Navigating AI's Effect On Privacy Issues In Social Media: An Indian Legal Perspective

Madhangi. N & Mahalakshmi. S
5th Year B. Com LL.B (Hons.) Students
School of Law
SASTRA Deemed To Be University,
Thanjavur, Tamil Nadu, India

ABSTRACT

Social Media - an interactive technology that facilitates the connection of individuals at different hemispheres with just a single tap. It with its growing consumption has become an indispensable part of everyone's life. Data – 'the new oil' used by social media is not just a digital byproduct but a component of strategic growth and innovation. With the advent of Artificial Intelligence, society has been benefitted in numerous ways but due to inadequacy in regulations, protecting our privacy has become almost impossible. The AI's deployment in Social media is an even bigger threat to the privacy. Data is generated from post, comments, likes, shares and interactions in massive quantity by social media platforms. AI Algorithm exploits this data from social media to provide content suggestions, personalized services, targeted advertising and etc**.** Therefore, this paper attempts to shed light on the AI's repercussions on privacy in social media by emphasizing the necessity of its regulations, as it violates rights enshrined under Article 21 of the Indian constitution. This paper further highlights the lacunas in the Indian Legislations and suggests imposition of certain regulations to address them. It employed a qualitative method of research utilizing various primary and secondary sources. The study identified that the employment of AI in social media platforms renders the Information Technology Act, 2008 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 insufficient to regulate the content moderation practices and it is likely to violate certain provisions of these regulations. The Digital Personal Data Protection (DPDP) Act's effectiveness in regulating artificial intelligence (AI) is limited due to the exemptions of publicly available data and data processed for research purposes from the ambit of this Act. The absence of stringent oversight mechanisms further exacerbates these limitations.

KEYWORDS: Artificial Intelligence, Social Media, Privacy, the Information Technology Act, 2008, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection (DPDP) Act, 2023.

I. INTRODUCTION

Artificial Intelligence (AI) refers to computer programs that are capable of performing complex tasks that were previously only performed by humans, such as reasoning, problem-solving, and decision-making. It is transforming every aspect of existence. It is not a vision of the future; rather, it is something that exists now and is being employed in many different sectors. This covers industries including banking, healthcare, criminal justice, national security and transportation. The impact of artificial intelligence is most prominent in social media platforms

which facilitate communication between individuals around the world. Artificial intelligence and social media platforms are closely twined with one another.

Artificial intelligence is employed by social media to improve user experience and personalization. AI tools assist in improving social media platform features and managing social media operations at scale in various contexts, such as creating text, graphic content, managing ads, conducting brand awareness campaigns and more. It analyzes the data generated by posts, comments, likes, shares, and interactions.

Thus, AI has become an indispensable tool to any social media platform on the planet. Facebook uses advanced machine learning to provide personalized content and recognizes face that facilitates advertising to the target users. AI tools facilitate LinkedIn, in suggesting and recommending jobs that might interest the user and Snapchat to track facial features and overlay filters that move with our faces in real-time.

Huge data is relied upon to train their algorithms, which will enhance user experiences on social media platforms that act as a detriment to the one who provides data. Data can include personal information such as names, addresses, financial information, and other sensitive information such as medical records and social security numbers. Unauthorized collection or processing of this data results in violation of the right to privacy guaranteed under Article 21 of the Indian Constitution. It is pertinent to note that the use of AI in social media has a graver impact on privacy and is an issue across jurisdictions.

The Federal Trade commission vs. Facebook (2019)[1], is one of the landmark lawsuits that depicts the impact of the employment of AI tool in social media platforms. In this case, despite repeated claims to its billions of users worldwide that they would have control over how their personal information was shared, Facebook frequently employed deceptive disclosure and settings to undermine users' privacy preferences. These strategies enabled the corporation the use of Artificial Intelligence to collect and share users' personal information with third-party apps without their consent downloaded by the user's Facebook "friends". It informed its users that it would gather their phone numbers to enable a security feature, but failed to disclose that those numbers would also be used for advertising purposes. Facebook agreed to pay $5 billion to settle the claims of FTC and a future privacy order was issued that overhauls the way the platform takes privacy decision-making by increasing transparency.

The US Federal Trade Commission on September 19, 2024, also published a report on reviewing several social media platforms including Meta Platforms, Byte Dance's TikTok, Amazon's gaming platform, YouTube, social media platform X, Snap, Discord and Reddit. The findings of the report showed that the teens and kids are prone to unique risks due to the It stated that data management and retention policies of these platforms are not in alignment with regulating AI's employment in these platforms which collected or guessed users' age, gender, income, education and family status. It further stated that this threatens people's privacy which further interferes with their freedom and subjects them to several harms that might even endanger their life.[2]

[1] Federal Trade Commission v. Facebook, Inc., No. 19-cv-02184 (D.D.C. July 24, 2019)

[2] **Alvaro M. Bedoya, Statement on the Social Media 6(b) Report,** Fed. Trade Comm'n (Dec. 6, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/bedoya-statement-social-media-6b-report.pdf.

The Internet Governance and Policy Project examined the compliance reports submitted by significant social media intermediaries to the Ministry of Electronics and Information Technology, as stipulated by Rule 4(1)(d) of the IT Rules, 2021, and published a report in October 2024. The report primarily focused on determining the transparency commitments of these intermediaries by assessing their adherence to the obligations outlined in the IT Rules, analyzing the compliance reports of different platforms and comparing instances of varying levels of disclosure between platforms, while also reviewing transparency standards in other jurisdictions that could enhance the Indian regulatory framework. The findings of the report highlighted the need for stricter monitoring of the disclosure reports from significant social media platforms to ensure completeness and consistency. It also emphasized on robust transparency standards in response to the increased use of automated tools in content moderation and the rise in misinformation, hate speech and harmful online content[3]. Thus, the rapid technological advancements heightening these risks serves as an eye opener, necessitating regulatory frameworks and ethical guidelines to address privacy issue.

II. BACKGROUND:

The sharing of opinions, ideas and news with one another was possible only with the various means of communication like cave paintings and sculpting to newspapers, letters, books, telegraph, telephone, television and etc. This evolution spurred the rise of mass media, which connected people from different places. Initially, only a few were able to communicate and provide their opinion, share ideas and news. However, with the emergence of internet in the 1990s, everyone was allowed to share their thoughts, ideas and experiences which led to the development of social media. The first social media sites to appear in the late 1990s were Friendster, Six Degrees, and MySpace. Through fundamental features like texting and profile customization, these social media sites primarily made it easier for friends to communicate. These sites relied on simple algorithms. Privacy issues were minimal due to limited sharing of personal information.

Renowned social media platforms like Facebook, LinkedIn, and Twitter developed in the mid 2000s. These social media platforms employed algorithms which used huge data for personalized content and enhanced user experience. Thus, data scrapping led to data privacy concerns. Social media platforms like Facebook brought privacy settings that allowed users to have control over their posts. Users were unaware to the privacy considerations, therefore the impact was modest.

The 2010s saw the emergence of social media sites such as Instagram, Snapchat, and TikTok, which began using sophisticated AI algorithms for targeted advertising, image recognition, and tailored feeds. These algorithms scrape data without explicit user agreement, raising severe privacy concerns and necessitated the need for stronger privacy safeguards.[4]
Until 2017, privacy was not identified as a fundamental right but was recognised as a right by the courts in numerous cases with various dimensions. Since, right to privacy was not a guaranteed right under the Indian Constitution, it was considered only as a part of life and personal liberty enshrined under Article 21 of the Constitution. Then the Supreme Court in the landmark case of

[3] **Internet Governance and Policy Project**, *Social Media Transparency Reporting: A Performance Review*, **IGAP** (2024), https://igap.in/social-media-transparency-reporting-a-performance-review/.
[4] **TechTarget**, The History and Evolution of Social Media Explained, https://www.techtarget.com/WhatIs/feature/The-history-and-evolution-of-social-media-explained.

Justice K.S. Puttaswamy v Union[5], 2017, popularly known as the Aadhaar Case, held that Privacy is a fundamental right under Article 21.The Court's opinion in this case is that right to privacy must be protected against both state and non-state actors, however it was not declared as absolute right and has restrictions.

The Supreme Court in this case provided a three-fold requirement: there should be a law in existence, the legislation should have reasonable content and restrictions free from arbitrariness, and be proportional to the purpose of the law to justify that privacy is being violated. Thereby, it emphasized that the state has the duty to make legislations and to take all measures to protect the privacy of the individual. It also underscored that the balance between the legitimate concerns of the state and individual interest must be ensured while balancing the data regulation and individual privacy. The judgment emphasized principles such as consent, choice, purpose, collection, disclosure, retention, proportionality and legitimacy.

The Justice K. Puttaswamy judgment and the growing privacy concerns due to the technological advancement had a significant impact in prompting the state to take measures to protect and balance the privacy of individuals and society without obstructing the technological advancements. The enactment of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and the Digital Personal Data Protection Act, 2023 are some measures by the government in compliance of guidelines of Justice K. Puttaswamy Judgment to protect privacy. [6]

The increased complaints by the users against the intermediaries being ignorant about objectionable content and suspension of accounts led to the replacement of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 with the 2011 Rules. The intent of the rules is to make an open, safe, trusted and accountable internet and also to uphold the fundamental rights under Article 14, 19 and 21. This rule explicitly included the social media intermediaries and the significant social media intermediaries.

The Digital Personal Data Protection Act, 2023 Act imposed accountability on entities that collects and processes personal data. It mandated the entities to provide notice to users and obtain consent from users regarding the purpose of the processing of data. It guarantees the users the right to access, erase and port their data and had also brought in robust grievance redressal systems by establishing Data Protection Board of India.

In future, AI tools will be employed by social media platforms to automatically recognize harmful content such as hate speech, misinformation and also help users in generating content, from automated video editing to AI-generated artwork and writing. However, the growing artificial intelligence will create bias, continuous surveillance, erosion of trust, data breach, and issues of transparency that could negatively impact the life of the people, mandating the need for vigorous privacy regulations and a culture of accountability.

[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)
[6] Sharma, V. and Sharma, S., 2023. Information Technology: Law and Practice: Cyber Laws and Laws Relating to E-commerce, Privacy, Social Media, Defamation. Universal: LexisNexis.

III. LITERATURE REVIEW:

Social media and artificial intelligence, important components of technological advancement have amplified privacy concerns. The use of AI system in social media has increased the ambit of privacy violations to an even greater extent. Previous research focused on the impact of social media on privacy, the impact of AI on privacy, the impact of AI's employment in social media but not on the impact of AI being employed in social media on privacy particularly in respect of Indian legislations. Thus, the primary focus of this research is to analyse and identify if the Indian legislations are sufficient to regulate the AI's employment in social media.

Dr. Lukose. L & Mathur. A (2019), examined the role of social media in respect of human rights, both as a tool for education and awareness, and in facilitating abuses like surveillance, data theft, and privacy violations. The potential threats found by the research are surveillance, interception, data theft, privacy, unauthorized access and retention of data etc. They suggested that if the social media is used sensibly then it can create an interwoven environment whereby the human rights can be protected, promoted and enforced effectively.[7] Dr. Shashi Punam, Dr. Manu Sharma, Dr Sanjeev Kumar (2024) examined the developing legal frameworks on social media and stressed the significance of establishing encryption laws to strike a balance between data security and privacy concerns. They identified that encryption will be a guardian of data in the digital realm.[8]

Elsir Ali Saad Mohamed, Murtada Elbashir Osman and Badur Algasim Mohamed (2023) analysed the effects of AI on social media content, highlighting implications for creators and consumers, with a particular focus on misinformation and filter bubbles. It identified that the AI algorithms prioritize content that confirms users' existing beliefs leading to polarization and lack of exposure to opposing viewpoints. Additionally, AI algorithms promote sensational or emotional content likely to go viral, even if inaccurate. The study recommended that the social media platforms must ensure transparent and ethical practices to maintain user trust, promote media literacy and employ human moderation.[9]Matthew N.O. Sadiku, Tolulope J. Ashaolu, Abayomi Ajayi-Majebi, and Sarhan M. Musa (2021) examined AI tools employed in social media, their applications, and their pros and cons. They identified AI tools such as Fuzzy logic, Machine learning, Neural networks, expert systems, Deep Learning, Natural Language Processors and Robots being employed in social media platforms. These tools are used for advertising, marketing, automation, social insights, crime prevention and ensuring security and justice. Some of the benefits of using these tools are refined content targeting, cost reduction, increased audience engagement, reducing marketing costs with better return on investments, incremental revenue and etc. The challenges were identified to be privacy concerns, AI models inaccuracy and shortage of talent.[10]

[7] Lukose, L. and Mathur, A., 2019. Human Right and Social Media. Elcop Yearbook of Human Rights, March, pp.31-38.
[8] Punam, S., Sharma, M. and Kumar, S., 2024. Socio-Legal Aspect Of Social Media In India: Navigating Encryption And Legal Frameworks For Social Media Regulation. Educational Administration: Theory and Practice, 30(5), pp.12129-12135.
[9] Mohamed, E. A. S., Osman, M. E. & Mohamed, B. A. (2024). The Impact of Artificial Intelligence on Social Media Content. Journal of Social Sciences, 20(1), 12-16.
[10] Sadiku, Matthew & Ashaolu, Tolulope Joshua & Ajayi-Majebi, Abayomi & Musa, Sarhan. (2021). Artificial Intelligence in Social Media. International Journal Of Scientific Advances. 2. 10.51542/ijscia.v2i1.4.

Rowena Rodrigues (2020) examines the legal and human rights issues surrounding AI, how are the problems being addressed and the existing gaps and challenges. The researcher also focuses on the impact of these issues on vulnerable groups and on human rights principles. The study considered certain key issues that include algorithmic transparency, cyber security vulnerabilities, bias, unfairness, lack of contestability, adverse effects on workers, privacy and data protection issues, and lack of accountability. The study identified that the lack of algorithmic transparency and accountability to be the main problem and suggests solutions such as creating awareness, algorithmic transparency standards**,** by bestowing a right to object to automated decision making etc. It also stipulated that the developers should follow the ethical and regulatory restrictions at each stage of data processing. It was identified in this study that the human rights principles such as right to fair trial, free elections, privacy, freedom of expression, elimination of discrimination, right to life and personal liberty, right to equality and right to effective remedies are affected by the use of AI tools. The study discovered that the vulnerable groups are the most disadvantaged population as a result of the use of AI technologies.[11]

Navmi Joshi and Dr. Monica Kharola (2024) explored the intricate issues surrounding privacy protection in the age of artificial intelligence. They also looked at the evolving relationship between privacy laws and technological advancements. This article highlights the significance of robust legal frameworks and decentralized AI platforms for safeguarding privacy. The study's conclusions show that pursuing privacy protection in the AI era requires teamwork and the convergence of technological innovation, ethical responsibility, and regulatory foresight.[12]

IV. RESEARCH PROBLEM

The employment of Artificial Intelligence in social media platforms raises privacy concerns due to the lack of transparency in algorithms and easily exploitable security systems, necessitating effective regulations. Despite these concerns, there is a lack of comprehensive study regarding the effectiveness of the regulations. This research paper bridges this gap by examining whether the existing regulations on social media platforms and data privacy in India adequately address these issues.

V. RESEARCH QUESTION:

1. Whether the existing Indian Laws and regulations sufficient to address privacy concerns related to Artificial Intelligence deployed in social media platforms?
2. How can Indian data protection laws be strengthened to regulate AI-driven social media platforms?

VI. RESEARCH OBJECTIVE:

1. To study whether the existing Indian laws and regulations are sufficient to address privacy concerns due to the employment of AI in social media.

[11] Rodrigues, R., 2020. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, p.100005.

[12] Joshi, N., 2024. Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence. International Journal of Law and Policy, 2(4), pp.55-77.

2. To recommend various measures for strengthening of Indian data protection laws relating to regulate AI-driven social media platforms.

VII. RESEARCH METHODOLOGY:

This study follows the doctrinal research methodology that is predominantly conceptual and literature-based. It examined research papers, legislation, books and newspaper articles. The legal frameworks analysed were The Information Technology Act, 2000, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Digital Personal Data Protection Act, 2023. The study strives to identify lacunae and loopholes in these existing regulations to determine if they are sufficient to regulate the deployment of AI in social media. Additionally, suggestions are provided to make the regulations reliable in alignment with technological advancements.

VIII. RESEARCH METHOD:

This doctrinal research study analysed research papers, legislation, books and newspaper articles, whereby most of the information was collected from secondary sources. The K. Puttaswamy judgment was studied to show the importance of privacy and significant principles endorsed in the judgment relating to privacy. Further, newspaper articles and other online sources were analysed to portray the impact of AI on privacy. The literature review was based on research papers that primarily focused on social media's impact on privacy, AI's impact on privacy, the impact of employing AI in social media platforms and the impact of AI on privacy regulations. The literature review helped in finding the research gap and the research problem is: whether the existing privacy and social media regulations in India are sufficient to regulate the deployment of AI in Social media platforms. The Information Technology Act, 2000, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Digital Personal Data Protection Act, 2023 was analysed to identify lacunae and loopholes in these existing regulations and to provide suggestions to regulate AI deployed in social media platforms. The European Union Artificial Intelligence Act, 2024 was also referred to provide recommendations to safeguard privacy.

IX. FINDINGS AND DISCUSSIONS:

The Information Technology Act, 2000 & The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021

The Information Technology Act, 2000, defines an intermediary under Section 2(w) as any person who, on behalf of another person, receives and stores or transmits electronic records, or provides any related service. This definition was extended in 2008 to include telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes. The social media intermediaries are classified under web hosting service providers, thereby bringing them under the regulatory framework of the IT Act.

Section 79 of the Act provides exemption to the intermediaries from their liability if they limit their function to facilitating communication systems to transmit information to third parties. They will be held liable only if they initiate transmission, select the receiver, modify the

information, involve in criminal acts, or fail to remove or disable access to a material within 36 hours of being notified by the appropriate government.

Further, under Section 79(2)(c), it provides that the non-observance of the due diligence guidelines laid under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, will not only lead to the loss of the safe harbor clause but also hold the intermediary liable under the Information Technology Act, Indian Penal Code, or under any other law in the territory. Thus, this section strives to strike balance between individual and societal interests while encouraging technological advancement.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, provide due diligence guidelines under Rule 3 and 4 to be observed by both the social media intermediary and the significant social intermediary. These guidelines provide self-regulating mechanisms for content moderation, which are to be complied by the intermediaries as a statutory duty. Significant Social Intermediaries have more registered users in India than the thresholds set by the Central Government and are required to submit a report monthly stating the compliance of the IT rules 2021. The IT rules 2021 provides the intermediaries to regulate the content, classify the contents based on age and to ensure better grievance redressal mechanism to the users while upholding creative freedom. The main purpose of the rules is to ensure transparency and accountability to the users in content moderation practices.

Rule 3(1)(a) mandates that consumers be well informed about the rules, regulations, privacy policy, users agreement by the intermediary by publishing it in its website in a manner that makes the user to understand in a easy manner. Rule 3(1)(b) and the appendix to Rule 8 stipulate the intermediaries must not host or handle content that invades privacy, is obscene, incites violence, or causes the integrity of the nation. However, the use of AI and automated tools for content moderation lacks algorithmic transparency and accountability, keeping the users in dark about content moderation practices, resulting in violation of these rules.

Rule 3(1)(k) stipulates intermediaries shall not make changes to the technical configurations that deviate from the normal course of operation and violate any law, but may do so if it enhances the user's security. The employment of AI tools in social media is a shift from the normal course of operation and enhances user experience. However, it doesn't ensure user security as it lacks transparency and accountability.

Rule 4(1)(d) requires significant social media intermediaries to publish a monthly compliance report detailing grievances received, actions taken, and the number of contents removed. It must also include the methods used to identify and address content violations, which includes the use of automated tools for content regulation. These tools lack transparency, which prevents full disclosure by the intermediaries in the report.

Section 43A of the Information Technology Act, 2000 and Rule 3(1)(i) of the 2021 Rule mandate the body corporate, including intermediaries and government entities that deal with the sensitive personal data to follow the standards as provided in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 and secure their computer resources without negligence. If these are implemented or maintained negligently and result in wrongful loss or wrongful gain to any person, then the body corporate will be liable to pay damages. Nevertheless, the use of AI and automated tools in the content

moderation practices lacks transparency as the standards under these rules have become outdated not enough to regulate the artificial intelligence tools employed in social media.

Section 67C of the Act and Rule 3(h) dictate that intermediaries can preserve and retain the information collected from users for registration on the computer resource for a period of 180 days after the users withdraw or cancel their registration. This provision establishes the right to erasure or the right to be forgotten. However, AI fails to guarantee this right because information provided becomes permanent and never gets erased.

Section 72A of the Act provides that when an intermediary gains access to personal information about another person under a lawful contract, it must not disclose it to a third party with an intent or knowledge of causing wrongful loss or gain to that person without the person's consent. Such a breach may result in imprisonment for up to 3 years or a fine up to 5 Lakhs or both. The deployment of AI tools on social media platforms fails to impose penalties, as users remain unaware of whether a breach has occurred. Even if a breach is identified, it is difficult to establish due to a lack of transparency.

Thus, the employment of AI in social media platforms presents a challenge to the existing legal frameworks, such as the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These regulations are insufficient to address complexities of AI-driven content moderation practices and threaten privacy, underscoring the need to revise them.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act aims to safeguard individuals' privacy by establishing a comprehensive framework for the processing of personal data. The Act emphasizes two pivotal principles: Purpose Limitation and Data Minimization. Purpose Limitation dictates that personal data can only be processed for predefined, legitimate purposes with informed consent, while Data Minimization ensures only necessary data relevant to the declared purpose is collected and processed to prevent excessive data collection. The Act seeks to protect the privacy of individuals by enacting a extensive framework for processing personal information. The Act focuses on two key principles: Purpose Limitation and Data Minimization. Purpose Limitation requires that personal data be processed solely for specific, legitimate reasons with the individual's informed consent, whereas Data Minimization guarantees that only essential data pertinent to the specified purpose is gathered and processed to avoid unnecessary data accumulation.

Though there is no specific inclusion or exclusion of AI from the Act's scope, nor is AI mentioned in any provision or part of the Act. The DPDPA governs how social media platforms use and process personal data, which in turn impacts the AI which processes the data.

Under this Act, social media platforms must obtain consent from users (data principals) before processing their personal data and ensure that the processing is for a legitimate reason. The use of artificial intelligence to process personal data should be restricted to only what is necessary for the specified purposes. These platforms are required to uphold the rights of data principals, including the right to receive a summary of their personal data that is being processed by a Data Fiduciary, as well as the identities of all other Data Fiduciaries and Data Processors to whom the

data is shared. Other rights include right to correction, completion, updating and erasure of her personal data, right of grievance redressal, right to nominate given under Chapter III of the Act. Social media platforms have a duty to implement robust security measures to safeguard personal data against unauthorized access, disclosure, modification, and destruction. A comprehensive security policy should encompass encryption, secure storage, and access controls for AI systems that manage large amounts of sensitive data.

Although the act contains provisions that safeguard privacy, it also contains certain provisions that significantly undermine its effectiveness and render it ineffective.

A significant provision Section 3(c)(ii) under the DPDPA is the exclusion of publicly available data entirely from the scope of regulation.Data that is publicly accessible online is susceptible to data scraping, and artificial intelligence (AI) can exploit this to analyze vast amounts of information for illegal purposes, which could undermine the privacy protections intended by the Act. The scenario in which personal data that was once public is later restricted raises another complex issue. For example, a user may start with a public Instagram profile and subsequently switch it to private. It remains ambiguous whether personal information that was previously public can still be processed by AI once it is no longer accessible.

According to Section 4 of the Act, data processing must be done solely for specific legitimate purposes. There is a strict oversight system in place to verify that Artificial Intelligence processes the data only for these legitimate reasons in the case of significant data fiduciaries. Under Section 10, significant data fiduciaries are required to designate an independent data auditor to perform a data audit and carry out regular Data Protection Impact Assessments.

Under Section 12 of the Act data principal shall have the right to erasure of personal information. The ability of AI systems to delete its own memory is a matter of debate.This highlights the necessity to either retrain AI systems or explore alternative methods to adhere to the regulation.

As stipulated in Section 17(2)(b) of the DPDPA, processing data for research purposes is exempt from the regulations laid out in this act. However, this exemption is applicable only if the processing does not involve making "any decision specific to a data principal" and complies with the standards set by the Central Government. At present, it remains unclear whether the research exemption within the DPDPA will be applicable solely to academic entities or extend to businesses engaged in research activities. Social media platforms like Instagram process data for research and provide data to external researchers and there is a significant risk of misusing this provision.

The 2019 draft of the bill included a specific category of "sensitive personal data," which encompassed attributes such as sexual orientation, transgender or intersex status, caste or tribe, religious or political beliefs or affiliations and biometric information and processing such sensitive data needed a stricter level of compliance. In contrast, the current law does not differentiate between personal data and sensitive personal data. The collection and processing of such data render the data principals vulnerable, potentially infringing on fundamental rights and resulting in greater harm if misappropriated. Although the 2019 bill did not explicitly include safeguards against discrimination, it identified and aimed to prevent possible methods through which discrimination might occur.

Thus the Act's effectiveness is diluted due to the above mentioned lacunas.

X. SCOPE & LIMITATION:

This study focuses only on evaluating the Indian laws that regulates data privacy and social media platforms. This research relied on the secondary sources including articles, book, expert opinions and etc which may contain inherent biases. Since, the Data protection laws are still at a developing stage in India, there may be potential changes in the legal framework during the research.

XI. RECOMMENDATIONS:

The swift progression of artificial intelligence and the lacunae in the existing regulation to regulate artificial intelligence has prompted the researchers to suggest revising the existing legal frameworks to ensure effective governance. The employment of AI in social media is detrimental to privacy. Hence, researchers suggest the following recommendations:

- The principals of data minimization, purpose limitation and consent needs to be rigorously incorporated into the regulations so that AI tools in social media doesn't make unauthorized collection of data. Consumers should have the right to give consent only to those information or data they choose to share, which should be used only for the purpose as agreed upon by the consumer.
- Privacy policy, which contains details of how a company handles data must not be arbitrary and ensure the customer's data privacy. It should include how AI will collect and process data.[13]
- The Government must update the existing security standards in consonance with the technological advancement as necessary.
- The intermediaries must employ only approved algorithms and AI tools.
- The enactment of precise regulatory DPDP rules acquires essential significance in order to maintain consonance with developing technical advancements and to overcome current regulatory gaps.
- Exemption of publically available data dilutes privacy. Though the data fiduciaries are exempt from obtaining individual's consent, they should be imposed with the data protection obligations even when processing publicly available data.

The European Union Artificial Intelligence Act, 2024, endeavors to protect health, safety, and fundamental rights enshrined in the charter—democracy, the rule of law and environmental sustainability from the detrimental effects of AI systems, while promoting human-centric and trustworthy artificial intelligence, technological innovation in AI. The incorporation of the standards outlined in the Act into the Indian regulatory framework would ensure privacy in social media platforms. They are

- To ensure transparency, intermediaries must document data collection practices and regularly share them with consumers, empowering them to have better control over their data. The document should clearly outline how a person's data is being collected, what data is being collected, and the purposes for which it is used.

[13] King, J. and Meinhardt, C., 2024. Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World.

- To ensure compliance with stricter data protection standards and an user-friendly environment, platforms should be closely monitored to prevent data exploitation.
- To assure accountability, platforms must establish risk management systems, conduct regular audits, and maintain detailed records of AI processes to prevent harm caused by errors or misuse.
- Intermediaries must employ AI tools that detect, mitigate, and prevent discrimination and bias in automated decision-making, content moderation algorithms, personalized content recommendations and targeted advertising practices.[14]

XII. CONCLUSION:

Social media platforms, which have become an integral part of our lives, symbolize technological advancement; however, it raises significant privacy issues. The employment of AI in social media is an even bigger threat to privacy. Therefore, technological advancement must not be made at the cost of the privacy of an individual. Thus, there is a need to strike balance between technological advancement and privacy issues, which can be achieved by the enactment of rules that will ensure transparency and accountability among intermediaries and data processors. The Information Technology Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is deficient to address the complexities arising from the employment of AI in social media platforms**.** Therefore, it is necessary to make regulations that will ensure transparency and accountability of the social media platforms in content moderation practices. Due to presence of potential loop holes, the Digital personal Data Protection Act (2023) is inadequate in protecting personal data. Privacy safeguards are threatened by the exclusion of publicly available data and by inadequate oversight for legitimate processing. The exemption of research from the ambit presents hazards in the absence of defined regulations, even though it could help in progression of AI. We could protect personal data privacy while navigating the difficulties of an increasingly data-centric economy by adapting legal frameworks which accommodate evolving technology.

XIII. REFERENCES:

1. Federal Trade Commission v. Facebook, Inc., No. 19-cv-02184 (D.D.C. July 24, 2019)

2. Alvaro M. Bedoya, Statement on the Social Media 6(b) Report, Fed. Trade Comm'n (Dec. 6, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/bedoya-statement-social-media-6b-report.pdf.

3. Internet Governance and Policy Project, *Social Media Transparency Reporting: A Performance Review*, IGAP (2024), https://igap.in/social-media-transparency-reporting-a-performance-review/.

4. TechTarget, The History and Evolution of Social Media Explained, https://www.techtarget.com/WhatIs/feature/The-history-and-evolution-of-social-media-explained.

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

[14] Busra Oguzoglu, The EU AI Act: How Will It Shape the Future of Social Media?, MEDIUM (Nov. 15, 2024), https://medium.com/@busra.oguzoglu/the-eu-ai-act-how-will-it-shape-the-future-of-social-media-320c29376052.

6. Sharma, V. and Sharma, S., Information Technology: Law and Practice: Cyber Laws and Laws Relating to E-commerce, Privacy, Social Media, Defamation. (LexisNexis 2023).

7. Lukose, L. and Mathur, A., Human Right and Social Media. Elcop Yearbook of Human Rights, March 2019, at 31-38.

8. Punam, S., Sharma, M. and Kumar, S., Socio-Legal Aspect Of Social Media In India: Navigating Encryption And Legal Frameworks For Social Media Regulation. Educational Administration: Theory and Practice, 30(5), pp.12129-12135 (2024).

9. Mohamed, E. A. S., Osman, M. E. & Mohamed, B. A., The Impact of Artificial Intelligence on Social Media Content. Journal of Social Sciences, 20(1), at 12-16 (2024).

10. Sadiku, Matthew & Ashaolu, Tolulope Joshua & Ajayi-Majebi, Abayomi & Musa, Sarhan. Artificial Intelligence in Social Media. International Journal Of Scientific Advances. 2. 10.51542/ijscia.v2i1.4 (2021)..

11. Rodrigues, R., Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, p.100005 (2020)..

12. Joshi, N., Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence. International Journal of Law and Policy, 2(4), pp.55-77 (2024).

13. King, J. and Meinhardt, C., Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World (2024).

14. Busra Oguzoglu, The EU AI Act: How Will It Shape the Future of Social Media?, MEDIUM (Nov. 15, 2024), https://medium.com/@busra.oguzoglu/the-eu-ai-act-how-will-it-shape-the-future-of-social-media-320c29376052.