DATA PRIVACY IN INDIA: HOW SAFE IS AN INDIVIDUAL'S PERSONAL DATA?

Dr. Sangeetha Bandlamudi

Principal, PSR Law College, Kakinada, Andhra Pradesh

Abstract: *Data privacy has become one of the most pressing concerns in India's rapidly digitizing ecosystem. With the exponential rise of internet penetration, Aadhaar-linked services, and digital transactions, the personal data of individuals is increasingly vulnerable to misuse, surveillance, and cybercrimes. This article examines the evolution of data privacy in India, tracing its judicial recognition from Kharak Singh v. State of Uttar Pradesh to the landmark Justice K.S. Puttaswamy v. Union of India judgment that declared privacy a fundamental right. It further analyzes the existing legal framework, including the Information Technology Act, 2000, the Aadhaar Act, and the recently enacted Digital Personal Data Protection Act, 2023. Through relevant case laws, the paper highlights the challenges in safeguarding privacy, such as mass surveillance, data breaches, weak enforcement, and low public awareness. While the DPDP Act is a step towards aligning India with global standards like the EU's GDPR, the practical safety of personal data still depends on robust enforcement, transparency, and citizen empowerment. The study concludes that data privacy in India is legally recognized but practically fragile, requiring a balance between technological progress, state surveillance, and individual autonomy.*

Introduction:

In today's digital age, personal data has become one of the most valuable assets in the world. Every time an individual makes a phone call, opens a mobile application, uses social media, or even visits a hospital, some form of their personal information is collected, stored, and processed. This data may include sensitive details such as financial records, medical history, biometrics, browsing habits, and even location trails. While technology has made life convenient, it has also exposed individuals to the risk of their data being misused, leaked, or exploited. The question therefore arises: *How safe is an individual's personal data in India?*

India, with its population of over 1.4 billion and one of the fastest-growing digital economies, stands at the centre of this debate. The government has been promoting initiatives like **Digital India**, Aadhaar-linked services, and online banking, which encourage citizens to adopt technology. Private companies, both Indian and multinational, are equally engaged in collecting and analyzing user data to improve services, advertising, and consumer profiling. However, the lack of robust awareness among citizens, weak enforcement mechanisms, and aggressive state surveillance programs have made data privacy a matter of deep concern.

The Indian legal framework for privacy has not developed overnight. Historically, privacy was not even expressly recognized as a fundamental right in the Constitution of India. The earliest constitutional debates considered privacy to be a matter of personal liberty but did not carve out a specific right. Over the years, the Supreme Court, through its evolving jurisprudence, laid the foundation for privacy as a constitutional guarantee. Starting from *Kharak Singh v. State of Uttar Pradesh (1962)*, where surveillance practices were questioned, to the landmark judgment in *Justice K.S. Puttaswamy v. Union of India (2017)*, the Court finally held that privacy is a **fundamental right under Article 21 of the Constitution**. This judgment changed the legal landscape, giving Indian citizens a constitutional shield against arbitrary intrusion into their personal lives.

Despite this recognition, the **practical safety of personal data in India remains fragile**. Cybersecurity incidents, unauthorized data sharing, and misuse of Aadhaar information have raised alarm bells. India has witnessed several high-profile data breaches involving telecom companies, banking institutions, and even government portals.

The increasing reliance on Aadhaar authentication for basic services such as ration distribution, education, and healthcare has intensified concerns about surveillance and profiling.

Recognizing these issues, the Indian legislature has attempted to create statutory safeguards. The **Information Technology Act, 2000** and its rules introduced obligations for data protection, particularly for sensitive personal data. However, these provisions were often criticized for being outdated and inadequate to tackle the complexities of the digital world. To address this gap, India recently enacted the **Digital Personal Data Protection Act, 2023 (DPDP Act)**, which provides a framework for how personal data should be processed, stored, and protected. The Act draws inspiration from international standards such as the **European Union's General Data Protection Regulation (GDPR)** but also reflects India's unique socio-political challenges.

At the same time, there is a delicate balance to be struck between the right to privacy and the state's responsibility for **national security, public order, and governance**. Surveillance systems, such as the Central Monitoring System (CMS) and the National Intelligence Grid (NATGRID), have been established to monitor communication and strengthen security. However, these have often been criticized for operating without adequate checks and transparency, leading to fears of overreach and misuse.

Thus, while India has formally recognized data privacy as a constitutional and statutory right, the **safety of personal data is still questionable in practice**. The effectiveness of laws depends not just on their existence, but on **implementation, accountability, and public awareness**. Citizens must not only be protected through legal frameworks but also empowered to understand how their data is used.

This article explores the current state of data privacy in India, examining judicial developments, statutory protections, major case laws, and challenges in enforcement. It aims to answer the critical question: *Is personal data in India truly safe, or is it vulnerable to misuse despite the legal safeguards?*

Understanding Data Privacy:

Data privacy is not merely about keeping information secret; it is about ensuring that individuals retain control over their personal datawho collects it, how it is used, and for what purpose. In simple terms, **data privacy is the right of a person to decide what information about them should be shared, with whom, and under what conditions**. It recognizes that personal data, much like property, is a part of an individual's autonomy and dignity.

In the modern digital world, personal data has evolved into a kind of "currency." Companies, governments, and organizations collect vast amounts of data every dayranging from phone numbers and addresses to highly sensitive details like medical records, biometric identifiers, and financial information. This data is then analyzed, traded, or stored for purposes like targeted advertising, fraud detection, or governance. While the collection of data itself is not inherently problematic, the **misuse, unauthorized access, or negligent handling of data creates serious risks** for individuals.

Key Elements of Data Privacy

1. Consent and Choice

At the core of data privacy lies the principle of consent. Individuals must have the freedom to decide whether or not they want to share their information. True consent must be informed, free, and specific. Unfortunately, in India, most people click "I Agree" on digital platforms without actually reading terms and conditions, leading to situations where personal data is used in ways the user never intended.

2. Purpose Limitation

Personal data must be collected for a specific purpose and used only for that purpose. For instance, if a bank collects Aadhaar details to verify identity, it should not use the same data for marketing or share it with third parties without the individual's permission.

3. Data Minimization

Organizations should only collect as much data as is necessary for their function. Collecting excess

information increases the risk of misuse and violates the principle of proportionality.

4. Security and Safeguards

Protecting personal data is not just about law but also about robust security practices. Data must be encrypted, securely stored, and guarded against hacking, leaks, or unauthorized internal access.

5. Transparency and Accountability

Entities handling personal data must be transparent about their practices. Individuals should know what data is being collected, why it is collected, how long it will be stored, and with whom it will be shared. Accountability ensures that organizations can be held responsible if they fail to protect user data.

Why Data Privacy Matters in India:

India presents a unique landscape when it comes to data privacy. With one of the world's largest populations and rapid digital adoption, the scale of data being generated is enormous. Initiatives such as Aadhaar, UPI (Unified Payments Interface), online banking, and widespread mobile connectivity have brought millions of people into the digital fold. For a middle-class family, for instance, everyday activities like paying electricity bills, applying for school admissions, or accessing government subsidies now require digital interactions that involve sharing personal data.

However, awareness of data rights remains relatively low among Indian citizens. Many individuals do not realize the value of their data or the consequences of misuse until they become victims of fraud, identity theft, or harassment. Moreover, in a society where trust in institutions is often fragile, data misuse can erode confidence in both private corporations and government initiatives.

The Indian Context of Data Privacy

Globally, data privacy is considered a fundamental part of human rights. Documents like the **Universal Declaration of Human Rights (1948)** and the **International Covenant on Civil and Political Rights (1966)** recognize the right to privacy as essential for human dignity. In India, however, privacy as a legal concept developed slowly. Initially, the Indian Constitution did not expressly include the right to privacy. It was only through judicial interpretation that privacy began to be seen as part of the right to life and personal liberty under Article 21.

The recognition of privacy as a **fundamental right in Justice K.S. Puttaswamy v. Union of India (2017)** marked a watershed moment in Indian legal history. The judgment acknowledged that in the age of technology, safeguarding privacy is essential for protecting individual freedom, dignity, and democracy itself.

Challenges in Defining Privacy in India

Unlike property or contract, privacy is difficult to define in absolute terms. In India, the challenge is compounded by:

- **Cultural differences**, where collective family or community identity sometimes overshadows individual autonomy.
- **Socio-economic disparities**, where many people trade personal data for access to free or subsidized services.
- **State surveillance practices**, justified on grounds of national security and governance, but often criticized as invasive.

Thus, while privacy is a constitutional right, its practical application in India remains contested and fragile.

Evolution of Privacy as a Right in India:

The journey of privacy in India is not one of immediate recognition but of gradual judicial evolution. Unlike some countries where the right to privacy is explicitly enshrined in the Constitution, India's Constitution, drafted in 1950, did not expressly mention "privacy." Instead, it was the judiciary that steadily carved out privacy as an essential component of personal liberty under Article 21 of the Constitution.

Early Reluctance: Privacy Not Recognised (1950s–1960s)

In the initial decades, Indian courts were hesitant to acknowledge privacy as a constitutional right. Two significant judgments reflect this position:

1. M.P. Sharma v. Satish Chandra (1954)

- In this case, the Supreme Court examined whether search and seizure under the Code of Criminal Procedure, 1898 violated the right to privacy.
- The Court held that the Indian Constitution did not explicitly guarantee a right to privacy similar to the U.S. Fourth Amendment.
- It concluded that privacy was not a fundamental right, and thus state authorities had broad powers of search and seizure.

2. Kharak Singh v. State of Uttar Pradesh (1962)

- The issue concerned police surveillance of a criminal suspect, which included night visits and monitoring of movements.
- The majority opinion of the Supreme Court held that the Constitution did not expressly protect privacy. However, it struck down intrusive practices like "domiciliary visits" at night, as they violated Article 21 (Right to Life and Personal Liberty).
- Interestingly, Justice Subba Rao's dissenting opinion became influential later. He argued that privacy is intrinsic to liberty and dignity, planting the seed for future recognition.

These early rulings revealed a judicial reluctance to expand fundamental rights beyond the express wording of the Constitution.

Gradual Acceptance: Privacy Linked to Liberty (1970s–1990s)

By the 1970s, India was experiencing rapid political and social changes. The judiciary began interpreting **Article 21** more liberally, especially after the **Emergency (1975–1977)**, which highlighted the need to protect individual freedoms against state intrusion.

3. Gobind v. State of Madhya Pradesh (1975)

- This case involved police surveillance under the **M.P. Police Regulations**.
- Justice Mathew, while upholding some forms of surveillance, observed that privacy could indeed be part of the right to life and personal liberty.
- He acknowledged that though not absolute, the right to privacy deserved recognition as a constitutional value.

4. Malak Singh v. State of Punjab (1981)

- The Supreme Court emphasized that surveillance must be exercised within reasonable limits and should not violate individual dignity.

5. R. Rajagopal v. State of Tamil Nadu (1994) — also known as the **Auto Shankar case**

- This case related to the publication of the autobiography of a death-row convict.
- The Court held that the right to privacy is implicit in the right to life under Article 21.
- It recognized the right of individuals to safeguard personal matters from unwanted publicity, except in cases involving public officials where public interest prevailed.

6. People's Union for Civil Liberties (PUCL) v. Union of India (1997)

- The case challenged phone tapping by government agencies.
- The Supreme Court declared that telephone conversations are private and protected under Article 21.
- It laid down guidelines requiring safeguards against arbitrary state surveillance.

By the 1990s, privacy had gained recognition as an **implicit fundamental right**, though still not formally declared by a larger bench.

The Aadhaar Era and The Puttaswamy Breakthrough (2010s):

The digital revolution and the rollout of **Aadhaar**, India's biometric identification system, raised pressing questions about mass surveillance, data storage, and individual autonomy. These concerns culminated in one of the most significant constitutional rulings in Indian history.

7. Justice K.S. Puttaswamy v. Union of India (2017)

- A retired judge, Justice Puttaswamy, challenged the Aadhaar scheme on grounds of privacy violation.

- A **nine-judge Constitution Bench** unanimously ruled that the **right to privacy is a fundamental right** under **Article 21**, as well as Articles 14 and 19.
- The Court stressed that privacy includes informational privacy, bodily integrity, and decisional autonomy.
- Importantly, the judgment overturned earlier rulings in *M.P. Sharma* and *Kharak Singh* to the extent they denied privacy as a right.

This judgment was a **watershed moment**—not only did it affirm privacy as a core of human dignity and liberty, but it also placed India in alignment with international human rights standards.

Post-Puttaswamy Developments: Data Protection and Beyond (2018–2023):

After privacy was recognized as a fundamental right, the focus shifted to creating a robust data protection law.

- In **2018**, the Supreme Court delivered its **Aadhaar judgment**, upholding the Aadhaar scheme but striking down provisions that allowed private companies to demand Aadhaar details.
- The **B.N. Srikrishna Committee Report (2018)** laid the groundwork for a data protection framework in India.
- Finally, in **2023**, the **Digital Personal Data Protection Act** was passed, marking India's first comprehensive data privacy law, heavily influenced by global models like the **GDPR (General Data Protection Regulation)** of the European Union.

Legal Framework for Data Privacy in India:

India's data privacy laws are still evolving. The legal ecosystem can be divided into **statutory provisions**, **sectoral regulations**, and the newly enacted **comprehensive legislation**.

1. Information Technology Act, 2000 (IT Act)

- Section 43A: Holds companies accountable if they fail to protect sensitive personal data, requiring them to compensate affected individuals.
- Section 72A: Prescribes punishment for disclosure of personal information without consent.
- Rules on Sensitive Personal Data (2011): Introduced the requirement of consent before collecting sensitive data like health records, passwords, financial details, etc.

2. Sectoral Regulations

- **RBI Guidelines**: Mandate banks to protect financial data of customers.
- **IRDA Regulations**: Protect health and insurance-related data.
- **Aadhaar Act, 2016**: Governs biometric information collected by UIDAI.

3. Digital Personal Data Protection Act, 2023 (DPDP Act)

Recognizing the gaps in earlier laws, Parliament passed the **Digital Personal Data Protection Act, 2023**, India's first comprehensive privacy legislation.

Key features include:

- Consent-based data processing.
- Special protections for children's data.
- Rights to correction, deletion, and grievance redressal.
- Data Protection Board to oversee compliance.
- Significant penalties for data breaches (up to ₹250 crores).

This Act aims to align India's framework with global standards like the **EU's GDPR**.

Challenges in Protecting Data Privacy in India:

Despite legal progress, several challenges remain:

1. Mass Surveillance Concerns

- Use of Aadhaar and facial recognition technologies raise fears of state surveillance.
- Projects like NATGRID and CCTNS centralize citizen data without strong oversight.

2. Frequent Data Breaches

- Reports of large-scale leaks from government databases, including Aadhaar, voter ID, and health records.
- Private companies often lack robust cybersecurity infrastructure.

3. Low Public Awareness

- Many users share personal data online without understanding risks.
- Privacy settings in apps and social media are often ignored.

4. Weak Enforcement

- Unlike the EU's GDPR, India still struggles with strict enforcement and accountability.

Relevant Case Laws on Data Privacy:

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

- Telephone tapping violates privacy unless authorized under due process.

2. Mr. X v. Hospital Z (1998)

- Right to privacy balanced against public interest; disclosure of HIV-positive status upheld for protection of others.

3. Aadhaar Judgment (2018)

- Upheld Aadhaar's constitutional validity but restricted its mandatory use by private companies.

4. Anuradha Bhasin v. Union of India (2020)

- Held that indefinite internet shutdowns violate freedom of expression and indirectly affect privacy rights.

How Safe is Personal Data in India?

Government Collection of Data: Safety vs. Surveillance:

The Indian government is one of the largest collectors of personal data, especially through projects like **Aadhaar**, the **National Population Register (NPR)**, and digital initiatives such as **DigiLocker**. Aadhaar alone stores biometric and demographic details of more than 1.3 billion citizens.

- **Safety Measures Claimed:** UIDAI (Unique Identification Authority of India) has stated that Aadhaar data is encrypted, stored securely, and protected under the Aadhaar Act, 2016.
- **Concerns:** However, multiple reports of Aadhaar data leaks, even from government websites, have cast doubt on these assurances. In 2018, a media investigation revealed that Aadhaar details were being sold for as little as ₹500 on WhatsApp.

Thus, while Aadhaar has enabled financial inclusion and digital identity, the scale of data collection makes it a potential goldmine for hackers and raises fears of **state surveillance**.

Corporate Handling of Data: The Big Tech Challenge:

Private companies ranging from e-commerce platforms to fintech startups also collect vast amounts of data. The danger here lies in **profiling, targeted advertising, and misuse** of customer information.

- **Case Example:** In 2021, Facebook-owned WhatsApp updated its privacy policy, allowing greater data-sharing with its parent company. This triggered mass outrage, leading to the filing of petitions before the Supreme Court.
- **Reality Check:** Unlike the European Union's GDPR, which imposes heavy penalties for data misuse, India (until 2023) lacked a strong data protection framework. Companies operated in a regulatory grey area, often exploiting users' lack of awareness.

Cyber security Risks: Breaches and Hacking:

India is among the top three countries in the world for cyberattacks, according to global cybersecurity reports. The **CERT-In (Indian Computer Emergency Response Team)** regularly issues alerts about phishing attacks, ransomware, and data breaches.

- **High-Profile Breaches:**

- In 2020, personal details of 7 million BHIM app users were reportedly exposed.
- In 2021, Domino's India allegedly faced a data breach exposing customer names, phone numbers, and addresses.
- In 2023, reports suggested that the CoWIN vaccination portal leaked sensitive health and ID data of millions.

These incidents show that **personal data safety in India is still vulnerable**, especially due to poor cyber security infrastructure in both government and private databases.

Judicial Safeguards: The Role of Courts:

The Indian judiciary has been a crucial guardian of privacy and data security. After the landmark **Justice K.S. Puttaswamy (2017)** judgment, the courts have consistently held that informational privacy is part of the fundamental right to privacy.

- In **PUCL v. Union of India (1997)**, the Court curbed arbitrary telephone tapping.
- In **Puttaswamy (Aadhaar, 2018)**, while Aadhaar was upheld, the Court struck down provisions allowing private companies to demand Aadhaar authentication.

The judiciary has repeatedly stressed that data collection must be **proportionate, necessary, and safeguarded**.

The Legal Framework: Is It Enough?

Until recently, India relied heavily on the **Information Technology (IT) Act, 2000**, and its **Reasonable Security Practices Rules (2011)** to regulate data. These laws were outdated and weak compared to global standards.

The game-changer came with the **Digital Personal Data Protection Act, 2023 (DPDP Act)**. Key highlights:

- Recognises individuals as "Data Principals" with rights over their personal data.
- Imposes obligations on "Data Fiduciaries" (companies/government) to ensure data security.
- Provides penalties up to ₹250 crore for serious breaches.
- Establishes a **Data Protection Board of India** for oversight.

However, critics argue that the Act gives **broad exemptions to the government** under "national interest," which could dilute its effectiveness.

Ground Reality: How Safe Is Data Today?

Despite the new legal framework, **data safety in India remains questionable** for several reasons:

1. **Implementation Gap:** Laws exist, but enforcement is weak. Many companies still operate without robust data security practices.
2. **Lack of Awareness:** A large portion of India's population is digitally illiterate and unaware of their data rights.
3. **Government Exemptions:** The DPDP Act allows wide state surveillance powers, which could erode personal privacy.
4. **Cyber security Deficiency:** India lacks enough trained cyber security professionals to protect its digital ecosystem.

The Way Forward:

1. **Strong Implementation** of the DPDP Act with an empowered Data Protection Board.
2. **Regular Cyber security Audits** for both government and private entities.
3. **Awareness Campaigns** to educate citizens about digital privacy.
4. **Striking a Balance** between national security and individual privacy.
5. **Learning from Global Best Practices** like GDPR in the EU and CCPA in California.

Conclusion:

The debate on data privacy in India is not just a legal or technological issue it is about human dignity, individual autonomy, and the trust that citizens place in institutions. While India has taken

commendable steps by recognising privacy as a **fundamental right** and enacting the **Digital Personal Data Protection Act, 2023**, the true test lies in implementation. Laws on paper do not automatically translate into safety in practice.

The reality is that personal data in India remains vulnerable be it through repeated cyber attacks, corporate misuse, or unchecked state surveillance. Citizens often find themselves powerless when their information is leaked or exploited, as remedies are either delayed or inaccessible. The government, as both the largest data collector and the regulator, has a dual responsibility to lead by example: ensuring strict compliance, building stronger security infrastructure, and respecting constitutional values of proportionality and necessity in surveillance.

Ultimately, the question "How safe is personal data in India?" cannot yet be answered with certainty. It is **safer than before**, thanks to judicial interventions and legislative reforms, but **not as safe as it needs to be** for a billion-plus people entering a digital economy. The future of India's digital trust will depend on three pillars—**robust enforcement, greater public awareness, and a cultural shift among institutions to treat data not as a commodity, but as an extension of the individual.**

Only when these conditions are met can India truly claim to have built a digital society where personal data is respected, protected, and secure.

References:

- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
- Govind v. State of Madhya Pradesh, (1975) 2 SCC 148.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- K.S. Puttaswamy v. Union of India (Aadhaar Case), (2019) 1 SCC 1.
- Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
- Mr. X v. Hospital Z, (1998) 8 SCC 296.
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- The Digital Personal Data Protection Act, 2023.
- The Information Technology Act, 2000.
- Reserve Bank of India (RBI). (2016). *Cyber Security Framework in Banks*.
- Insurance Regulatory and Development Authority of India (IRDAI). (2017). *Guidelines on Information and Cyber Security for Insurers*.