International Journal for Research Trends in Social Science & Humanities
Volume 4, Issue 2
Mar-Apr- 2026, PP 1-11

Privacy, Power, and the Digital State: An Interdisciplinary Inquiry into Data Governance and Democracy in India

Lokanath Patra
Research Scholar (Law), Berhampur University, Berhampur

Abstract- The fast expansion of digital technology has significantly altered the dynamics of governance, citizenship, and political engagement. The rise of the digital state in India, defined by data-driven governance, platform-based service provision, and algorithmic decision-making, has transformed the interaction between the State and its citizens. Although digital governance offers efficiency, inclusivity, and openness, it simultaneously consolidates novel forms of power through extensive data collection and management, thereby creating significant concerns about privacy, autonomy, and democratic accountability. This study conducts an interdisciplinary examination of the nexus between privacy, power, and democracy in modern India. This paper analyzes how data governance frameworks shape power dynamics within the digital state, drawing on constitutional law, political theory, sociology, and ethics. This analysis contextualizes India's constitutional acknowledgment of the right to privacy and the developing data protection framework, evaluating their effects on democratic engagement, public trust, and personal dignity.The paper contends that privacy should be perceived not solely as an individual right but as a fundamental democratic safeguard that curtails the concentration of power inside the digital state. Excessive datafication and monitoring jeopardize citizen autonomy, inhibit political participation, and erode the deliberative basis of democracy. The paper critically analyzes state behaviors and legal frameworks, emphasizing the conflict between government efficiency and constitutional principles.The paper advocates for a rights-based, human-centric form of data governance that integrates privacy, accountability, and transparency into the fundamental practices of the digital state. This strategy is crucial to ensuring that digital transformation enhances democratic governance rather than undermining its fundamental values.

Keywords: Digital State; Privacy and Power; Data Governance; Democracy in India; Constitutionalism; Human Rights.

I. Introduction

Digital technology has revolutionized government, economic activity, and citizen–state relations in the 21st century. Digital infrastructures, artificial intelligence, and large-scale data analytics are helping governments worldwide improve public administration and policy delivery. The “digital state,” where digital technology and data infrastructures dominate governing processes, has emerged from this shift.

India is a major example of this transition. Over the past decade, India has adopted various large-scale digital initiatives, including the Digital India Programme, Aadhaar, UPI, and DBT schemes. India's Digital Public Infrastructure (DPI) aims to improve governance, financial inclusion, and service delivery. India is digitizing at unprecedented levels. The largest biometric digital identity system in the world, Aadhaar, has generated over 144 crore numbers as of March 2026. Over 2,707 crore Aadhaar authentication transactions were made in 2024–25, showing how digital identification is integrated into administration and service delivery.

The Unified Payments Interface has made India a global leader in digital payments. In April 2025, UPI processed over 1,867.7 crore transactions worth ₹24.77 lakh crore, involving 460 million users and 65 million merchants. Global figures show that India accounted for 49% of real-time digital payment transactions in 2023, showing the rapid growth of digital financial infrastructure. India's digital economy transition has been expedited by digital payments and online governance. The Reserve Bank of India reported that 99.8% of retail payment transactions in the first half of 2025 were digital, demonstrating widespread adoption of digital financial services.

Large-scale internet connectivity and digital infrastructure developments have extended India's digital ecosystem. BharatNet has connected over 2.15 lakh Gram Panchayats to optical fibre networks, allowing digital governance in rural and remote areas. UMANG, the government's digital service platform, offers over 2,100 government services in 23 Indian languages through a single digital interface. These developments show how India's digital transformation has transformed state-citizen relations. Digital technology has helped governments improve welfare distribution, eliminate administrative waste, and increase financial inclusion. The JAM Trinity—Jan Dhan bank accounts, Aadhaar identification, and mobile connectivity—has enabled direct welfare benefit transfers to millions of beneficiaries, reducing corruption and bureaucratic inefficiencies.

Privacy, surveillance, and state informational power have become major problems as digital governance has grown rapidly. Biometric identity systems, financial platforms, and digital service portals collect and process huge amounts of personal data, raising important considerations concerning storage, protection, and use. Modern governance systems use personal data to shape power interactions between governments, companies, and citizens. Scholars call this the “datafication of governance,” where individuals' identities, behaviors, and interactions are turned into digital data that can be examined and used to inform policy and administration. Such systems promise efficiency and evidence-based government, but they also risk large-scale surveillance and informational disparities between the state and citizens. Governments' ability to gather and analyze large datasets may affect public autonomy, expression, and political engagement. Data protection and privacy regulations are crucial safeguards against excessive state power in democratic nations.

The historic Supreme Court ruling in Justice K.S. Puttaswamy v. Union of India (2017) clarified India's constitutional recognition of privacy. The Court unanimously held that the right to privacy is a fundamental right under Articles 14, 19, and 21 of the Constitution, thereby creating a constitutional framework for informational privacy in the digital age. After this legislation, India passed the Digital Personal Data Protection Act, 2023, to govern data processing and give data principals rights. Despite these improvements, legal safeguards, governmental exemptions, and digital governance accountability measures remain hotly debated. Thus, India's digital transformation issues center on privacy, power, and democracy. Digital technologies can improve governance and economic prospects, but they also create new forms of power that may alter democratic institutions and citizen–state relations.

This study draws on constitutional law, political philosophy, sociology, and digital governance to analyze how data governance frameworks shape democratic values in India. The report examines legal advancements, digital infrastructures, and governance practices to determine how India may use technology while protecting constitutional rights and democratic accountability.

II. Conceptual Framework: The Digital State and Data Governance

The digital state and data governance systems must be explained to understand the relationship between privacy, power, and democracy in modern government. Digital governance has changed governmental power, administrative decision-making, and citizen participation. The digital state integrates digital technology, data infrastructures, and algorithmic processes into government tasks, altering the state-citizen relationship. This section examines data governance, the digital state, and its effects on democratic institutions.

The Emergence of the Digital State

A governance paradigm called the digital state relies on digital technologies for public administration and policy execution. For public services and administrative operations, governments increasingly use digital infrastructures, big data analytics, AI, and online platforms. Scholars believe the digital state is the next step in governance, following the bureaucratic and regulatory states (Margetts & Naumann, 2017). Traditional bureaucratic governance used hierarchical administrative organizations and paper-based records. Information and communication technologies (ICTs) have enabled governments to move toward networked governance systems, where information flows quickly across institutional boundaries and decision-making is automated. Several characteristics define the digital state:

- Digital Identify Systems: Governments can uniquely identify and verify persons in digital contexts via digital identity infrastructures. Aadhaar links biometric identity to welfare, banking, and public services in India, forming the backbone of digital administration.
- Data-driven Governance: Contemporary governance uses massive datasets to inform policy decisions, monitor outcomes, and assess public initiatives. Data analytics helps governments uncover social and economic patterns and create evidence-based policies.
- Public Service Platforms: Governments can provide public services online with digital platforms. Citizens can interact directly with state institutions via government portals, mobile apps, and digital payment methods.
- Algorithmic Choice: Artificial intelligence and automated decision-making systems are increasingly used for administrative decisions and information processing. Such methods may increase efficiency but also raise transparency, accountability, and bias concerns.

The Digital India Programme integrates these factors to create a digitally empowered society and knowledge economy in India. Aadhaar, UPI, DigiLocker, and the Open Network for Digital Commerce are part of India's Digital Public Infrastructure (DPI).

Digital identity, payments, and services are enabled by these platforms. However, the digital state raises governance issues. Cybersecurity, data privacy, digital exclusion, and government and private-sector data misuse are problems as digital infrastructure becomes more important.

Data Governance and Regulatory Frameworks

Data governance has become increasingly important in public policy and legal discourse as digital technologies generate massive amounts of personal and institutional data. Data governance regulates data collection, storage, processing, sharing, and protection through frameworks, principles, and institutions. Data governance requires government, corporate, civil society, and public participation. Data governance focuses on responsible data use while protecting individual rights and public interests. Key elements of data governance:

- Data Gathering and Processing: Governments and corporations use digital identities, financial transactions, health records, and communication networks to collect personal data. Data governance frameworks regulate data gathering and processing.
- Privacy and Data Protection: Data protection laws protect personal data from unlawful access, abuse, and disclosure. These regulations usually define purpose limitation, data reduction, informed consent, and accountability. The Digital Personal Data Protection Act, 2023, is India's main data protection law. Data fiduciaries and data principals are introduced by the Act.
- Institutional Control: Regulatory bodies are vital to data protection compliance. Independent regulators oversee data processing, investigate infractions, and impose penalties.
- Data Sharing, Interoperability: Sharing data between government organizations and private businesses is another issue for data governance systems. Interoperability standards allow digital systems to communicate, enabling seamless service delivery while protecting privacy.

Datafication and Power Transformation

Digital governance transforms social activities and human behavior into quantifiable, analyzed, and stored data, which is one of its biggest effects. Datafication turns social action into online quantified data, allowing organizations to track, anticipate, and affect human behavior, according to van Dijck (2014). Governance and power dynamics are greatly affected by datafication. Traditional state power came from legal authority, coercive institutions, and administration. Power increasingly flows through information and data infrastructures in the digital age. Large-scale data systems let governments:

- Keep track of social and economic activity
- Analyze citizen behavior patterns
- Predict future trends and policy outcome

Such skills can improve governance efficiency but also increase informational power asymmetry. Large datasets controlled by governments and companies may impact individuals and societal institutions.

Surveillance and Digital Panopticon

Michel Foucault's "Panopticon" has been used to study the growth of digital surveillance. Foucault maintained that modern societies increasingly use surveillance to govern conduct, inspired by Jeremy Bentham's jail model, where convicts are always visible to guards. The digital era has made surveillance less dependent on physical observation. Digitization enables continuous monitoring through data collection, metadata analysis, facial recognition, and online tracking. Digital surveillance systems can be used for:

- National security and law enforcement
- Public health monitoring
- Smart city and urban governance projects
- Counter-terrorism operations

Yet intrusive surveillance threatens civil freedoms and democratic accountability. Scholars say that citizens who feel continually observed may self-censor and restrict their political involvement, hindering democratic discourse.

Balancing Innovation and Rights Protection

Modern states must balance the benefits of digital innovation with fundamental rights. Digital governance can boost administrative efficiency and public service delivery, but it requires robust institutional safeguards to prevent abuse of power. Rights-based data governance requires multiple principles:

- To ensure transparency, governments must disclose how personal data is acquired and used.
- Accountability - Public bodies must take responsibility for data misuse.
- Use proportionality - Only acquire data for justifiable purposes.
- Independent Oversight - Institutions must enforce data protection rules impartially through independent oversight.

We need these principles to sustain public trust in digital governance systems and ensure that technical innovation strengthens democratic institutions.

The conceptual framework above shows that the digital state transforms governance. Digital technologies and data infrastructures have increased government data collection and analysis, changing state-citizen power relations. Data-driven governance can improve public administration, but privacy, monitoring, and democratic accountability are major problems. Thus, data governance regulation is crucial to ensure digital transformation adheres to constitutional and human rights norms. This conceptual understanding underpins the analysis of India's constitutional privacy jurisprudence and digital data protection laws.

III. Constitutional Foundations of Privacy in India

The right to privacy is fundamental to modern constitutional discourse, especially in the context of digital governance and data protection. The Indian Constitution does not explicitly recognize privacy as a fundamental right, but the judiciary has increasingly construed it as part of individual liberty, dignity, and autonomy. Indian privacy jurisprudence shows how constitutional interpretation and the judiciary adapt to technological and social changes. Articles 14, 19, and 21 of the Constitution ensure equality before the law, fundamental freedoms, and the right to life and personal liberty, which underpin privacy. Judicial interpretation has broadened these protections to cover bodily integrity, informational privacy, decisional autonomy, and protection against state intrusion.

Early Judicial Privacy Approach

Indian courts interpreted privacy narrowly in the early decades after independence. Due to the lack of a constitutional clause, the judiciary first opposed privacy as a constitutional right.

Kharak Singh v. State of Uttar Pradesh (1962) was an early privacy lawsuit. This case challenged Uttar Pradesh Police Regulations that allowed surveillance of suspected criminals, including nocturnal visits to their homes. The Supreme Court ruled that intrusive surveillance breached Article 21's personal liberty provision. However, the majority verdict did not explicitly recognize privacy as a basic right. Justice Subba Rao's dissent in the case shaped privacy law. Personal liberty encompasses the right to privacy and freedom from undue government intervention, he claimed. This dissent influenced privacy rights-related court judgments.

Another landmark case was Gobind v. Madhya Pradesh (1975). The Supreme Court recognized that Article 21 may safeguard privacy in this case. The Court noted that personal autonomy and intimate decisions may warrant constitutional protection. The Court further stressed that privacy may be limited in the public interest and for public order and security. Early rulings paved the way for constitutional recognition of privacy, notwithstanding its unclear and inconsistent definition.

Privacy Jurisprudence Growth

In the late 20th century, the Supreme Court expanded the scope of Article 21 fundamental rights. The Court held that life and personal liberty include not only physical existence but also dignity.

Several landmark cases expanded privacy rights.

Rajagopal v. Tamil Nadu (1994). In the Auto Shankar case, the Supreme Court upheld the right to privacy in the dissemination of personal information. The Court ruled that people have a right to privacy and that publishing private information without

authorization violates that right. The Court stressed that privacy protects people from unwanted publicity and intrusion into their private lives.

PUCL v. India (1997). This case addressed the constitutionality of the Indian Telegraph Act's telephone tapping. Telephone calls constitute private communication under Article 21, according to the Supreme Court. The Court mandated authorization and periodic review of interception orders to prevent arbitrary surveillance. The court acknowledged that informational and communication privacy are vital to human liberty.

These judgments expanded privacy rights and showed the Court's adaptability to new technologies.

Justice K.S. Puttaswamy v. Union of India (2017): A Legal Milestone

The Supreme Court's Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) ruling was India's most significant privacy ruling. This lawsuit involved Aadhaar challenges and the question of whether the Constitution guarantees privacy. A nine-judge constitutional bench unanimously upheld the right to privacy under the Indian Constitution. The Court noted that privacy is essential to the right to life and personal liberty under Article 21 and stems from Article 19's freedoms and Article 14's equality concept. The judgment identified numerous key privacy aspects, including:

- Bodily Privacy: Preventing medical or biological incursion and preserving physical integrity.
- Informational Privacy: Control over personal data collection, usage, and disclosure.
- Decisional Privacy: Freedom to make familial, relationship, and religious decisions.

In the majority judgment, Justice D.Y. Chandrachud stressed that privacy protects individual dignity, autonomy, and freedom in a democracy. The Court highlighted that technological advances have allowed governments and corporations to acquire and analyze personal data, making privacy protection more crucial than ever. The judgment also established the three-fold criteria for privacy restrictions:

- Legality - Restrictions must be backed by valid laws.
- Legitimate Aim - Laws should serve a legitimate state aim.
- Proportionality - Measures must match the desired outcome.

It is a fundamental principle for assessing privacy-related laws and state actions.

Digital Governance and Privacy

Digital governance is greatly affected by privacy as a fundamental right. Modern governance systems capture and analyze vast amounts of personal data for digital databases, biometric identification, and data analytics.

In Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018), the Supreme Court reviewed these problems. The Court upheld Aadhaar's constitutionality but added regulations to protect privacy rights. The Court allowed welfare and income tax programs to use Aadhaar, but prohibited private businesses from requiring its use. The Court stressed the need for effective controls in large-scale data-gathering systems to prevent the misuse of personal information.

Data and information privacy

The Indian government began data protection reform after the Puttaswamy ruling. The Justice B.N. Srikrishna Committee (2018) advocated a robust data protection law to regulate the processing of personal data and protect informational privacy. The Digital Personal Data Protection Act, 2023, which regulates government and private data processing, was the result of these efforts. Individual rights under the Act include:

- Right to access personal data
- Right to correction and erasure
- Right to grievance redressal
- Right to withdraw consent for data processing

Debates persist over the scope of government exemptions and the efficiency of enforcement procedures under the Act.

Privacy as a Constitutional Value

Privacy is also a constitutional virtue linked to human dignity, autonomy, and democratic involvement. In Puttaswamy, the Supreme Court stressed that privacy allows people to develop their personalities, build relationships, and participate in politics without fear of surveillance or compulsion. Privacy protects persons' personal lives and information in democratic democracies from undue power consolidation. State surveillance and data collection without privacy protections can harm political participation, freedom of expression, and democratic institutions.

India's constitutional acknowledgment of privacy is a major constitutional advance. After a series of rulings, the Supreme Court established privacy as a basic right essential to personal liberty and human dignity in the Puttaswamy verdict. Privacy is even more important in the digital era, when technology allows unprecedented data collection and surveillance. The judiciary's constitutional framework protects against state intervention and lays the groundwork for extensive data protection regulations. Thus, privacy law must evolve to ensure India's digital transition adheres to constitutional and democratic principles.

IV. Data, Power, and Surveillance in the Digital State

Digital governance has rapidly transformed government power and citizen engagement. Data helps governments monitor social activities, formulate public policies, and administer administrative operations in modern governance systems. Digital technologies improve governance efficiency and transparency, but also enable state surveillance and control. Thus, the digital state presents basic problems about data,

power, and democratic accountability. Data-driven governance has emerged as governments collect and analyze massive volumes of personal data.

Data as a source of Power

Data and information are significant instruments for governance and decision-making in the digital age. Governments capture massive amounts of data through digital infrastructures like:

- Identity systems based on biometrics
- Financial transaction platforms
- Telecommunications networks
- Systems for monitoring social media
- Digital welfare databases

This data helps governments study behavior, predict social trends, and adopt targeted policy responses. Data control and processing create informational power asymmetry between the state and citizens. Political theorists believe that governments with vast personal data can affect social behavior and political engagement. Data control becomes crucial to governance in this phenomenon, known as informational power. Informational power concentration in democratic nations increases transparency, accountability, and concerns about civil liberties.

Digital Surveillance

State surveillance has always been used to safeguard public order and national security. Digital technology has transformed current surveillance systems. Digital surveillance uses mechanisms like:

- Biometric identification systems
- Facial recognition technology
- Analyzing communication network metadata
- AI-based monitoring tools
- Large-scale data analysis

Digital surveillance can be ongoing and undetected, unlike traditional kinds of surveillance.

The rise of such technology has led experts to call modern civilizations "surveillance societies," where government systems include individual monitoring.

Foucault and the Digital Panopticon

The French philosopher Michel Foucault's theory is used to study modern governance monitoring. Foucault investigated the Panopticon, Jeremy Bentham's jail design, in Discipline and Punish (1977). Prisoners behaved as if they were constantly being watched because the Panopticon allowed guards to see them without being seen. Modern civilizations implement similar monitoring methods in schools, hospitals, and workplaces, according to Foucault. Constant monitoring improves self-regulation. According to experts, the digital panopticon is more relevant today. Digital technologies allow governments and corporations to track people's actions,

conversations, and online conduct. Thus, surveillance knowledge or fear may have a "chilling effect," discouraging dissent and political debate. This situation poses serious challenges to democratic freedom.

Aadhaar and Data Governance Case Study

The Aadhaar biometric identification system is a major example of large-scale data collection in India. Aadhaar uses biometric and demographic data, such as fingerprints and iris scans, to assign individuals a unique ID. Aadhaar is used for many things:

- Authenticating welfare schemes
- Bank account opening
- Using digital services
- Verifying identity for government initiatives

Aadhaar advocates say it has enhanced benefit delivery by reducing fraud and duplicate beneficiary registrations. The system also helped millions get Direct Benefit Transfers (DBT). Critics have cited privacy and surveillance issues on multiple occasions. Concerns include:

- Biometric data misuse risk
- Data breaches and unauthorized access threats
- potential data-driven profiling of persons

Supreme Court Justice K.S. Puttaswamy v. Union of India (2018) challenged the constitutionality of Aadhaar. The Court maintained the system for welfare objectives, but restricted private enterprises' use of it and stressed data privacy.

Pegasus Surveillance Debate

The Pegasus spyware scandal in India illustrates the limitations of digital surveillance. NSO Group's Pegasus spying software can infiltrate devices and access personal data. Pegasus spyware may have monitored journalists, activists, political leaders, and government personnel in various countries, including India, according to 2021 reports. An impartial technical committee investigated charges in Manohar Lal Sharma v. Union of India (2021) in response to Supreme Court petitions. The Court noted that surveillance technologies, without legislative protections, could jeopardize fundamental rights such as privacy and free speech. The Pegasus controversy illustrates the challenges posed by advanced surveillance technologies in democratic societies.

Emerging Surveillance and Facial Recognition

Indian police have been testing facial recognition technologies (FRT) to improve policing and public security. Using digital cameras and surveillance networks, facial recognition systems identify people in real time based on biometric facial traits. These technologies have been used in:

- Monitoring huge public events
- Identifying suspects in criminal investigations
- Improving urban security

Facial recognition technologies may improve law enforcement, but accuracy, prejudice, and privacy problems remain. Facial recognition algorithms may skew results for certain demographic groups, according to studies. Mass surveillance without legal oversight may also result from the widespread use of such devices.

Private Data Collection and Surveillance Capitalism

Surveillance goes beyond state entities. Through digital platforms, social media, and other online services, private technology companies capture vast amounts of personal data. Shoshana Zuboff named this economic structure "surveillance capitalism," as firms collect and analyze user data to predict and influence customer behavior. Data collection methods on technology platforms include:

- Online search queries
- Interacting on social media
- Location tracking
- History of browsing

Targeted ads and personalized services are generated using this data. The integration of state surveillance and business data collection presents issues for data governance and privacy protection.

Democratic Impacts of Digital Surveillance

The growth of digital surveillance technologies affects democracy. Democracy requires freedom of expression, association, and political engagement without monitoring or retaliation.

By making people feel watched, excessive surveillance might weaken these freedoms. Unchecked spying poses several risks:

1. Civil freedoms erosion
2. Self-censorship among citizens
3. Lower political participation
4. Power concentration in state institutions

These concerns emphasize the need for strong legal and institutional surveillance supervision.

Citizens-state relations have changed dramatically due to data-driven governance. Digital technologies improve administrative efficiency and policy innovation, but they also produce new forms of power that can change democracy. Large-scale data collection, biometric identification, and improved monitoring allow governments to monitor social behavior like never before. These developments may undermine democratic accountability and fundamental rights without proper legal protections. Digital governance must balance privacy and state functions to comply with constitutional ideals. Strong data protection laws.

V. Challenges in India's Data Governance Framework

Although India has made tremendous progress in building a legislative framework for data protection through the Digital Personal Data Protection Act, 2023, and the DPDP Rules, 2025, implementing an effective data governance regime remains difficult. Technological, institutional, legal, and societal factors complicate personal data control in the ever-changing digital world.

Cyberattacks and Data Breach Increase

Data leaks and cyberattacks are becoming a major issue for India's digital governance structure. Cybercriminals can exploit new weaknesses arising from the rapid growth of digital platforms, online banking systems, and cloud infrastructure. More than 5.3 million user accounts were breached in India in a single year, according to recent studies. In recent years, data breaches have exposed over 100 million records containing sensitive personal information, such as Aadhaar numbers, financial information, and medical data, demonstrating the vulnerabilities of India's digital infrastructure. Cyberattacks have hit the financial industry hard. Over 248 data breaches and 15% more cyberattacks on Indian banks occurred in 2025. These incidents show that digitalization boosts the economy but puts citizens and institutions at danger of cybersecurity attacks.

Limited Digital Literacy and Awareness

A lack of public awareness of digital rights and privacy is another issue. Despite the DPDP Act, only 16% of Indian consumers know about the Digital Personal Data Protection law, and most don't know their rights. Furthermore, 56% of people are uninformed of their data rights, limiting their legal recourse for privacy violations. Because people can't enforce rights they don't understand, data protection regulations are less effective. Digital literacy and public education are essential to data governance.

Regulatory and Institutional Capacity Limits

Data protection law enforcement involves institutional strength, technical expertise, and regulatory independence. India's data governance framework has institutional issues. Parliamentary talks on digital governance have highlighted deficiencies in cybersecurity capacity and infrastructure, underlining the need for stronger institutional support for data protection and cybersecurity agencies. The new Indian Data Protection Board is designed to regulate data processing activities. However, this institution's efficacy depends on aspects like:

- Access to skilled technical staff
- Freedom from political influence
- Sufficient finance and resources
- Coordinating with cybersecurity agencies

Without institutional competence, data protection rules may be weakly enforced.

Organizational Compliance Issues
Organisations across India are still trying to comply with the new data protection framework. Many organizations struggle with compliance, according to surveys. As an example:

- Nearly 70% of enterprises struggle to comprehend the DPDP Act.
- 45% report budget constraints for privacy system implementation.
- 77% lack technology for privacy compliance, including consent management and data discovery.

These findings show that a comprehensive data protection framework requires significant technological and professional expenditures.

Broad Government Exemptions and Surveillance Issues
The scope of government exemptions under the DPDP Act is another major problem. The law allows the central government to exclude agencies from data protection for national security, public order, and sovereignty. Critics say these broad exemptions may weaken privacy protections and allow excessive governmental snooping. Policy analysts also worry that the data protection framework may limit access to information and undermine openness. Balance national security with privacy rights is one of the most difficult data governance concerns.

New Technological Risks
Artificial intelligence, facial recognition, and deepfake technologies provide new vulnerabilities that data protection systems may fail to manage. Recent reports suggest that 65% of Indian enterprises have experienced deep fakes, highlighting the growing significance of AI in cyberattacks and misinformation operations. These changes show that data protection regulations must adapt to new technologies.

VI. Policy Recommendations for Rights-Based Data Governance

A rights-based data governance framework is needed to ensure India's digital revolution is constitutional and democratic. While promoting responsible technological innovation, this strategy should prioritize openness, responsibility, and fundamental rights.

Institutional Independence Improvement
The Data Protection Board should be an independent regulatory body with technical skills and budgetary autonomy. Maintaining public trust and ensuring impartial enforcement of data protection legislation require institutional independence.

Cybersecurity Infrastructure Improvement
India must aggressively invest in its cybersecurity ecosystem due to rising cyberattacks and data breaches. This includes:

- Advanced threat detection systems
- Data encryption standards for storage and transmission
- Regular cybersecurity audits for government and corporate entities

These methods will protect sensitive personal data and prevent vulnerabilities.

Digital Literacy and Awareness
Public awareness programs should teach citizens about their digital rights, data privacy, and grievance processes. Schools, universities, and public awareness campaigns can execute educational efforts. People can exercise their data protection rights with better digital literacy.

Data Processing Transparency Improvement
Transparent data collection, processing, and sharing should be implemented by the government and private institutions. Simple consent and privacy statements will boost user trust and accountability.

Judicial Surveillance Oversight
Judicial oversight and proportionality evaluation should apply to communications interception and large-scale data monitoring. This ensures that surveillance tactics meet the Supreme Court's constitutional safeguards.

Global Standards and Cooperation
India should follow international norms, such as the EU's General Data Protection Regulation (GDPR) and other global privacy frameworks, as digital data flows across borders
While protecting privacy, international cooperation will enable cross-border data exchanges.

The difficulties above show that data governance in the digital age is constitutional and democratic, not just technological. Thus, effective regulation must balance technological progress, individual rights, and democratic accountability. India can create a data governance system that supports digital development and constitutional freedoms by boosting legal frameworks, institutional capability, and public awareness.

VII. Conclusion

The digital state has changed citizen-government-technology relationships. Digital governance initiatives such as Aadhaar, Digital India, UPI, and large-scale digital welfare systems have improved administrative efficiency, financial inclusion, and service delivery in India. These developments show how digital technologies can boost economic growth and governance. Meanwhile, data-driven governance has raised privacy, surveillance, and informational power issues. State and private enterprises can now monitor and evaluate citizen behavior via large-scale data collection, biometric identification systems, algorithmic decision-making, and digital surveillance. Such skills can improve policy execution and security management, but they also threaten human autonomy, civil liberties, and democratic accountability.

Justice K.S. Puttaswamy v. Union of India (2017) was a turning point in constitutional privacy jurisprudence when the Supreme Court of India declared privacy a basic right. Privacy is essential to human dignity, personal liberty, and democratic engagement, the

verdict said. It also established that privacy restrictions must be legitimate, necessary, and proportional.

The Digital Personal Data Protection Act, 2023, is a major step toward developing a comprehensive data governance regulatory framework in India. The Act establishes data processing norms and gives individuals rights over their personal data. However, strong institutional structures, regulatory oversight, and ongoing technological adaptation will determine the effectiveness of the data protection regime.

Cybersecurity vulnerabilities, insufficient public knowledge, regulatory capacity constraints, and concerns about government exemptions underscore the need for a more comprehensive, rights-oriented approach to digital governance in India. Transparent regulatory institutions, independent scrutiny, and effective accountability frameworks are needed to protect constitutional freedoms from technological innovation.

Privacy serves a vital purpose in democratic society beyond individual rights. It protects the balance of power between citizens and the state, allowing people to exercise autonomy, express criticism, and engage freely in politics. In the digital age, where personal data is fundamental to governance and economic activity, informational privacy is crucial to democratic legitimacy.

Therefore, India's future digital governance framework must prioritize human-centric data governance that incorporates constitutional principles, technical innovation, and democratic accountability. India can create a governance model that benefits from digital change while protecting fundamental rights by strengthening legal protections, institutional capacity, digital literacy, and transparency in data processing. The ability of technology and legal and political institutions to protect citizens' privacy, dignity, and freedom will determine the success of India's digital state.

References

1. Margetts, H., & Naumann, A. (2017). Government as a platform: What can Estonia show the world? Oxford Internet Institute.
2. van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. Surveillance & Society, 12(2), 197–208.
3. Foucault, M. (1977). Discipline and punish: The birth of the prison. Pantheon Books.
4. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6. Justice K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 SCC 1.
7. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
8. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
9. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
10. People’s Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
11. Manohar Lal Sharma v. Union of India, Writ Petition (Civil) No. 314 of 2021 (Supreme Court of India).

12. Government of India. (2023). Digital Personal Data Protection Act, 2023. Ministry of Law and Justice.
13. Government of India. (2025). Digital Personal Data Protection Rules, 2025 (Draft/Proposed).
14. Justice B. N. Srikrishna Committee. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. Government of India.
15. Reserve Bank of India. (2025). Annual report on payment systems. RBI.
16. Unique Identification Authority of India (UIDAI). (2026). Aadhaar statistics and authentication data. Government of India.
17. National Payments Corporation of India (NPCI). (2025). UPI transaction statistics. NPCI.
18. Ministry of Electronics and Information Technology. (2025). Digital India Programme progress report. Government of India.
19. Telecom Regulatory Authority of India (TRAI). (2025). Telecom and internet penetration report. Government of India.