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

SOCIAL MEDIA DATA MINING: ETHICAL AND LEGAL CONCERN

AUTHOR - AMAN KUMAR MISHRA, STUDENT AT AMITY LAW SCHOOL, AMITY UNIVERSITY, MUMBAI

BEST CITATION - AMAN KUMAR MISHRA, SOCIAL MEDIA DATA MINING: ETHICAL AND LEGAL CONCERN, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (9) OF 2025, PG. 236-246, APIS – 3920 – 0001 & ISSN - 2583-2344.

This article is published in the collaborated special issue of Amity Law School, Amity University, Mumbai and the Institute of Legal Education (ILE), titled "Emerging Trends in Law: Exploring Recent Developments and Reforms" (ISBN: 978-81-986345-1-1).

Abstract

This paper provides a critical analysis of the ethical and legal aspects of social media data mining, with a particular emphasis on the legal context in India. It utilizes global case law, ethical theories, statutory frameworks, and judicial interpretations to highlight the shortcomings in existing regulations and to suggest a rights-based regulatory framework that is prepared for the future. The analysis seeks to align global best practices with the realities in India, ultimately aiming to deliver actionable policy recommendations and encourage informed legal reform.

1. Introduction

1. Introduction

The 21st century has seen social media evolve into more than just a communication tool; it has become a global socio-political ecosystem. As of 2024, there are over 4.95 billion users worldwide on platforms like Facebook, Instagram, Twitter (now X), LinkedIn, and TikTok. These platforms play a crucial role in shaping public discourse, influencing political outcomes, and even guiding economic decisions[375]. However, the vast amount of data generated by users—ranging from personal information to behavioral trends—has turned social media into a treasure trove for data miners.

Social media data mining, which involves extracting valuable insights from user-generated content, has emerged as a key resource in various fields, including marketing, law enforcement, and political campaigning. Nevertheless, this growing practice raises significant ethical and legal challenges. Central to these concerns is a critical question: how can society reconcile the commercial and analytical benefits of mined data with individuals' rights to privacy, autonomy, and dignity?

India, with its large digital population and evolving legal framework, finds itself at a pivotal moment. The absence of comprehensive data protection laws, combined with the judiciary's acknowledgment of privacy as a fundamental right, creates a paradox where technological advancement outstrips regulatory measures. Globally, frameworks like the European Union's General Data Protection Regulation (GDPR) and the United States' sector-specific laws offer contrasting governance models that provide valuable insights for Indian legal practices.

This paper seeks to explore the ethical dilemmas and legal complexities associated with social media data mining, analyzing how Indian law is equipped to address these techno-legal challenges by examining insights from international standards. Ultimately, it aims to determine if existing laws are sufficient to safeguard individual rights in a world that is increasingly influenced by digital surveillance and algorithmic decision-making.

[375] Number of worldwide social network users 2028| Statista. (2024, May 17). Statista. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

2. Conceptual Framework: Understanding Social Media and Data Mining

To fully grasp the legal and ethical implications of data mining on social media, it is essential to first understand the two core concepts both separately and together.

2.1 Social Media: The Digital Agora

Social media encompasses online platforms that enable users to create, share, and interact with content within a network. Notable examples include Facebook, Instagram, Twitter (now X), LinkedIn, YouTube, Snapchat, and TikTok. These platforms function as hybrid environments—part public forum and part private database—where users engage voluntarily, often under the misconception that they have control over their personal data.

The primary legal challenge stems from the uncertainty regarding whether the content shared on these platforms is public or private. While users willingly share information, the distinction between public expression and private communication is often unclear. In the case of R v. Cole, the Canadian Supreme Court determined that a "reasonable expectation of privacy" can persist even for data stored on devices owned by employers[376], establishing a precedent that has global implications.

2.2 Data Mining: The New Oil Rush

Data mining is the computational process of identifying patterns, trends, and relationships in large data sets through techniques like machine learning, statistical analysis, and artificial intelligence. When used in the context of social media, this process enables organizations to deduce specific personal traits, including political views, mental health conditions, sexual orientation, and buying habits.

The social media data mining process typically includes:

- **Data Collection**: Through APIs, web scraping, or user consent-based access.
- **Pre-processing**: Cleaning and structuring raw data.
- **Analysis**: Applying algorithms to detect trends or make predictions.
- **Actionable Insights**: Using results for targeted advertising, behavioral nudging, or surveillance.

Notably, in the infamous *Cambridge Analytical* scandal, data from over 87 million Face book users was harvested without adequate consent and used to influence political outcomes in the US and the UK[377] . This event exposed the vulnerability of user data and the potential for its exploitative manipulation.

2.3 The Intersect: Data Mining in the Social Media Context

The convergence of social media and data mining has given rise to a new form of "participatory surveillance," where users unwittingly contribute to a data economy that benefits from their actions. This type of surveillance is often presented as a trade-off for free services; however, the imbalance of power between platform owners and users poses significant ethical and legal challenges.

Additionally, the notion of "dataveillance"—ongoing surveillance through data mining—raises important issues regarding informed consent, proportionality, and potential misuse by both corporate and governmental entities. Although the Indian judiciary has acknowledged the right to privacy as a fundamental right in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India[378], it has yet to fully address the extent of dataveillance occurring within the private tech industry.

3. Ethical Issues in Social Media Data Mining

Ethics, in contrast to established laws, focus on the principles that determine right and wrong behavior. When it comes to social media data mining, ethical considerations frequently take

[376] R v Cole [2012] 3 SCR 34 (Supreme Court of Canada).

[377] Cadwalladr C and Graham-Harrison E, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' The Guardian (18 March 2018).

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

precedence over, and can even surpass, legal requirements. The primary ethical dilemma revolves around the use of user-generated data without genuine understanding or consent, which raises significant concerns about fundamental values like autonomy, dignity, and justice.

3.1 Informed Consent: The Great Illusion

Informed consent is fundamental to ethical data collection. Ideally, users agree to data collection by accepting the terms of service (ToS) and privacy policies. However, in reality, these documents are often lengthy, complex, and filled with legal jargon, making them seldom read or understood. A 2019 Deloitte survey revealed that over 90% of users accept legal terms and conditions without actually reading them[379]. This raises a significant ethical concern: can consent truly be considered valid if it is neither fully informed nor freely given?

Moreover, the concept of "notice and choice" presupposes that users have genuine alternatives, which is frequently not the case. Social media has become essential for communication, job opportunities, and political participation, rendering the option to opt out nearly impossible.

3.2 Privacy and Surveillance: The Participatory Panopticon

Drawing on Bentham's panopticon model, the current social media environment resembles a "participatory surveillance" system. In this setup, users willingly share their data, which can then be used to monitor, profile, and influence them. This situation raises ethical concerns when data collected for one purpose, such as social interaction, is repurposed for another, like political advertising. For example, targeted political campaigns that utilize psychological profiling, as seen in the Brexit and US elections, highlight issues of voter manipulation and threaten the integrity of democracy.

India's constitutional right to privacy, as outlined in the Puttaswamy case, recognizes informational privacy as a component of personal liberty. However, without comprehensive data protection legislation to provide statutory support, these ethical standards are only partially upheld.

3.3 Data Ownership and Control: Who Owns 'You'?

From an ethical perspective, user-generated data should be viewed as an extension of an individual's identity. However, many platforms assert broad licenses over this data, often retaining, sharing, and analyzing it even after users delete their accounts. This commodification of personal identity fosters an exploitative data economy. As legal scholar Julie Cohen states, "privacy is not simply an individual right, but a necessary precondition for human flourishing." When platforms treat data as proprietary assets, users lose their status as rights-bearing individuals and are reduced to mere raw material.

The ethical issue of ownership also relates to autonomy and control. In the absence of mechanisms for data portability or deletion—often referred to as the "right to be forgotten"—users remain indefinitely bound to their digital footprints.

3.4Algorithmic Bias and Discrimination: Ethics in Code

Although algorithms are often viewed as neutral, they frequently perpetuate and exacerbate existing societal biases. Research indicates that AI models used for criminal predictions, job recruitment, and credit scoring tend to disproportionately disadvantage minorities, women, and marginalized groups.

Data mining from social media often contributes to these biased systems. For instance, algorithms trained on historical data may identify certain dialects or expressions as signs of radicalism, criminality, or unreliability, effectively creating a form of digital redlining.

[379] Deloitte, Consumer Privacy in Retail Survey: The Next Regulatory and Competitive Frontier, PR Newswire, October 9, 2019. Available at: https://www.prnewswire.com/news-releases/deloitte-consumer-privacy-in-retail-survey-the-next-regulatory-and-competitive-frontier-300931506.html

In India, where caste, religion, and gender already influence access to opportunities, algorithmic bias presents a significant ethical dilemma. In the absence of transparency and accountability, these systems risk reinforcing systemic discrimination while masquerading as efficient solutions.

4. Legal Framework Governing Social Media Data Mining

The regulation of social media data mining intersects with technology law, privacy rights, data protection, and constitutional law. Different legal systems around the world have addressed this issue with varying levels of sophistication and enforcement. Although India has made some forward-thinking judicial rulings, it has yet to establish a comprehensive legal framework. This section explores the domestic legal landscape and offers comparative insights from international regulations such as the GDPR (EU) and CCPA (California, USA).

4.1 The Indian Legal Landscape

4.1.1 Constitutional Right to Privacy

In the significant case of Justice K.S. Puttaswamy (Retd.) v. Union of India[380] , the Supreme Court of India unanimously upheld the right to privacy as a fundamental right under Article 21 of the Constitution. The ruling specifically acknowledged informational privacy, which encompasses the control individuals have over their personal data shared on digital platforms. However, this constitutional recognition has not yet translated into comprehensive statutory protection.

The existing legal framework, primarily based on the outdated Information Technology Act of 2000, lacks the necessary precision, depth, and enforcement capabilities needed in today's data-driven environment.

4.1.2 The Information Technology Act, 2000

The IT Act serves as the cornerstone of digital legislation in India, focusing mainly on cybercrimes and e-commerce. Sections 43A and 72A outline certain responsibilities for corporations regarding the management of sensitive personal data and impose penalties for unauthorized disclosures. However, these provisions are narrow in scope, lack clarity, and do not establish mandatory standards for data minimization, purpose limitation, or algorithmic transparency.

4.1.3 Data Protection Bill(s): The Legislative Limbo

India's data protection laws have been in a state of uncertainty. The Personal Data Protection Bill, 2019, which drew inspiration from the GDPR, was withdrawn in 2022 due to criticism over its bureaucratic tendencies and insufficient safeguards. A revised version, the Digital Personal Data Protection Act, 2023, has been proposed, but it has also received backlash for its extensive government exemptions, limited user empowerment, and weak enforcement mechanisms.

This ongoing legislative uncertainty puts Indian users at risk of unchecked data mining by both private companies and the government[381].

4.1.4 Surveillance and the Role of the State

State-sponsored data mining for law enforcement or national security often escapes public scrutiny. Provisions like Section 69 of the IT Act allow the government to intercept, monitor, and decrypt information in the interest of national security, but without adequate judicial oversight.

The *Pegasus* spyware controversy, where journalists and activists were reportedly targeted, epitomises the risks of unregulated state surveillance[382].

4.2 International Legal Frameworks

4.2.1 European Union: General Data Protection Regulation (GDPR)

The GDPR is widely regarded as the gold standard for data protection legislation.

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

[381] Ministry of Electronics and Information Technology (MeitY), Digital Personal Data Protection Act, 2023.

[382] Reporters Without Borders, *India: NSO Pegasus spyware scandal* (2021).

Enforced since 2018, it sets out robust principles such as:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy and storage limitation
- Accountability

It also grants individuals powerful rights: access, rectification, erasure ("right to be forgotten"), and objection to automated decision-making[383].

Notably, the GDPR has extraterritorial application—meaning Indian platforms handling EU citizen data are also bound by it.

4.2.2 United States: California Consumer Privacy Act (CCPA)

The US lacks a comprehensive federal data protection law. However, the CCPA, effective since 2020, represents a significant step forward. It gives California residents the right to know what personal data is collected, to whom it is sold, and to opt out of such sales.

Unlike the GDPR, the CCPA is more business-centric and less focused on algorithmic accountability, but it still sets a notable precedent for market-based data regulation[384].

4.3 Comparative Reflection and Need for Reform in India

While India's legal journey is still in progress, it can draw valuable lessons:

- From the **GDPR**, India can adopt stronger user rights and impose stricter obligations on data controllers.
- From the **CCPA**, India can explore mechanisms for empowering consumer choices and mandating corporate disclosures.

However, Indian reform must be context-specific—addressing challenges like digital illiteracy, infrastructural gaps, and the high concentration of tech power among a few private players.

5. Judicial Trends and Case Law Analysis

Judicial interpretations provide the necessary scaffolding to understand how the law grapples with evolving technology. Courts across the globe—especially in India, the United States, the European Union, and Canada—have had to balance technological innovation with the protection of individual rights. This section explores pivotal judicial pronouncements that shape the legal narrative on social media data mining.

5.1 India: The Rise of Constitutional Morality in Digital Jurisprudence

5.1.1 *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)

This watershed judgment not only recognised privacy as a fundamental right under Article 21 of the Constitution but also acknowledged *informational privacy* as a distinct category deserving protection[385]. The Court cautioned against the unchecked processing of personal data and called for legislative action—effectively laying the foundation for India's data protection discourse.

Notably, the Court drew upon international legal principles and affirmed that personal data collection must be *proportional*, *necessary*, and backed by *legitimate purpose*.

5.1.2 *Anuradha Bhasin v. Union of India* (2020)

While not directly about data mining, this case involved internet shutdowns in Jammu and Kashmir and reaffirmed that access to the internet is integral to the exercise of fundamental rights[386]. It is relevant insofar as any surveillance or data extraction that limits or manipulates access to information indirectly infringes constitutional guarantees.

[383] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
[384] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq.
[385] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
[386] Anuradha Bhasin v Union of India (2020) 3 SCC 637.

5.1.3 *Internet Freedom Foundation & Ors. v. Union of India* (Pegasus Case, Pending)

The Pegasus spyware case, currently under judicial review, has sparked renewed discussions about state surveillance. The Supreme Court has formed a committee to investigate the alleged invasion of privacy, emphasizing that the right to privacy cannot be dismissed by ambiguous national security claims[387].

These cases show a steady movement in Indian jurisprudence toward recognising and protecting digital rights. However, enforcement remains a concern.

5.2 United States: Sectoral and Precedent-Driven Approach

5.2.1 *Carpenter v. United States* (2018)

The US Supreme Court held that warrantless collection of location data from cell service providers violated the Fourth Amendment[388]. While this ruling focused on geolocation, its logic extends to any mass data collection by state or private actors without judicial oversight.

The judgment underscores that reasonable expectations of privacy persist in digital contexts—an argument highly relevant for social media platforms mining behavioural data.

5.2.2 *United States v. Facebook Inc.* (FTC Consent Decree, 2019)

Following the Cambridge Analytica scandal, Facebook faced a historic $5 billion fine and had to adopt new privacy governance mechanisms[389]. The Federal Trade Commission found that Facebook misled users about how their data was shared with third parties—making this a landmark case in the realm of corporate data accountability.

5.3 European Union: Judicial Endorsement of Strong Privacy Norms

5.3.1 *Google Spain SL v. Agencia Española de Protección de Datos* (2014)

This case established the "right to be forgotten," holding that individuals can request the removal of search engine links containing outdated or irrelevant personal information[390]. The European Court of Justice (ECJ) grounded its decision in the principles of dignity and data protection under the GDPR.

5.3.2 *Schrems II* (Data Protection Commissioner v. Facebook Ireland, 2020)

In this case, the ECJ invalidated the Privacy Shield framework that permitted data transfer between the EU and US, citing inadequate safeguards against US surveillance practices[391]. The judgment affirmed that cross-border data transfers must ensure "essential equivalence" in data protection standards

5.4 Canada: Balancing State Interests and Individual Rights

5.4.1 *R v. Cole* (2012)

The Canadian Supreme Court recognised that employees have a reasonable expectation of privacy in workplace digital devices—even if the devices are owned by the employer[392].

This has implications for data mining policies by platforms and corporations claiming ownership over user environments.

Conclusion of Section

[387] Supreme Court of India, Pegasus Technical Committee Report (interim orders, 2021–2022).

[388] Carpenter v United States 138 S. Ct. 2206 (2018).

[389] Federal Trade Commission, Facebook, Inc., In the Matter of (Case No. 182 3109, 2019).

[390] Google Spain SL v Agencia Española de Protección de Datos (Case C-131/12) [2014] ECLI:EU:C:2014:317.

[391] Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems (Case C-311/18) [2020] ECLI:EU:C:2020:559.

[392] *R v Cole* [2012] 3 SCR 34.

Courts around the world are increasingly acknowledging the complex implications of social media data mining. Indian courts have established a solid constitutional framework but still lack comprehensive statutory support. In contrast, EU courts have developed a strong set of rights supported by robust legislation, while US courts are advancing gradually within a fragmented legal system. Collectively, these judicial trends provide both guidance and caution for the future of data governance in India.

6. Regulatory Gaps and Challenges

While global and national legal frameworks have made progress in addressing social media data mining, several challenges persist. These gaps are not only legal and regulatory but also infrastructural, philosophical, and socio-political. In India, the need for robust, enforceable, and technologically adaptive regulation is especially urgent given the country's massive social media user base and its digital policy ambitions.

6.1 Absence of a Comprehensive Data Protection Law

Despite the *Puttaswamy* judgment's call for a statutory framework, India still lacks a GDPR-level data protection law. The **Digital Personal Data Protection Act, 2023**—though a step forward—is riddled with issues:

- Excessive exemptions for the state under the pretext of national security;
- Limited scope for user redressal;
- Absence of data fiduciary obligations like algorithmic accountability and data portability[393];

Lack of an independent and empowered Data Protection Authority.

Without strong legislative teeth, the right to informational privacy remains a paper tiger.

6.2 Weak Enforcement and Oversight Mechanisms

Even existing obligations under the Information Technology Act, 2000 (such as Section 43A) are weakly enforced. There are no regular audits, compliance checks, or meaningful penalties for breaches. The government's dual role as a regulator and a surveillance actor further erodes trust in enforcement.

By contrast, the European Data Protection Board under the GDPR has the power to issue massive fines (up to 4% of annual global turnover), suspend data flows, and compel compliance—creating actual deterrence[394].

6.3 Algorithmic Opacity and Lack of Explainability

Algorithms used by platforms for data mining and targeted advertising are often "black boxes." Users don't know:

- How their data is used;
- What inferences are being drawn;
- What consequences those inferences might have (credit scoring, political profiling, etc.).

India's legal framework lacks any obligation for algorithmic transparency or fairness testing. This is especially problematic in a country with high levels of digital illiteracy and limited tech access.

6.4 Consent Fatigue and Tokenism

The consent model currently relied upon—both globally and in India—is broken. Users routinely click "I Agree" without understanding the implications. There's little to no granularity in how consent is obtained, and often no option to refuse without foregoing the service entirely.

Moreover, consent does not equal ethical treatment. Just because a user "agreed" to being tracked across platforms doesn't make it morally sound or legally just. As Shoshana

[393] Digital Personal Data Protection Act, 2023, Ministry of Electronics and IT (MeitY), Government of India. ⏎

[394] European Data Protection Board (EDPB), Annual Report 2022.

Zuboff puts it, "Consent in surveillance capitalism is always coerced[395]"

6.5 State Surveillance and Lack of Judicial Oversight

Government data mining remains a major blind spot in regulatory conversations. India's laws, including the IT Act and Telegraph Act, allow interception and monitoring of communications with minimal transparency or judicial review.

In a digital society, where states are among the largest data gatherers, lack of oversight mechanisms (like judicial warrants or parliamentary committees) risks creating an Orwellian reality. Recent incidents such as the Pegasus spyware allegations make this risk alarmingly real[396].

6.6 Cross-Border Data Flows and Jurisdictional Challenges

Social media platforms often store and process data outside India. This raises issues like:

- Lack of jurisdiction for Indian regulators;
- Inaccessibility of user redressal;
- Risks from foreign surveillance (as highlighted in *Schrems II*).

India has flirted with data localisation in draft policies, but critics argue that localisation alone doesn't guarantee better privacy—it must be coupled with strong data governance practices.

6.7 Digital Inequality and Inclusion Deficit

Lastly, any regulatory framework must account for the socio-economic disparities in India. Rural users, first-time internet users, and marginalised communities are especially vulnerable to manipulation and exploitation through opaque data practices.

Without a rights-based, inclusion-sensitive regulatory approach, any legal reform risks privileging urban, English-speaking elites while leaving the majority digitally disenfranchised.

Conclusion of Section

India's regulatory architecture currently resembles a ship held together by duct tape and hope. Without substantial reform in statutory law, regulatory enforcement, and judicial oversight, social media data mining will continue to thrive in a legal vacuum—leaving citizens algorithmically profiled, emotionally manipulated, and digitally naked.

7. Policy Recommendations and the Way Forward

A robust, forward-looking legal framework for regulating social media data mining in India must be informed by constitutional morality, technological realism, and democratic values. This section offers a blueprint for reform—combining legal, regulatory, institutional, and technological recommendations that can usher in a rights-based digital future.

7.1 Enact a Comprehensive and Independent Data Protection Law

India must finally deliver on the promise made in the *Puttaswamy* judgment by enacting a **comprehensive data protection statute** that:

- Clearly defines **personal**, **sensitive**, and **anonymised** data;
- Recognises **data fiduciary obligations** such as data minimisation, purpose limitation, and algorithmic transparency;
- Establishes a **truly independent** Data Protection Authority (DPA) insulated from executive overreach;
- Provides for **meaningful penalties**, class action rights, and whistleblower protections.

The current Digital Personal Data Protection Act, 2023 needs urgent amendment to remove the broad exemptions given to the State and to introduce transparency mandates akin to the EU's GDPR[397].

[395] Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs 2019).

[396] Reporters Without Borders, India and the Pegasus Scandal (2021).

[397] Justice B.N. Srikrishna Committee Report on Data Protection, 2018.

7.2 Create Judicially Monitored Surveillance Guidelines

Inspired by the UK's **Investigatory Powers Act** and the US's **Foreign Intelligence Surveillance Act**, India needs a **judicial warrant-based system** for surveillance authorisations. This should include:

- Pre-surveillance approval by a designated judicial body;
- Annual public disclosures of the number and nature of interceptions;
- Parliamentary oversight committees to evaluate State surveillance programs.

This is vital in light of the Pegasus spyware controversy and general lack of clarity around who monitors the monitors[398].

7.3 Mandate Algorithmic Accountability and Audits

Platforms should be statutorily required to:

- Conduct **impact assessments** of their data processing algorithms;
- Provide **explainability** of automated decisions to users;
- Allow third-party **independent audits** of algorithmic fairness and data ethics.

This is especially urgent as AI-driven recommendation systems can reinforce echo chambers, biases, and political manipulation.

7.4 Introduce Granular, Informed Consent Mechanisms

India needs to move beyond the "I Agree" model to a **contextual consent framework**, which includes:

- Layered disclosures written in plain language;
- Opt-in systems for third-party sharing;
- Fine-grained control over specific data categories (e.g., location, browsing behaviour);
- Clear "right to object" options, especially for targeted ads.

Borrowing from GDPR and user-centric UX design, these reforms will restore user agency[399].

7.5 Promote Digital Literacy and Ethical Tech Education

Policy reforms must be accompanied by a **national digital literacy campaign**—especially focused on:

- High-risk groups (rural users, first-time internet users);
- School and university curriculums that integrate **data ethics**, **cyber law**, and **critical digital thinking**;
- Government-led public awareness programs around consent, privacy, and safe browsing.

Empowered users are the first line of defence against unethical data mining.

7.6 Enable Cross-Border Data Protection Agreements

India should enter into **data protection adequacy agreements** with countries that meet minimum human rights benchmarks. This will:

- Facilitate secure cross-border data transfers;
- Build diplomatic trust in the global digital economy;
- Harmonise India's regime with international best practices.

This approach is consistent with *Schrems II*, which emphasised the need for "essential equivalence" in privacy protections for data transfers[400].

7.7 Encourage Privacy-by-Design in Tech Architecture

[398] Supreme Court of India, Pegasus Committee Interim Report, 2022.

[399] Solove, Daniel J., Understanding Privacy (Harvard University Press, 2008).

[400] Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems (2020) CJEU Case C-311/18.

India must integrate **Privacy-by-Design** principles into platform development. The law should incentivise companies to:

- Use encryption by default;
- Collect only the minimum data needed (data minimisation);
- Provide built-in opt-out mechanisms;
- Adopt federated and decentralised data storage where possible.

This design philosophy treats privacy not as an afterthought but as an engineering imperative.

7.8 Foster a Human Rights-Centric Regulatory Ecosystem

Ultimately, all legal and policy reforms must be anchored in a **human rights framework**. That includes:

- Recognising privacy, data autonomy, and freedom from manipulation as **non-negotiable rights**;
- Ensuring that marginalised communities are protected from discriminatory data profiling;
- Framing data protection as **digital dignity**, not just a compliance burden.

In this regard, India must shift from being a digital colony of Big Tech to a **data-sovereign, rights-respecting democracy**.

Conclusion of Section

India stands at a crossroads. It can either drift further into a surveillance economy dominated by opaque algorithms and unaccountable platforms—or it can reclaim its digital sovereignty by enshrining data rights into law, culture, and code. The recommendations above offer a constitutional, technologically nuanced, and globally informed path forward.

8. Conclusion

The rapid growth of social media platforms has fundamentally changed society, connecting people across the globe, fostering grassroots activism, and altering political discussions in unprecedented ways. However, this remarkable connectivity has come with significant drawbacks: the commercialization of personal data, a decline in informational privacy, and the emergence of unseen algorithmic governance.

This paper aims to critically analyze the ethical and legal ramifications of social media data mining, particularly within the Indian context, while also considering global legal trends. By examining ethical challenges, international legal frameworks, Indian constitutional law, judicial precedents, and regulatory shortcomings, it is clear that the existing regulatory framework is severely lacking in addressing the complex issues associated with data mining.

While international developments like the GDPR, Schrems II, and Carpenter have advanced the understanding of digital rights, India's legal response remains disjointed and inconsistent. The Puttaswamy judgment provided a strong constitutional foundation, but legislative and executive inaction has undermined its potential. The Digital Personal Data Protection Act, 2023, while a step forward, does not establish a comprehensive and rights-based regulatory environment. Meanwhile, social media platforms continue to collect user data extensively, often without adequate consent or transparency, while the State's role fluctuates between that of a regulator, enabler, and violator.

To progress, India needs to adopt a comprehensive, human-centered data governance model. This model should view privacy not as a luxury but as a constitutional right, and not as an obstacle to innovation, but as a cornerstone of trustworthy innovation. Ethical principles should guide legal frameworks, which must then ensure ethical behavior through enforceable rights and meaningful accountability.

In the 21st century, the digital economy will be shaped not only by technology but also by values. India has the chance to emerge as a global leader—not just in technology adoption, but also in technology regulation, grounded in constitutional morality, democratic oversight, and digital dignity. This is not merely a legal requirement; it is a fundamental civilizational necessity.