent must be explicit and meet specific criteria. The request must be clear, easy to understand, and available in English or any of the 22 languages listed in the Eighth Schedule to the Indian Constitution. It must also provide the contact information for the data protection officer or approved representative.[16]

- **Safeguards**

To protect consumer data and prevent breaches, businesses need to have security policies, procedures, and measures. The new rules outline certain particular security measures that must be followed. Security

[13] Silvia Lucia Cristea & Viorel Banulescu, *The Right to Personal Data Protection. The Right to Privacy.A Comparative Law Approach,* 64 Analele Stiintifice Ale Universitatii Alexandru Ioan Cuza Din IasiStiinte Juridice 1, 3-5 (2018).
[14] The Digital Personal Data Protection Act, 2023, No.22, Acts of Parliament, 2023(India).
[15] The Digital Personal Data Protection Act, 2023, Act 22 of 2000), s. 2(j).
[16]The Digital Personal Data Protection Act, 2023, Act 22 of 2000), s. 4.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 9 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

provisions must also be included in contracts between data processors and data fiduciaries (data controllers under the DPDP Act).

- **Required Data Fiduciary Notice**

A comprehensive notice outlining the data principal's rights, the rationale for the collecting and processing of personal data, and the steps for filing a complaint with the Board must be provided by the data fiduciary. If consent was granted before the DPDP Act, the notice should be issued as soon as possible in plain English, as a separate document, electronically, or in compliance with requirements.[17]

In the event of a data breach, the data fiduciary is required to notify the affected data principals as well as the Data Protection Board, India's enforcement agency. Unless an extension is granted by the authority, information on the breach must be submitted within 72 hours of its discovery.

- **Removal of data**

Personal data must be deleted when the data principle withdraws their consent or the collection's legitimate purpose is achieved. In any event, the data fiduciary must give the data principal 48 hours' notice before deleting the data.

- **Specific officers**

Companies have established standards for the hiring of a data protection officer, one of which is that the officer's headquarters be in India. Businesses without a data protection officer must at least designate a specialist to handle data owners' concerns about their personal information. Information about the designated individuals must be posted on the websites of all businesses.

- **People With Disabilities**

Before processing a person with a disability's personal data, businesses must obtain the verifiable consent of the individual's parent or legal guardian.

- **Cross border**

The transfer of personal data for processing outside of India may be subject to additional regulations and restrictions from the Indian government. The Act regulates the transfer of private data outside of India. If a data fiduciary processes personal data in India or abroad while offering goods or services to Indian citizens, they are subject to several rules. The central government has the authority to give particular or general directives that the fiduciary must follow. These rules, which govern the exchange of personal data with foreign countries, organisations, or their agencies, protect the privacy of Indian citizens.

- **The DPDP Act's Penalties and Liabilities**

Penalties of up to INR 250 crore may be imposed for certain infractions under the DPDP Act, such as neglecting to prevent breaches of personal data. Crucially, the INR 500 crore cap on single-instance fines has been removed. This rule, in contrast to previous iterations, prohibits data principals impacted by breaches from pursuing damages from data fiduciaries. Rather, the Board has the authority to fine data principals who don't fulfil their responsibilities up to INR 10,000.

IV. DIGITAL PERSONAL DATA PROTECTION ACT IN RELATION TO SOCIAL MEDIA DATA AGGREGATION

- **Right Given To Social Media Users**

Data Principals are granted many rights under the DPDPA that allow individuals to have greater control over their personal data. Following are rights given as stated below –

- **To Get Information**

People have a right to know what personal data is being collected, why, and how it will be put to use. Because of this transparency, people may make informed decisions about sharing data.

- **Erasure and Correction**

Data Principals can seek the correction of inaccurate or misleading data. They also have the right to request the deletion of any data that is no longer needed for the original purpose.

- **Portability of Data**

[17] AZBPARTNERS, https://www.azbpartners.com/bank/digital-personal-data-protection-bill-2023-key-highlights last visited (Jan 25, 2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Although the DPDPA does not expressly address the right to data portability—a right observed in other nations such as the GDPR—it does provide users with some flexibility in how they handle their data between platforms.

- **Can object to processing**

People may object to the processing of their data in some situations, especially if it is being used for reasons different than those for which it was originally collected.

- **Redress of Grievances (Data Protection Board)**

Data principals can file a complaint with the Data Protection Board of India (DPBI) if they believe their rights have been violated or their data has been handled incorrectly. To ensure proper implementation of the DPDP Act, the government will establish a Data Protection Board (DPB). The board will play a key role in balancing the rights of individuals (data principals) with the responsibilities of companies (data fiduciaries). The DPB will perform the majority of its business online in order to promote efficiency and accessibility. It will handle accusations of data breaches, ensure that companies follow data protection laws, and monitor companies to ensure compliance.[18]

If a corporation doesn't comply, the board has the authority to stop operations, provide orders, or cancel its registration.Anyone can appeal to the appellate tribunal if they don't agree with the DPB's decisions. Appeals must be filed digitally.

- **Child and Social Media**

Children under the age of eighteen must have parental permission to create accounts on social media sites such as YouTube, Tinder, or Meta, according to the DPDP Act. When seeking consent from minors, social media businesses are required to confirm the minors' age and the identities of their parents or guardians. The Act suggests two ways to confirm parental consent. It can use the parent's current age and identity information if they are already active users of the platform. For instance, the platform may utilise the parent's details to confirm their identification if the child requests a YouTube account and the parent has a confirmed YouTube account. An authorised organisation, like a government agency or a digital locker service, can confirm the child's identification and the parent's agreement if the parent does not use the site.[19]
"Companies could use virtual tokens linked to a parent's identity and age, which would be voluntarily provided by the parent," explained Ashwini Vaishnaw, Minister of Electronics and Information Technology. Depending on how the system develops over time, these tokens, which will be produced by the industry itself, may be connected to several different types of identities. There are a few exceptions, such as when medical personnel need to process a child's data without the parents' permission in order to deliver medical care or safeguard the child's health. Data can be processed for educational reasons by educational institutions as well. Similar to this, organisations that offer licenses, certifications, subsidies, or benefits may process a child's data in order to deliver those services. A punishment of up to Rs 200 crore may be imposed for noncompliance with the measures.

- **Breach of online data**

As soon as a data fiduciary discovers a breach involving personal data, the Act requires it to notify all affected data principals or individuals. The short and clear communication must contain the nature, extent, and timing of the breach as well as any potential consequences for those affected. The company must also reveal the measures it has taken to lower risks and provide the public with information on how to safeguard their data.
The data fiduciary must also notify the data protection board right away. They must report on the corrective measures being taken to prevent such incidents in the future, in addition

[18] The Digital Personal Data Protection Act, 2023, Act 22 of 2000), s. 18.

[19] The Digital Personal Data Protection Act, 2023, Act 22 of 2000), s. 9.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 9 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

to the details of the notifications sent to the affected data principals.

V. COMPARISON WITH INDIA AND DEVELOPED COUNTRIES

Data protection is crucial in the digital era to uphold honour and privacy. With a focus on the differences resulting from their disparate legal and cultural frameworks, this article compares and analyses the data protection legislation of the US and India. The US adopts a fragmented strategy, permitting industry-specific legislation like as COPPA, HIPAA, and CCPA while encouraging self-regulation to make enforcement easier. However, the 2023 DPDP Act of India offers a unique structure that is applicable across all industries and outside its borders. India's DPDP Act unifies government functions related to data management to offer sectoral rights, such as approval and deletion, but US legislative laws split control and enforcement of these agencies through sectoral and multi-agency verticals. Despite variations in regulatory concerns, the application of laws, and the extent of governmental control, these schematic methods serve to safeguard privacy and economic objectives. Understanding these techniques bolsters the case for loose and adaptable data protection regulations in the quickly expanding digital era.[20]

- **THE COMPARISON**

Scope and Applicability: In US regulations typically target sector-by-sector information silos as well as specific entities like banking institutions or healthcare systems. The California Consumer Privacy Act and its siblings set even greater standards, with various state-level laws placing further limitations on businesses headquartered in or operating in their states.[21] In India The DPDP Act, a more extensive, sector-neutral law, applies to all organisations that handle the personal data of Indian individuals. In terms of data processing activities conducted with the goal of delivering products or services (to be provided) within the territory, it has extraterritorial application. It also affects non-citizens who are based in India.

Individual Rights: In US number of rights are awarded based on the industry under U.S. law. Californians can see, delete, or opt out of data sales under the CCPA, parents have rights over data gathered about their children under COPPA, and individuals have authority over their health information under HIPAA.[22] In India People have many rights over their personal information under the DPDP Act, including the ability to provide their consent, withdraw their consent to access it, and request that it be updated or destroyed. By mandating data fiduciaries to inform individuals of the organisations to which their personal information has been given, the Act exemplifies transparency.

Enforcement and Regulation Supervision: In the US, enforcement is decentralised, with multiple bodies monitoring different sectors. HIPAA is enforced by the Department of Health and Human Services (HHS), whereas consumer protection laws like COPPA and GLBA are largely enforced by the Federal Trade Commission (FTC). Enforcing state laws, including the CCPA, is the responsibility of state solicitors. In India The Data Protection Board (DPB) is a regulatory body charged with investigating and penalising data breaches in accordance with the DPDP Act. The DPB's independence may be jeopardised, nevertheless, because, in contrast to the former DPA, it has the power to establish regulations or standards of conduct, and its members are selected by the government.

Data location: United States Some sector-specific legislation, such as those issued by the Department of Defence, may compel the location of specific sensitive data, even though there are no federal data localisation requirements in the United States.

[20] Rautdesai, R., Nandekar, U., Kedari, A., & Patil, Y. "Big data and privacy-a legal perspective and comparative study of the USA and India"9 *International Journal of Process Management and Benchmarking*,250-275 (2019).

[21] Illman, E., & Temple, P. *California consumer privacy act. The Business Lawyer*,1646 (2019).

[22] Warmund, J. "Can coppa work-an analysis of the parental consent measures in the children's online privacy protection act" *Fordham Intell. Prop Media & Ent. LJ*, 135 (2000).

India: The previous data localisation system's limitations are loosened by the DPDP Act. The DPDP Act has formally repealed this ban, unless law enforcement officials require it for security-related reasons. That criterion is less strict than in previous drafts.
United States Governmental Authorities and Exemptions U.S. law also permits some exemptions, such as those related to national security or a specific enforcement provision; however, these are typically specifically mentioned and restricted to specific circumstances. In India The DPDP Act gives the government extensive power to handle data without consent for state security purposes, the identification and avoidance of criminal threats, or even public health situations, as well as to exempt certain types of data custodians from specific rules. Concerns about overzealous government interference have been raised by this expansive power.

Data protection rules in the US and India are influenced by the differences in their legal and cultural systems. In the US, there has been a great deal of variation at the state level, with laws being passed to address a range of sectors, such as banking and healthcare. On the other hand, India's DPDP Act, which is somewhat similar to GDPR, attempts to address a number of issues through a centralised mechanism that would encompass everything in a single regulation. It is effective and gives the government a lot of latitude, but it is also generously dotted with exclusions of all types. Although both systems protect personal data, they employ distinct strategies, which is indicative of the larger differences between the two nations.[23]

VI. CRITICISM

- **Lack of safety standards**

The legislation's ambiguous provisions for managing data from Data Fiduciaries raise concerns about potential data leaks, eavesdropping, and cross-agency data interchange, which could jeopardise sensitive corporate information.

- **Operational Guidelines' Ambiguities**

Data processors are required by the rule to give 48 hours' notice before deleting data, however it is yet unclear how this notification would be distributed. Because there are no established protocols, organisations may take diverse approaches. Questions of arbitrary enforcement and the repression of free speech are raised by the ambiguity of phrases like "reasonable security measures," for instance.

- **High Cost of Compliance for Small Entities**

The annual Data Protection Impact Assessments, operational capacity requirements, and the INR 2 crore net worth criteria may disproportionately affect smaller enterprises, which could hinder their ability to innovate and diversify their markets.

- **Verification Gaps and Parental Consent**

There are no particular rules pertaining to parental consent and verification in the draft guidelines for data processing for adolescents under the age of 18. This requirement is open to interpretation due to the absence of clear restrictions. It is unclear who is liable in cases of deceit if a youngster is not regarded as a juvenile.

- **Absence of oversight mechanisms and concentration of authority**

The head of the Data Protection Board can move swiftly in the absence of clear review mechanisms, which raises concerns about unchecked power. This centralisation jeopardises accountability and transparency, which are essential components of sound data protection governance.

- **Language Barriers Precluding Participants Who Do Not Speak English or Hindi**

The limitations restrict accessibility and diversity by limiting public input to remarks in Hindi and English, excluding companies and experts, and prohibiting non-Hindi or English speakers.

[23] Bisht, A. K., & Sreenivasulu, N. S. *Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023. In Data Privacy-Techniques, Applications, and Standards*. IntechOpen, (2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

VII. EMERGING ISSUES AND UPCOMING PROGRESS

A date for the DPDP Act's implementation has not yet been set. The DPDP rules are open for public comment until February 18, 2025. Because of this, the above-mentioned suggested changes might not be completed or might be changed before they are. Additionally, it is anticipated that the DPDP Act and related regulations will be implemented gradually. As a result, when the new laws take effect, employers will have time to get ready.

The swift development of social media technology still presents difficulties for governmental regulation. The legal system must be updated frequently to address problems like deepfakes, bitcoin advertising, and AI-powered content moderation. The confluence of social media with other digital services, digital payment systems, and OTT platforms all require coordinated regulatory responses.[24]

The intricate issue of juggling conflicting interests in the digital age is reflected in India's legal framework for social media regulation. Effective execution, stakeholder collaboration, and flexibility in the face of new obstacles are essential to this framework's success. The legal system must adapt as social media develops in order to safeguard fundamental rights and encourage proper conduct online. To handle emerging technological challenges while upholding fundamental rights and social harmony, India's social media laws would probably need to be modified frequently.

VIII. CONCLUSION

India's data protection has advanced significantly since the Digital Personal Data Protection Act, 2023 was passed. It strikes a balance between the growing need for data in the digital economy and the need to protect people's privacy. The Act gives people rights and places obligations on organisations by offering a thorough framework for the gathering, handling, and archiving of digital personal data.[25]

Despite being a significant positive step, the DPDPA has a number of problems. To guarantee the Act's efficacy, concerns around consent management, cross-border data transfers, and the brief tenure of DPBI members must be resolved.

The DPDPA, 2023, will probably be updated and revised in response to new technology developments and the changing digital landscape as India continues to lead in the digital era. This law creates a strong basis for data protection that safeguards people's rights and aids India in realising its goal of becoming a "Digital India."

REFERENCES

- The Digital Personal Data Protection Act, 2023, No.22, Acts of Parliament, 2023.
- Dhiraj R. Duraiswami, *Privacy and Data Protection in India, 6 J.L. & CYBER WARFARE*, 169-172(2017).
- NANDAN KAMATH, *Law Relating To Computers, Internet, And E-Commerce: A Guide To Cyber LawsAnd The Information Technology Act*, 2000 121 (Kamal Law House, Calcutta,1st Ed. 2020).
- Jason Asbury, Maria McClelland, Kris Torgerson, India Vincent & Jennifer Boling, "Law and BusinessTechnology: Cyber Security & Data Privacy Update" 20 *Transactions: TENN. J. BUS. L.* 1065, 1067-71(2019).
- AZBPARTNERS, https://www.azbpartners.com/bank/digital-personal-data-protection-bill-2023-key-highlights last visited (Jan 25, 2025).
- Sha Suri, Rajat Kathuria, *Digital Personal Data Protection Act: The speedbumps ahead,* INDIANEXPRESS (Feb 1, 2025, 1:05 PM).
- DUBEY,R.K.,VERMA,A.*Data Protection And Privacy Implementation: India Perspective* 12(Independently published 2019).

[24] sha Suri, Rajat Kathuria, *Digital Personal Data Protection Act: The speedbumps ahead*, INDIANEXPRESS (Feb 1, 2025, 1:05 PM)

[25] DUBEY,R.K.,VERMA,A.*Data Protection And Privacy Implementation: India Perspective* 12(Independently published 2019)