



## MSB-International Journal of Interdisciplinary Research

Associating Researchers; Nourishing Innovation

Peer Reviewed

Vol. 3, Issue 1, March 2025-June 2025

28-40, MSB-IJIR

# Consent and Control: Unpacking the Constitutional Dangers of Data Harvesting

Shambhavi Srivastava<sup>1</sup>  
Dr. Taru Mishra<sup>2</sup>

<sup>1</sup>LL.M, Amity Law School

<sup>2</sup>Assistant Professor, Amity Law School,  
Amity University, Lucknow, Uttar Pradesh

## Abstract

*Data has become a valuable resource in the age of digital capitalism and algorithmic governance, driving surveillance systems, business innovation, and governance effectiveness. However, there are serious constitutional issues with this monetisation of personal data. With a focus on the degradation of fundamental rights like privacy, dignity, and autonomy, this research paper examines the constitutional ramifications of data collecting in India. The paper outlines privacy as a tripartite notion, including informational privacy, bodily integrity, and decisional autonomy, and criticises how digital infrastructures frequently transgress these values, drawing on the seminal Justice K.S. Puttaswamy v. Union of India ruling. The architecture and methods of data harvesting, including cookies, tracking technologies, algorithmic profiling, and data broking networks, are first defined in the study. After that, a constitutional analysis is presented, showing how permission in digital settings is frequently forced or fictitious, resulting in legal fictions that fall short of the requirements for "free and informed consent." It also emphasises how algorithmic systems negatively affect Articles 14 (equality), 19 (freedom of expression), and 15 (non-discrimination). The study highlights both improvements and shortcomings in India's regulatory environment, notably in areas like algorithmic transparency, state exemptions, and institutional accountability, by carefully analysing the country's laws, including the IT Act of 2000 and the Digital Personal Data Protection Act of 2023. Global insights can be gained by comparing the GDPR (EU), CCPA (USA), and laws in Brazil and South Korea. The real-world risks are further contextualised by case studies like the Pegasus malware, WhatsApp's privacy policy dispute, the Aadhaar lawsuit, and the Cambridge Analytica scandal. The study ends by suggesting structural and legislative changes that are grounded in constitutional morality. These changes include the institutionalisation of privacy literacy, the creation of a strong Data Protection Authority, and the acknowledgement of algorithmic rights. A legislative framework based on democratic accountability and constitutional principles is necessary to protect human dignity in India's digital future.*

**Keywords:** *Data Harvesting, Privacy Rights, Indian Constitution, Consent Mechanisms, Algorithmic Profiling, Digital Surveillance, Fundamental Rights, Autonomy, Data Protection Law,*

## **Introduction**

In today's hyper-connected digital environment, personal data has emerged as a powerful economic and political resource. Popularly described as the "new oil," data fuels the business models of technology giants, informs governmental policy, and drives innovations in artificial intelligence and behavioural analytics. However, this shift towards a data-driven economy has also revealed the darker side of technological advancement—one where individuals are persistently monitored, profiled, and targeted, often without their knowledge or consent.

At the centre of this ecosystem lies the practice of data harvesting, the large-scale collection and processing of user data through tools such as cookies, tracking software, mobile permissions, and AI-powered algorithms. While these mechanisms offer personalization and efficiency, they also expose users to manipulation, surveillance, and discrimination. The opaque nature of data collection practices, the imbalance of power between users and platforms, and the transformation of human experience into digital capital raise profound legal, ethical, and constitutional questions.

India, the world's largest democracy and rapidly digitizing economy, is at a pivotal moment. In 2017, the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognized the right to privacy as a fundamental right under Article 21 of the Constitution. This landmark judgment emphasized the values of dignity, autonomy, and informational self-determination. Yet, despite this judicial affirmation, the practical enforcement of privacy remains elusive. Users continue to face coercive consent mechanisms, algorithmic opacity, and increasing instances of both corporate and state surveillance.

This research paper seeks to examine the constitutional implications of data harvesting in India. It evaluates the adequacy of the current legal framework—especially the Information Technology Act, 2000, and the recently enacted Digital Personal Data Protection Act, 2023—in protecting fundamental rights. The paper further explores ethical concerns around profiling, consent engineering, and surveillance capitalism, drawing on comparative insights from global regimes such as the EU's GDPR, Brazil's LGPD, and South Korea's PIPA.

Through doctrinal analysis, case studies, and comparative evaluation, the paper argues that India's digital governance must evolve to reflect not only technological efficiency but also constitutional morality. True digital empowerment can only be achieved when consent is meaningful, control is real, and data practices uphold the foundational values of a democratic society.

## **1. The Architecture of Data Harvesting**

### **1.1 Definition and Mechanism**

The term "data harvesting" describes the methodical collection and handling of enormous amounts of personal information from people, frequently without their knowledge or informed consent. The data economy is based on this process, which is now the foundation of behavioural profiling, targeted advertising, and algorithmic decision-making. Data harvesting takes advantage of digital traces, such as clicks, scrolling, likes, GPS movements, and even biometric identifiers, in contrast to traditional data collection, which involves people actively providing information. The asymmetry of power is the

root cause of the problem: users are still ignorant of the amount, type, and subsequent applications of the data that is gathered.

Predictive analytics, machine learning, and artificial intelligence (AI) are now essential components of data harvesting architectures. In addition to analysing personal data, these systems also deduce other attributes like psychological qualities, political preferences, and sexual orientation. The procedure turns unprocessed personal data into behavioural excess, a product that internet corporations sell.

## **1.2 Tools and Techniques**

### **Cookies and Third-Party Trackers:**

These tiny bits of code that are integrated into websites monitor consumers' internet activity on several websites. Third-party cookies, which are set by advertisers and data brokers, generate lasting digital profiles without the user's knowledge, even though some cookies are functional.

### **SDKs and Mobile App Permissions:**

Mobile apps frequently come with Software Development Kits (SDKs), which gather private data such as contact lists, phone logs, location information, and usage patterns. Bypassing informed consent, these rights are typically given during installation using vague and generalised language.

### **Real-Time Bidding Systems:**

Advertisers can place millisecond bids on user impressions thanks to this method. Although it makes personalised advertising possible, it also instantly shares user information with hundreds of unidentified parties, including location, device ID, and browsing history, which raises significant privacy and cybersecurity issues.

### **Data Broker Networks:**

To create thorough user profiles, data brokers compile information from a variety of sources, including social media, commercial databases, and public records. The distinction between state and private surveillance is further blurred when these profiles are sold to political strategists, corporations, and even government organisations.

## **1.3 Business Models in Algorithmic Marketplaces**

Platform capitalism is the new economic logic at the core of data gathering. Although the services provided by tech behemoths like Google, Amazon, and Facebook are ostensibly free, customers actually pay for them with their data. Algorithmic profiling and behavioural targeting are instruments of control as well as persuasion. For example, recommendation engines make predictions about what users will consume, think, or support based on data that has been acquired. According to philosopher Shoshana Zuboff, people are now "raw material" for predictive goods rather than clients. Autonomy becomes a negotiable asset when attention and behaviour become commodities.

Algorithmic markets prioritise profit and participation over the welfare of the individual. The personalisation loop, which is based on data that has been acquired, has negative effects on democracy, variety of opinion, and mental health since it limits exposure, strengthens prejudices, and produces echo chambers.

#### **1.4 Scale and Opacity**

The sheer size of contemporary data harvesting is one of its distinguishing characteristics. Every month, the typical smartphone user engages with more than 80 apps, the majority of which use third-party SDKs. Data flows across numerous servers, jurisdictions, and actors can be initiated with a single click. There is a significant lack of openness in this complex ecology.

Seldom are users given clear information about what data is being gathered, by whom, and why. Consent becomes an illusion as a result of this informational imbalance. Long privacy rules, pre-checked boxes, and click-wrap agreements are meant to provide legal protection rather than transparency.

The algorithms themselves are equally opaque. Users—or regulators—can hardly check judgements based on gathered data thanks to proprietary black-box technologies. Both accountability and trust are undermined by this invisibility.

The ramifications extend beyond personal privacy. Scaling and systematising data collection turns it into a tool for power. It can be used to discriminatorily divide communities, track dissent, or influence election results. As a result, the design is profoundly political in addition to being technological.

## **2. Constitutional Safeguards and Challenges**

The emergence of data harvesting methods in India necessitates careful examination from the perspective of constitutional law. Personal data in the digital ecosystem is more than just information; it is a representation of a person's identity, independence, and self-respect. Even though the Indian Constitution was not created with a digital world in mind, the courts have interpreted it broadly to uphold these core principles, particularly in the wake of the historic Justice *K.S. Puttaswamy (Retd.) v. Union of India (2017)*<sup>1</sup> ruling that acknowledged the right to privacy as a fundamental right under Article 21.

In *Puttaswamy*, the Court underlined that privacy has three fundamental components: decisional autonomy, bodily integrity, and informational privacy. In the context of data harvesting, when users' digital footprints are collected, profiled, and made profitable—often without explicit agreement or control—informational privacy becomes more crucial. When people are unaware of how their data is gathered, processed, or shared, it seriously undermines the concept of autonomy, which is the moral foundation of Article 21. As a result, the system functions in opposition to the liberty, dignity, and self-determination guaranteed by the constitution.

According to constitutional doctrine, consent ought to be "free, informed, and meaningful." But in the data economy, consent is frequently acquired via coercion or manipulation—a practice known as "consent fatigue." The user's agency is compromised by click-wrap agreements, ambiguous privacy policies, and opt-in defaults. As a result, permission becomes a legal fiction and is no longer a substantive protection but rather a procedural checkbox. The loss of genuine consent in a democracy is a constitutional issue, not a technical one.

---

<sup>1</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

Furthermore, the threat to personal dignity is increased by the employment of automated decision-making systems and algorithmic profiling. People are becoming more and more like behavioural datasets that are analysed, grouped, and targeted according to their prior behaviour. People are seen as passive objects rather than active beings with rights, which reduces human agency. An essential component of the right to privacy is decisional autonomy, which is violated when behaviour is manipulated through algorithmic nudging or content selection. The core constitutional architecture, which envisions equal respect and autonomy for every individual, is distorted by the power imbalance between data collectors and data subjects.

Data harvesting poses risks that go beyond **Article 21**. They extend to other constitutionally guaranteed fundamental rights. Algorithmic bias, for example, compromises Article 14, which ensures equality before the law and protection from capricious state action. AI programs that have been trained on skewed data sets have the potential to reinforce discrimination in hiring, loan approval, and law enforcement monitoring. These biases violate procedural and substantive equality by causing unfair treatment that is opaque and unassailable.

Data analytics is also linked to **Article 15**,<sup>2</sup> which forbids discrimination based on factors including religion, ethnicity, caste, sex, or place of birth. Algorithms that directly or indirectly classify users according to sensitive characteristics run the risk of perpetuating social stratification and denying underprivileged groups access to social or economic opportunities. Such discrimination can have significant repercussions, even if it is unintended or indirect, leading to the emergence of new types of inequality in the digital realm.

**Article 19(1)(a)**, which protects the right to freedom of speech and expression, is under strain due to the chilling effect created by pervasive surveillance and targeted content moderation. If users believe that their digital behavior is being monitored or recorded, they may self-censor, thus diluting the vibrancy of democratic discourse. Moreover, algorithmic amplification of misinformation or polarizing content further distorts the information ecosystem, making informed civic participation increasingly difficult.

Thus, it becomes crucial to consider how cyber governance and constitutional democracy interact. The data-driven digital economy runs the risk of normalising a system of covert monitoring and behavioural control in the absence of strong constitutional protections. This is especially risky when the government itself collects data or collaborates with private organisations for predictive governance, welfare, or law enforcement. In these situations, the need for accountability and transparency under the constitution must take precedence over administrative effectiveness alone.

To guarantee that the benefits of the digital age do not come at the expense of human rights, India's legal and constitutional framework must be fundamentally reevaluated. To uphold the constitutional ideals of equality, liberty, and dignity, judicial rulings, legislative changes, and institutional supervision must be coordinated.

### **3. India's Regulatory Landscape**

India's data protection laws have developed gradually and frequently in reaction to emergencies rather than proactively. The current regulations have not been able to keep up with the complicated reality of data gathering due to the exponential rise of digital platforms. This chapter compares the visionary but

---

<sup>2</sup> Constitution of India arts. 14, 15, 19, 21.

only partially implemented recommendations of the Justice B.N. Srikrishna Committee Report<sup>3</sup> with the current legislative instruments, particularly the Digital Personal Data Protection Act, 2023 (DPDPA)<sup>4</sup> and the Information Technology Act, 2000 (IT Act).

### 3.1 The Information Technology Act, 2000: A Legacy Framework

The IT Act<sup>5</sup> was never designed to handle the complexities of artificial intelligence, algorithmic profiling, or behavioural data collection; it was first passed to address cybercrimes and internet commerce. Only "body corporates" are covered by the basic Section 43A, which offers compensation in the event that sensitive personal data is handled carelessly. There are significant interpretation gaps when terminology like "personal data," "data processor," and "consent" are not defined. Furthermore, the Act's regulations, especially the 2011 SPDI Rules<sup>6</sup>, are unclear, unenforceable, and out of step with international best practices.

Notably, in an age of real-time data flows and predictive analytics, the IT Act is woefully insufficient since it ignores algorithmic opacity, cross-border data transfers, and state monitoring. Its ability to protect constitutional principles like autonomy, privacy, and dignity is constrained by its punitive rather than rights-based approach.

### 3.2 The Digital Personal Data Protection Act, 2023: A Mixed Step Forward

India's most extensive attempt to control personal data in a methodical and rights-based way is the DPDPA, 2023. Important terms like "data fiduciaries" and "data principals" are introduced, creating the idea that organisations that gather data hold it in trust for the people from whom it originates.

#### Strengths of the DPDPA include:

- **Consent-centric framework:** In addition to being "free, specific, informed, and unambiguous," consent must be restricted to the reason it is being taken.
- **Grievance redressal:** The law mandates clear grievance mechanisms, enhancing accountability.
- **Guardrails for children's data:** Special protections for minors and their data are included.

However, the Act has several **significant limitations** that dilute its protective potential:

- **Broad exemptions for the State:** For reasons like sovereignty, public order, or national security, the government may exempt any agency from compliance under Section 17. These exclusions have the potential to be abused since they are broad, ambiguous, and mostly unreviewable.
- **Lack of algorithmic transparency:** The law does not provide people a "**right to explanation**" about algorithmic profiling or compel businesses to reveal how automated systems make choices.
- **Absence of a strong independent authority:** While the Data Protection Board is created under the Act, its powers are limited, and it lacks the kind of institutional autonomy and oversight capacity necessary for regulating tech giants or powerful government entities.

---

<sup>3</sup> Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy*, MeitY (2018).

<sup>4</sup> Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

<sup>5</sup> Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).

<sup>6</sup> Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, Apr. 11, 2011 (India).

- **No mention of data localization mandates or impact assessments**, thereby weakening the infrastructure for secure data storage and processing.

### **3.3 Justice B.N. Srikrishna Committee: The Lost Opportunity**

In 2018, the Justice B.N. Srikrishna Committee released a draft Personal Data Protection Bill, proposing a comprehensive framework rooted in the constitutional principles of dignity, autonomy, and purpose limitation. The Committee underscored the need for:

- The implementation of data minimisation and purpose limitation principles;
- A robust, independent Data Protection Authority (DPA) with investigative and quasi-judicial authority.
- a right to be forgotten, which gives people back authority over their online selves.

Data localisation to protect jurisdictional integrity and prohibit abuse by foreign players; openness in algorithmic decision-making, including the right to an explanation; and transparency. Although early bill drafts included many of these suggestions, the final DPDPA, 2023, removed numerous essential protections from the framework. As a result, there is a law that talks about privacy but does not yet fully understand its meaning.

## **4. Way Forward**

Despite improvements in form brought about by the DPDPA, India's regulatory environment is still lacking in substance. Legal improvements run the risk of becoming performative in the absence of strong enforcement, impartial oversight, and constitutional conformity. India has to incorporate constitutional morality, judicial accountability, and public involvement into its legislation in order to effectively guard against the risks associated with data collection.

## **Chapter 4: Comparative Global Perspectives**

India may gain a lot from studying the strategies used by other jurisdictions, even though it is still developing a strong legislative framework to control data gathering. In addition to highlighting excellent practices, comparative analysis highlights the distinct constitutional and democratic issues that each system aims to address. This chapter looks at the regulatory strategies of the US, Brazil, South Korea, and the EU, each of which has a distinct data protection philosophy and enforcement framework.

### **4.1 European Union: The Gold Standard – General Data Protection Regulation (GDPR)**

The most extensive and rights-based data protection system in the world is generally acknowledged to be the General Data Protection Regulation (GDPR) of the European Union, which went into effect in 2018. Fundamentally, the GDPR is based on the concepts of accountability, transparency, and individual liberty—values that are consistent with India's constitutional values.

Consent must be freely granted, specific, informed, and unambiguous, according to the GDPR's express consent requirements. It gives people the "right to be forgotten," the right to data portability, and the right to correction, all of which improve informational self-determination and user control. The GDPR's requirement for Data Protection Impact Assessments (DPIAs) is among its most inventive features, particularly for operations requiring high-risk data processing. These evaluations guarantee that privacy issues are considered during the design phase, which is consistent with the "privacy by design" concept.

Additionally, algorithmic openness is required under the GDPR. Unless express consent is acquired or required for contractual performance, people have the right under Article 22 to not be subject to

decisions that are made only on the basis of automated processing, including profiling. In order to stop discrimination online, this is essential.

Strong supervisory authorities in each member state enforce the rule, and infractions can result in fines of up to €20 million, or 4% of a company's worldwide revenue. This serves as a potent disincentive against non-compliance.

#### **4.2 United States: Fragmented and Sectoral Regulation**

There isn't a single comprehensive data protection law in the US. Rather, it uses a hodgepodge of federal and state rules and takes a sector-specific approach. The Health Insurance Portability and Accountability Act (HIPAA), which governs health data, is one important statute.

The California Consumer Privacy Act (CCPA)<sup>7</sup> and California Privacy Rights Act (CPRA), which expand GDPR-style safeguards within the state of California; the Children's Online Privacy Protection Act (COPPA) for data pertaining to children under the age of 13; and the Gramm-Leach-Bliley Act for financial information. Rights including access, deletion, and opt-out of the selling of personal data are granted under the CCPA/CPRA framework. Nevertheless, the GDPR's unified enforcement mechanism and constitutional depth are absent from these regulations. Furthermore, there is no federal data protection authority, which results in uneven enforcement and inadequate supervision. The U.S. Constitution's lack of a basic right to privacy, other from what is inferred by judicial interpretation, is another important restriction. As a result, market incentives, rather than rights-based obligations, dominate corporate data practices.

#### **4.3 Brazil and South Korea: Emerging Global Leaders**

In 2020, Brazil implemented the **Lei Geral de Proteção de Dados** <sup>8</sup>(LGPD), which was heavily influenced by the GDPR. It lays down solid guidelines including responsibility, data minimisation, and purpose limitation. It gives data subjects access, correction, erasure, and processing information rights. Enforcement is supervised by the National Data Protection Authority (ANPD), an autonomous organisation.

Crucially, LGPD ensures checks on governmental monitoring by applying to both public and private entities. The Brazilian Constitution provides a solid basis for future legal interpretation by acknowledging the right to privacy as a basic right.

In contrast, South Korea boasts one of Asia's most stringent data privacy regulations. Its **Personal Information Protection Act (PIPA)**<sup>9</sup> demands that sensitive personal data be handled with exceptional care and that data controllers have prior consent before collecting personal data. The Personal Information Protection Commission, which operates with significant autonomy and authority, is responsible for enforcing the law. Both South Korea and Brazil serve as examples of how important it is to have robust, independent regulatory bodies supported by constitutional protections in order to provide effective data protection in democracies.

#### **Takeaways for India**

India may learn the value of algorithmic accountability, rights-based framing, and robust enforcement measures from the EU. The United States can identify the risks of letting market forces regulate data

---

<sup>7</sup> California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2022).

<sup>8</sup> Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.08.2018 (Braz.) (General Data Protection Law).

<sup>9</sup> Personal Information Protection Act (S. Kor.).

and the shortcomings of disjointed sectoral legislation. Models of comprehensive, legally based, and enforced frameworks that combine civil liberties and regulatory foresight can be found in South Korea and Brazil. Finding a balance between promoting digital innovation and defending constitutional principles is India's dilemma. In order to accomplish this, it must absorb the democratic principles and institutional frameworks that give those frameworks their efficacy rather than just copy regulation texts from other countries.

## **5. Ethical Concerns and Human Rights**

The emergence of data harvesting has profound ethical and human rights ramifications in addition to legal and constitutional aspects. Fundamentally, data collection has an impact on people's self-perception, interactions with digital systems, and ability to manage their personal space. This chapter discusses the moral conundrums and human rights issues brought about by data-driven technologies, particularly as they relate to algorithmic prejudice, psychological manipulation, surveillance capitalism, and consent engineering.

### **5.1 Dark Patterns and Consent Engineering**

Dark patterns are dishonest design techniques frequently used in contemporary digital interfaces to influence users to make choices that benefit businesses rather than individuals. These include strategies like delayed "opt-out" alternatives, deceptive button placements, default opt-ins, and unclear privacy settings. Consent is often obtained through deceptive or coercive means, making it unethical even though it is stated as a legal need.

The loss of user autonomy is the moral dilemma here. A fundamental component of human dignity and informational self-determination, the principle of voluntary agreement is violated when consent is obtained by manipulation. These strategies amount to digital exploitation, particularly when directed at vulnerable groups like children or the elderly.

### **5.2 Discrimination and Profiling**

Biassed datasets are frequently used to train algorithmic decision-making systems, which mostly rely on data that has been gathered. This results in algorithmic discrimination, where past injustices are reflected and sustained in hiring, lending, policing, and educational outcomes. When automated algorithms reject chances for marginalised communities based on presumptions, they make them particularly vulnerable to digital exclusion<sup>10</sup>.

In terms of equity, justice, and fairness, this presents significant ethical and human rights issues. People are further deprived of the chance to challenge or even comprehend decisions that impact their life due to the opaqueness of these procedures.

### **5.3 Surveillance Capitalism**

The term "**surveillance capitalism**," coined by researcher Shoshana Zuboff, describes how behavioural data is extracted and turned into prediction products, thereby commodifying the human

---

<sup>10</sup> Sandra Wachter, Brent Mittelstadt & Chris Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, 41 *Comput. L. & Sec. Rev.* 105567 (2021).

experience. This methodology not only observes user behaviour but also gently modifies it to provide favourable results for businesses.

The distinction between psychological manipulation and financial gain is blurred by this approach. Without their knowledge, people are prodded, nudged, and swayed, which goes against the moral precepts of mental sovereignty and informed choice. This eventually leads to a digital world where participation and financial gain are valued more highly than personal liberty and democratic discussion.

#### **5.4 Mental Health and Manipulation**

Increased anxiety, despair, and other mental health problems—especially among teenagers—have been connected to algorithmic content curation, notably on social media platforms. In order to maintain user engagement, recommendation algorithms frequently boost information that is divisive or emotionally charged.

Users become trapped in feedback loops that take advantage of psychological weaknesses as a result, creating an attention economy. This ethical transgression is wilfully developing systems that put addiction ahead of health, frequently with no controls or safeguards in place. Furthermore, through imperceptible measures of popularity and engagement, these systems have a disproportionately negative impact on young people's brains, influencing their perceptions of their bodies, their sense of self, and their worldview.

#### **6: Case Studies<sup>11</sup>**

To fully grasp the implications of data harvesting and its intersection with constitutional and ethical concerns, real-world case studies offer valuable insight. These examples illustrate how platforms, private corporations, and governments have navigated (or failed to navigate) the thin line between innovation and intrusion. The following four cases—Cambridge Analytica, Aadhaar, WhatsApp's Privacy Policy, and the Pegasus spyware incident—highlight key constitutional, legal, and ethical lessons.

##### **6.1 Cambridge Analytica and the Manipulation of Democracy**

The Cambridge Analytica scandal, which exposed how the personal information of more than 87 million Facebook users was collected without their consent and used to sway political behaviour, is arguably the most notorious case of data exploitation in history. Large amounts of user data, such as buddy networks, likes, and behaviour patterns, were retrieved through ostensibly harmless personality tests and app permissions.

Later, the information was used to micro target political ads, influencing election results such as the Brexit referendum and the 2016 U.S. presidential election. This example demonstrated how democratic principles like free will, informed decision, and deliberative involvement can be compromised by covert algorithmic manipulation.

The controversy highlights how data collecting can have a chilling impact on free expression from a constitutional perspective (Article 19 of the Indian Constitution).

---

<sup>11</sup> Karmanya Singh Sareen & Anr. v. Union of India & Ors., W.P. (C) No. 7663 of 2016 (Delhi High Ct. Aug. 25, 2016) (India).

## 6.2 Aadhaar and the Question of Surveillance

The original goal of India's biometric identification system, Aadhaar, was to provide equitable access to government assistance programs. But issues with its scope, required service connection, and monitoring potential started to surface.

The Supreme Court upheld the right to privacy as a basic right in Justice *K.S. Puttaswamy (Retd.) v. Union of India (2017)*<sup>12</sup>, placing special emphasis on physical autonomy and informational privacy. The Aadhaar plan was later confirmed by the Court in *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India (2018)*, but with several restrictions: Aadhaar could not be made required for services like banking and telecom.

There have continued to be cases of governmental overreach in spite of these restrictions. Bank accounts, school admissions, and mobile SIMs have all been connected to Aadhaar data. Furthermore, there are serious worries about state monitoring and the loss of personal control due to the lack of algorithmic transparency in the data processing and storage.

The Aadhaar case highlights the need for strict constitutional review of state-led data collecting and serves as an example of the tension between technical efficiency and constitutional morality.

## 6.3 WhatsApp Privacy Policy and Consent Without Choice<sup>13</sup>

WhatsApp's privacy policy was updated in 2021, and users had to agree to share metadata with parent firm Facebook (now Meta) or risk having their access to the app revoked. A legal challenge was filed in the Delhi High Court as a result of the public outcry.

The petitioners contended that the policy was incompatible with Puttaswamy's requirements for free and informed consent and infringed upon users' rights to informational self-determination. Despite WhatsApp's assertion that end-to-end encryption was still in place, detractors pointed out that non-content data, such transaction information, device IDs, and conversation frequency, could still be made money off of and combined for behavioural profiling.

## 6.4 Pegasus Spyware: State Surveillance and the Death of Anonymity<sup>14</sup>

The use of Pegasus malware, created by Israeli cyber-intelligence outfit NSO Group, is arguably the most unsettling case in India's digital landscape. Journalists, human rights advocates, opposition politicians, and attorneys in India were identified as possible or verified Pegasus monitoring targets in 2021.

Pegasus, in contrast to conventional malware, permits zero-click device infection, giving access to encrypted platforms, microphones, cameras, messages, and conversations. The fact that this

---

<sup>12</sup> Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2018) 1 S.C.C. 809 (India).

<sup>13</sup> Facebook–Cambridge Analytica Data Misuse: Questions for the Future, U.K. Parl., House of Commons (2018).

<sup>14</sup> Manohar Lal Sharma v. Union of India, (2021) 10 S.C.C. 1 (India).

surveillance was purportedly carried out without legal authorisation or court supervision added to the incident's seriousness.

Noting that "**the power of surveillance must not be used to trample fundamental rights**," the Supreme Court of India formed a committee to look into the use of Pegasus in *Manohar Lal Sharma v. Union of India*. The Court acknowledged that such an infringement constituted an insult to the right to privacy (Article 21) and could have a chilling impact on the freedom of speech (Article 19).

Pegasus serves as a stark reminder of the **asymmetry of power between the State and citizens**. In the absence of strong data protection laws, state surveillance practices—whether overt or covert—can nullify the safeguards of liberty guaranteed by the Constitution.

### **Conclusion and Way Forward**

The way societies engage with information has undergone a radical change as a result of the digital age. Data, an unseen currency that drives algorithmic markets, influences public behaviour, and restructures the relationship between the state and its citizens, is at the core of this change. However, this article has demonstrated through empirical case studies, comparative frameworks, and constitutional analysis that data collection, if unregulated, poses serious dangers to democracy, autonomy, and dignity. It is a constitutional issue, not just a technological or policy one.

India is at a pivotal point in its history. Although *Justice K.S. Puttaswamy v. Union of India* established a strong normative foundation for the acknowledgement of privacy as a basic right, the legal and regulatory framework that has been established since then has been fragmented and occasionally subservient to strong corporate or state interests. Despite being a positive step, the Digital Personal Data Protection Act, 2023 falls short of instituting robust user safeguards, algorithmic transparency, and accountability. Because of the State's extensive exemptions and lax control, residents are at risk of being watched, profiled, and manipulated.

In order to bring India's data governance system into compliance with its constitutional obligations, this study suggests a five-point framework:

#### **1. Amend the DPDP Act to Recognize Algorithmic Rights**

Rights pertaining to automated decision-making, like the right to an explanation and the right to protest profiling, must be included immediately. Without these, people are helpless against opaque and biased algorithmic systems that affect their freedom of expression, credit, opportunities, and health.

#### **2. Establish an Independent Data Protection Authority (DPA)**

India must establish an independent, constitutionally accountable Data Protection Authority with the authority to conduct investigations, audits, and provide remedy in order to guarantee equity and legality in data processing. This body should function with institutional integrity and openness rather than being influenced by executive interests.

#### **3. Mandate Data Impact Assessments and Algorithmic Audits**

Borrowing from the EU's GDPR framework and Brazil's LGPD, India should enforce **Data Protection Impact Assessments (DPIAs)** for high-risk data practices. Mandatory **algorithmic audits** will ensure that AI systems comply with principles of fairness, non-discrimination, and explainability.

#### 4. Enhance Digital Literacy and Privacy Awareness

Without the empowering of citizens, no reform can be successful. To empower people to make knowledgeable decisions about their digital identities, privacy education must be incorporated into curriculum and awareness campaigns at public platforms, schools, and universities.

#### 5. Embed Constitutional Morality into Data Laws

Constitutional principles like liberty, fraternity, and dignity must be included into digital policymaking rather than existing as abstract ideas. Every rule or practice pertaining to data must be examined for both legality and ethical compatibility with the equality and justice envisioned in the constitution.

In conclusion, India's digital future depends on its capacity to protect the fundamental rights of its people as much as on technological advancement. The state must actively protect constitutional morality in cyberspace rather than serving as a passive regulator. After all, data is about people, not just machines. Furthermore, under a constitutional democracy, the people are in charge.

### References

#### Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
2. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2018) 1 S.C.C. 809 (India).
3. Karmanya Singh Sareen & Anr. v. Union of India & Ors., W.P. (C) No. 7663 of 2016 (Delhi High Ct. Aug. 25, 2016) (India).
4. Manohar Lal Sharma v. Union of India, (2021) 10 S.C.C. 1 (India).

#### Statutes and Rules

5. Constitution of India arts. 14, 15, 19, 21.
6. Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
7. Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
8. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, Apr. 11, 2011 (India). Government and Committee Reports
9. Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, MeitY (2018).
10. Facebook–Cambridge Analytica Data Misuse: Questions for the Future, U.K. Parl., House of Commons (2018).

#### Books and Scholarly Literature

11. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).
12. Sandra Wachter, Brent Mittelstadt & Chris Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, 41 Comput. L. & Sec. Rev. 105567 (2021).
13. Jonathan Haidt & Jean M. Twenge, *Social Media Use and Mental Health: A Review*, 11 Curr. Opin. Psychol. 48 (2022).
14. Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of I1K Shopping Websites*, 2021 Proc. ACM Hum.-Comput. Interact. 1, Foreign Laws
15. Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
16. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2022).
17. Lei Geral de Proteção de Dados (LGPD), Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.08.2018 (Braz.).
18. Personal Information Protection Act (PIPA) (S. Kor.).