JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 3 (Jul.-Sep.) | 2026 Art. 9

Balancing Privacy, Consumer Trust and Public Interest in the Digital Age

Krutaghya Kothari
Law Student,
2nd Year, BA.LL.B. (Hons.),
Amity Law School, Amity University, Bengaluru

Recommended Citation
Krutaghya Kothari, *Balancing Privacy, Consumer Trust and Public Interest in the Digital Age*, 2 JILPS 156-174 (2026).
Available at www.jilps.in/current-issue/

Balancing Privacy, Consumer Trust and Public Interest in the Digital Age

ABSTRACT

India's digital growth has changed the way people share, store, and use personal information. Services such as Aadhaar, UPI, DigiLocker, online shopping, digital banking, and artificial intelligence have made everyday life easier, but they have also increased concerns about privacy, data security, and consumer protection. The Digital Personal Data Protection Act, 2023 is India's first comprehensive law dealing with digital personal data and aims to create a balance between protecting individual privacy and supporting governance, business, and innovation. This article examines whether the DPDP Act achieves that balance. It discusses the constitutional right to privacy recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India, the rights and responsibilities created under the Act, the impact of government exemptions, and the growing importance of consumer trust in India's digital economy. It also compares India's approach with the European Union's General Data Protection Regulation (GDPR) to understand what lessons India can adopt while developing its own data protection framework. The article concludes that the DPDP Act is an important beginning, but its long-term success will depend on transparency, accountability, effective implementation, and public trust. As technologies such as artificial intelligence, cloud computing, digital public infrastructure, and cross border digital services continue to grow, India's data protection framework must continue to evolve while protecting both individual rights and legitimate public interests.

KEYWORDS

Digital Personal Data Protection Act, DPDP Act, Privacy, Right to Privacy, Data Protection, Consumer Protection, Government Exemptions, GDPR, Artificial Intelligence, Digital Public Infrastructure, Personal Data, India.

INTRODUCTION

India has changed more in the last decade than it did in the decades before it, at least when it comes to technology. Today, almost everything has a digital alternative. People pay through UPI instead of cash, store important documents on DigiLocker instead of carrying physical copies, verify their identity through Aadhaar, book hospital appointments online, file income tax returns digitally, and even write competitive examinations through online platforms. Private companies have also

become more dependent on personal data through online shopping, digital banking, social media, artificial intelligence, and personalised advertising. Every one of these services depends on collecting, storing, and processing personal information.[1]

This digital growth has made life easier, but it has also created new problems. Personal data is now one of the most valuable resources in the digital economy. Data breaches, identity theft, financial fraud, targeted advertising, online scams, deepfakes, and AI driven profiling have become more common than ever before. At the same time, the Government has become one of the largest collectors of personal data through Digital Public Infrastructure, while private companies continue to expand their use of consumer data for business and innovation. As more personal information moves online, the question is no longer whether data should be collected, but how it should be protected and who should be responsible for protecting it.[2]

The importance of protecting personal data became even more evident after the Supreme Court delivered its landmark judgment in Justice K.S. Puttaswamy, Retd. v. Union of India. The Court recognised privacy as a fundamental right under the Constitution and observed that privacy is not limited to physical space but also extends to informational privacy. In simple terms, people have a right to know how their personal information is collected, used, stored, and shared. The judgment also made it clear that while the State may restrict privacy for legitimate reasons such as national security or public order, those restrictions cannot be unlimited and must satisfy constitutional principles such as legality, necessity, and proportionality.[3]

Against this background, Parliament enacted the Digital Personal Data Protection Act, 2023. The Act is India's first comprehensive legislation dealing exclusively with digital personal data. It gives individuals certain rights over their personal information, places obligations on organisations that process personal data, and creates a framework for data governance in India. It also reflects the Government's larger objective of strengthening India's digital economy, improving consumer confidence, and encouraging responsible innovation. At the same time, the Act has generated significant debate because it grants the Government broad powers to exempt certain agencies from several of its

[1] Ministry of Electronics and Information Technology, Digital Personal Data Protection Act, 2023; PRS Legislative Research, The Digital Personal Data Protection Bill, 2023.

[2] Grant Thornton Bharat, Data Protection Act 2023's Impact on Consumer Businesses, The Way Forward; Lloyd Law College, Data Protection Laws and Their Impact on E Commerce; Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'.

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

provisions.[4]

These exemptions form the central issue of this article. They raise an important constitutional question. If privacy is a fundamental right, should the largest processor of personal data in the country be exempt from parts of the law designed to protect that very right. They also raise practical concerns for consumers and businesses. Trust has become the foundation of every digital service, whether it is an online payment, an e commerce transaction, a digital health record, or an AI powered application. Without trust, people become less willing to share their personal information, and without that trust, India's digital economy cannot continue to grow.[5]

This article examines whether the DPDP Act strikes the right balance between privacy, public interest, and effective governance. It analyses the constitutional principles laid down in Puttaswamy, the objectives of the DPDP Act, the impact of government exemptions on consumers and businesses, and the lessons that India can draw from the GDPR. The article argues that the DPDP Act is an important beginning, but its long-term success will depend on stronger safeguards, greater accountability, and continued public trust in India's digital ecosystem.

INDIA'S DIGITAL REVOLUTION AND THE NEED FOR A DATA PROTECTION LAW

India's digital economy has grown at a pace that few countries have experienced. Government services, financial transactions, education, healthcare, transportation, and even everyday communication have become increasingly dependent on digital platforms. Programmes such as Aadhaar, UPI, DigiLocker, CoWIN, ABHA, FASTag, and the Income Tax portal have made public services more accessible and efficient. At the same time, private companies have expanded their use of e commerce, digital banking, cloud computing, artificial intelligence, and personalised advertising to improve user experience and business operations. Personal data has become the foundation of almost every digital interaction.[6]

This transformation has created enormous opportunities for both the

[4] Digital Personal Data Protection Act 2023; PRS Legislative Research, The Digital Personal Data Protection Bill, 2023.

[5] Digital Personal Data Protection Act 2023 s 17; Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology 2018).

[6] Ministry of Electronics and Information Technology, Digital Personal Data Protection Act, 2023; PRS Legislative Research, The Digital Personal Data Protection Bill, 2023.

Government and businesses. Digital systems have reduced paperwork, improved service delivery, increased financial inclusion, and encouraged innovation. India's Digital Public Infrastructure is now recognised globally as one of the country's biggest achievements. However, the same systems that improve convenience also collect and process large amounts of personal information. Identity details, financial records, health information, educational records, location data, browsing history, and biometric information are now routinely stored in digital form. As the volume of data increases, so does the responsibility to protect it.[7]

The growing dependence on personal data has also exposed new risks. Data breaches have affected both public and private organisations. Cyber fraud, identity theft, phishing attacks, and financial scams have become more common. E commerce platforms rely on consumer data to personalise products and advertisements, while AI systems use large datasets to train models and make predictions about individual behaviour. Cryptocurrency platforms process identity documents through Know Your Customer requirements, while cloud services often transfer data across national borders. These developments show that privacy is no longer only about keeping information secret. It is about ensuring that personal information is collected fairly, used responsibly, stored securely, and deleted when it is no longer required.[8]

The debate around privacy became even stronger as India's digital ecosystem expanded. The Aadhaar project demonstrated how technology could improve welfare delivery and public administration on an unprecedented scale, but it also raised concerns regarding surveillance, consent, and the limits of State power. Questions surrounding the handling of data by online examination authorities, changing privacy policies of digital platforms such as WhatsApp, and the increasing use of AI in both the public and private sectors have further highlighted the importance of transparency and accountability. Each of these examples reflects the same underlying concern, people are willing to adopt digital services only when they trust that their personal information will be protected.[9]

For several years, India relied mainly on the Information Technology Act, 2000 and the Information Technology, Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011

[7] Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'; Grant Thornton Bharat, Data Protection Act 2023's Impact on Consumer Businesses, The Way Forward.
[8] K&S Partners, 'Data Protection and Privacy Risks in E; Forbes India, 'Can WhatsApp Read Your Messages'; KPMG India, 'Cleared for Take Off, Privacy in Aviation'.
[9] Justice K.S. Puttaswamy (Aadhaar-5J.) v Union of India (2019) 1 SCC 1; Forbes India, 'Can WhatsApp Read Your Messages'.

to regulate aspects of data protection. While these laws provided some safeguards, they were introduced at a time when India's digital economy was far smaller and less complex than it is today. They did not create a comprehensive framework governing the collection, processing, storage, transfer, and protection of digital personal data across different sectors.[10]

Recognising these limitations, the Justice B.N. Srikrishna Committee was constituted to examine the need for a dedicated data protection law. The Committee's report acknowledged that personal data had become an essential part of the digital economy and recommended a legal framework that balanced individual privacy, innovation, economic growth, and legitimate State interests. Many of these recommendations eventually shaped the Digital Personal Data Protection Act, 2023, although the final legislation also introduced significant changes, particularly in relation to government exemptions and regulatory oversight.[11]

The DPDP Act was therefore enacted at a time when India required more than a privacy law. It required a law that could support economic growth, encourage responsible innovation, improve consumer confidence, and establish clear rules for both public authorities and private organisations. Whether the Act successfully achieves these objectives, especially considering its broad exemption framework, remains one of the most important questions in India's evolving data protection regime.

PRIVACY AS A CONSTITUTIONAL RIGHT, DOES THE DPDP ACT MEET THE STANDARD

The idea of privacy did not suddenly appear in Indian law with the DPDP Act. It developed gradually through a series of Supreme Court decisions. In Kharak Singh v. State of Uttar Pradesh, the Court recognised that personal liberty under Article 21 deserved constitutional protection, although it stopped short of recognising privacy as a separate fundamental right. This position evolved in Gobind v. State of Madhya Pradesh, where the Court accepted that privacy could be read into Article 21, while also making it clear that the right was not absolute. Later decisions such as R. Rajagopal v. State of Tamil Nadu and People's Union for Civil Liberties v. Union of India strengthened this understanding by recognising an individual's control over personal information and imposing safeguards against arbitrary State surveillance.[12]

[10] Information Technology Act 2000; Digital Personal Data Protection Act 2023.
[11] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology 2018).
[12] Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295; Gobind v State of Madhya

The position was finally settled in Justice K.S. Puttaswamy, Retd. v. Union of India, where a unanimous nine judge Bench held that privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. The judgment recognised that privacy is closely connected with dignity, autonomy, and individual liberty. More importantly for today's digital society, the Court recognised informational privacy, meaning that individuals should have control over how their personal information is collected, processed, stored, and shared. The Court also laid down four principles that continue to guide privacy law in India. Any restriction on privacy must have a legal basis, pursue a legitimate State objective, be necessary and proportionate, and include safeguards against arbitrary exercise of power.[13]

These principles are particularly relevant because the Government has become one of the largest processors of personal data in the country. Aadhaar, DigiLocker, ABHA, CoWIN, FASTag, the Income Tax portal, and several other Digital Public Infrastructure platforms process millions of records every day. The issue is therefore no longer whether the Government can collect personal data. It clearly can, and in many situations it must. The real question is whether that power is exercised within clear constitutional limits.[14]

The Supreme Court revisited this balance in the Aadhaar judgment. While the Court upheld the Aadhaar programme as constitutionally valid, it also struck down certain provisions and emphasised that the collection and use of personal data cannot become unlimited merely because the objective is beneficial. Welfare, administrative efficiency, and technological innovation remain legitimate State interests, but they cannot override constitutional protections without sufficient justification. The Aadhaar judgment therefore reinforced the idea that even large-scale digital governance programmes must remain accountable to constitutional principles.[15]

The DPDP Act, 2023 attempts to translate these constitutional principles into statutory rights and obligations. It recognises Data Principals as the owners of their personal data and grants them rights such as access to information, correction and erasure of data, grievance redressal, and the right to nominate another person to exercise these rights in certain situations. At the same time, Data Fiduciaries are required to process personal data only for lawful purposes, implement reasonable security

Pradesh (1975) 2 SCC 148; R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632; People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.

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

[14] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; Digital Personal Data Protection Act 2023.

[15] K.S. Puttaswamy (Aadhaar-5J.) v Union of India (2019) 1 SCC 1.

safeguards, notify data breaches, and erase data when it is no longer required, unless another law requires its retention. The Act also introduces additional responsibilities for Significant Data Fiduciaries because of the greater risks associated with the volume and sensitivity of the data they process.[16]

These provisions represent a significant improvement over India's earlier legal framework. The Information Technology Act, 2000 and the Sensitive Personal Data Rules of 2011 provided only limited protection and were introduced long before India's digital economy reached its present scale. The DPDP Act creates a more structured framework that recognises privacy as a legal right while also encouraging responsible data governance and business compliance. Industry bodies have generally welcomed this development, noting that stronger data protection standards can improve consumer confidence, support cross border business, and strengthen India's position as a digital economy.[17]

However, recognising rights is only one part of the framework. Those rights must also remain meaningful when personal data is processed by public authorities. This is where the constitutional debate begins. If privacy is a fundamental right, then any exemption from the protections created by the DPDP Act must also satisfy the constitutional principles established in Puttaswamy. The next section therefore examines whether the Government's exemption powers under the Act maintain that balance between individual rights, public interest, and effective governance.

GOVERNMENT EXEMPTIONS UNDER THE DPDP ACT, BALANCING PUBLIC INTEREST AND INDIVIDUAL PRIVACY

The DPDP Act was enacted to create a single legal framework for protecting digital personal data in India. It gives individuals several statutory rights over their personal information and places corresponding obligations on organisations that collect and process that data. At the same time, the Act recognises that privacy cannot be treated as an absolute right. There are situations where the Government must process personal data to protect national security, maintain public order, investigate offences, deliver welfare schemes, collect taxes, regulate financial systems, and provide essential public services. A modern data protection law therefore cannot ignore the practical needs of

[16] Digital Personal Data Protection Act 2023.

[17] Information Technology Act 2000; Grant Thornton Bharat, Data Protection Act 2023's Impact on Consumer Businesses, The Way Forward; Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'.

governance.[18]

This is reflected in Section 17 of the DPDP Act, which allows exemptions from certain provisions of the Act in specific situations. These exemptions cover matters relating to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, maintenance of public order, prevention or investigation of offences, judicial proceedings, research, and statistical purposes. The Act also empowers the Central Government to notify certain instrumentalities of the State that may be exempt from obligations under the Act. On paper, these objectives appear reasonable because every democratic country recognises that governments require limited powers to protect larger public interests.[19]

The constitutional concern is therefore not the existence of exemptions, but the way they operate. In Puttaswamy, the Supreme Court accepted that privacy may be restricted where the restriction has a legal basis and serves a legitimate State purpose. However, the Court also made it clear that such restrictions must be necessary, proportionate, and accompanied by adequate procedural safeguards. A broad exemption without sufficient accountability risks shifting the balance away from individual rights and towards unchecked executive discretion.[20]

This concern becomes more significant because of the scale at which the Government now processes personal data. Platforms such as Aadhaar, DigiLocker, ABHA, CoWIN, FASTag, the Income Tax portal, and several other Digital Public Infrastructure initiatives handle millions of records every day. Citizens are often required to share personal information to access essential public services. Unlike many private services, these interactions are not always optional. This creates a greater responsibility on the State to ensure that personal data is processed fairly, securely, and transparently.[21]

The Justice B.N. Srikrishna Committee recognised this concern while recommending a comprehensive data protection framework for India. The Committee accepted that the State may require exemptions in limited circumstances, but it also emphasised that such powers should remain accountable and should not dilute the overall objective of protecting informational privacy. The Committee repeatedly stressed that trust is essential for a successful digital economy. Citizens are more likely to adopt digital services when they believe that their personal information is protected by clear legal safeguards and independent

[18] Digital Personal Data Protection Act 2023.
[19] Digital Personal Data Protection Act 2023, s 17.
[20] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
[21] K.S. Puttaswamy (Aadhaar-5J.) v Union of India (2019) 1 SCC 1.

oversight.[22]

The debate surrounding government exemptions is not only constitutional, but it also has practical consequences for consumers and businesses. The DPDP Act gives Data Principals rights such as access to information, correction, erasure, grievance redressal, and nomination. These rights strengthen an individual's control over personal data and encourage responsible data governance. However, where broad exemptions apply, individuals may find it more difficult to understand how their data is being processed or to exercise these rights effectively. If rights cannot be enforced against one of the largest processors of personal data in the country, questions naturally arise regarding their practical value.[23]

Businesses are also affected by this framework. The DPDP Act requires organisations to establish stronger compliance systems, improve cybersecurity practices, implement data retention and deletion policies, and maintain greater transparency while processing consumer information. Industry reports suggest that these measures are likely to increase consumer confidence and improve India's reputation as a trusted digital economy. At the same time, businesses have expressed concerns regarding compliance costs, evolving regulatory requirements, and the need for greater clarity under the Act. Despite these challenges, many organisations view stronger privacy standards as an investment that can improve customer trust and support long term digital growth.[24]

The relationship between data protection and consumer protection has also become increasingly important. Consumers now share personal information almost every time they shop online, book travel, order food, use digital banking services, or access entertainment platforms. E commerce companies rely on personal data to personalise recommendations, process payments, deliver goods, and provide customer support. While these services improve convenience, they also increase the risk of profiling, targeted advertising, dark patterns, unauthorised data sharing, and financial fraud. Privacy therefore cannot be viewed separately from consumer protection. A strong data protection framework also strengthens consumer rights by improving

[22] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India 2018)
[23] Digital Personal Data Protection Act 2023; Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India 2018) .
[24] Grant Thornton Bharat, Data Protection Act 2023's Impact on Consumer Businesses, The Way Forward; Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'.

transparency, informed consent, and accountability across the digital marketplace.[25]

These concerns become even more relevant when emerging technologies are considered. Artificial intelligence depends on large datasets to generate predictions and automate decisions. Cryptocurrency exchanges collect extensive identity documents through Know Your Customer requirements while operating across multiple jurisdictions. Cloud computing enables data to move across national borders within seconds. As technology continues to evolve, exemptions that were designed for traditional governance may require periodic review to ensure that they remain consistent with constitutional principles and technological realities.[26]

The debate therefore extends beyond Section 17 itself. It is ultimately about trust. Citizens trust governments with their identity, health records, financial information, educational records, and biometric data because they expect that information to be protected. Businesses invest in compliance because they believe stronger privacy standards encourage consumer confidence. The success of the DPDP Act will therefore depend not only on the rights it creates, but also on whether those rights remain meaningful in practice. This is where a comparison with the GDPR becomes particularly useful, because it demonstrates another approach to balancing governmental powers with transparency, accountability, and independent oversight.[27]

LEARNING FROM THE GDPR, BUILDING A STRONGER DATA PROTECTION FRAMEWORK

The GDPR is often described as the global standard for data protection. Many countries have referred to it while developing their own privacy laws, including India during the discussions leading to the DPDP Act. However, the purpose of comparing the two laws is not to decide which one is better. The European Union and India have different constitutional systems, different populations, and different administrative challenges. A better question is whether there are lessons that India can adopt while developing its own data protection framework.[28]

[25] Sai Krishna Associates, 'Navigating the Intersection of Data Protection and Consumer Protection Laws in India'; Legal Service India, 'Click, Cart and Rights, Consumer Protection in India's E Commerce Era'; Lloyd Law College, 'Data Protection Laws and Their Impact on E Commerce'.
[26] KPMG India, 'Cleared for Take Off, Privacy in Aviation'; Forbes India, 'Can WhatsApp Read Your Messages'.
[27] General Data Protection Regulation (Regulation (EU) 2016/679); Tsaaro Consulting, 'DPDP GDPR Divergence Map, A Practitioner's Comparative Analysis'.
[28] Ibid.

Both the GDPR and the DPDP Act recognise that governments need access to personal data in certain situations. National security, criminal investigations, taxation, public health, and welfare administration all require governments to process personal information. The difference lies in the safeguards that accompany those powers. Under the GDPR, even public authorities are generally expected to follow the same core principles that apply to private organisations. Personal data must be collected for a specific purpose, processed lawfully, limited to what is necessary, kept accurate, protected through appropriate security measures, and deleted when it is no longer required. Restrictions on these rights are permitted, but they must be clearly provided by law and remain proportionate to the objective they seek to achieve.[29]

Another important difference is institutional accountability. The GDPR requires every Member State to establish an independent supervisory authority responsible for monitoring compliance, investigating complaints, conducting audits, and taking enforcement action. Individuals also have clear rights to approach these authorities and seek judicial remedies when they believe their personal data has been misused. This creates a system where accountability does not depend entirely on the executive.[30]

India has adopted a different model through the Data Protection Board established under the DPDP Act. The creation of a dedicated regulatory body is an important step, but questions remain regarding its independence, powers, and effectiveness, especially in situations where government agencies are exempt from parts of the Act. As India's digital ecosystem continues to grow, strong institutions will become just as important as strong legislation. A law can recognise rights on paper, but those rights become meaningful only when there is an effective mechanism to enforce them.[31]

The GDPR also places greater emphasis on transparency. Organisations are generally required to inform individuals about why their personal data is being collected, how it will be used, how long it will be retained, and with whom it may be shared. Individuals have rights to access their data, correct inaccurate information, request deletion in certain circumstances, object to forms of processing, and seek remedies when these rights are violated. These measures encourage public confidence because people understand what happens to their personal

[29] General Data Protection Regulation (Regulation (EU) 2016/679).
[30] Ibid.
[31] Digital Personal Data Protection Act 2023; General Data Protection Regulation (Regulation (EU) 2016/679).

information.[32]

The DPDP Act moves India in the same direction by recognising several rights for Data Principals and introducing obligations for Data Fiduciaries. However, the practical impact of these rights depends on consistent implementation. Consumer confidence is influenced not only by the existence of legal rights but also by the ease with which those rights can be exercised. Businesses have similarly recognised that stronger privacy standards can improve customer trust, strengthen digital commerce, and support international business relationships. Compliance should therefore be viewed not merely as a legal obligation, but as an important part of responsible corporate governance.[33]

The comparison becomes even more relevant when emerging technologies are considered. Artificial intelligence now analyses consumer behaviour, recommends financial products, detects fraud, assists public administration, and influences commercial decisions. Facial recognition systems are increasingly used for security and identity verification. Cryptocurrency exchanges process sensitive identity documents while operating across multiple jurisdictions, and cloud computing allows personal data to move instantly across international borders. These technologies were not as widespread when many earlier privacy laws were introduced. As a result, modern data protection frameworks must be flexible enough to respond to technological developments without compromising constitutional values.[34]

Recent developments around AI regulation in the European Union also demonstrate that data protection alone cannot address every challenge created by new technologies. Issues such as automated decision making, algorithmic bias, deepfakes, and transparency require broader regulatory frameworks working alongside privacy laws. India is beginning to face similar questions as AI becomes part of banking, healthcare, education, recruitment, law enforcement, and public administration. While the DPDP Act provides a foundation, future reforms may need to address these issues more directly.[35]

This does not mean that India should copy the GDPR. India's governance structure, constitutional priorities, digital public infrastructure, and

[32] General Data Protection Regulation (Regulation (EU) 2016/679).
[33] Digital Personal Data Protection Act 2023; Grant Thornton Bharat, Data Protection Act 2023's Impact on Consumer Businesses, The Way Forward; Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'
[34] KPMG India, 'Cleared for Take Off, Privacy in Aviation'; Forbes India, 'Can WhatsApp Read Your Messages'.
[35] General Data Protection Regulation (Regulation (EU) 2016/679); KPMG India, 'Cleared for Take Off, Privacy in Aviation'.

developmental needs are very different from those of the European Union. A direct transplant of European law would neither be practical nor desirable. However, certain principles deserve serious consideration. Stronger institutional independence, clearer limits on government exemptions, greater transparency, periodic review of exemption powers, better grievance redressal, and increased public awareness would strengthen the existing framework without restricting the Government's ability to perform legitimate public functions.[36]

Ultimately, the GDPR demonstrates that protecting privacy and promoting innovation are not competing objectives. Strong privacy laws encourage consumer trust, responsible business practices, and long-term digital growth. As India continues expanding its digital economy through AI, Digital Public Infrastructure, fintech, healthcare technology, smart cities, and cross border digital services, maintaining that balance will become increasingly important. The success of the DPDP Act will therefore depend not only on how well it protects personal data today, but also on how effectively it adapts to the technological challenges of tomorrow.[37]

THE ROAD AHEAD, STRENGTHENING INDIA'S DATA PROTECTION FRAMEWORK

The DPDP Act is an important step towards protecting digital personal data in India, but it should not be seen as the final stage of India's privacy journey. Technology is changing faster than legislation, and the law will need to evolve to address new challenges while continuing to protect constitutional rights. Future reforms should therefore focus on improving the existing framework rather than replacing it.[38]

The first priority should be improving transparency and accountability in relation to government exemptions. National security, public order, and effective administration are legitimate State interests, and the Government must have sufficient powers to perform these functions. However, exemptions should remain limited, clearly defined, and subject to periodic review. Greater transparency regarding the use of exemption powers would strengthen public confidence without preventing the Government from carrying out its legitimate

[36] General Data Protection Regulation (Regulation (EU) 2016/679); Tsaaro Consulting, 'DPDP GDPR Divergence Map, A Practitioner's Comparative Analysis'.
[37] General Data Protection Regulation (Regulation (EU) 2016/679); Digital Personal Data Protection Act 2023; Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'.
[38] Digital Personal Data Protection Act 2023; Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India 2018).

responsibilities.[39]

A second priority is strengthening institutional oversight. The Data Protection Board has an important role in enforcing the DPDP Act, but public confidence also depends on the perception that regulatory decisions are fair, independent, and effective. As India's digital economy grows, regulatory institutions will need adequate resources, technical expertise, and operational independence to respond to increasingly complex privacy issues involving both public authorities and private organisations.[40]

Consumer awareness should also become a key part of India's data protection framework. Many people continue to share personal information without understanding how it may be collected, analysed, stored, or shared. Privacy policies are often lengthy and difficult to understand, while consent is frequently treated as a routine formality rather than an informed decision. Improving digital literacy, simplifying privacy notices, and encouraging responsible data practices would allow individuals to exercise their rights more effectively.[41]

Businesses also have an important role to play. Compliance should not be viewed only as a legal requirement or a financial burden. Strong privacy practices can improve customer confidence, reduce cybersecurity risks, strengthen corporate governance, and create long term commercial benefits. As more Indian businesses expand internationally, aligning with globally recognised privacy standards may also improve cross border trade and digital cooperation.[42]

Future reforms should also prepare for technologies that are developing much faster than existing legal frameworks. Artificial intelligence, facial recognition, blockchain, cloud computing, and cross border digital services continue to raise new questions regarding transparency, accountability, automated decision making, and data security. Rather than waiting for these issues to become widespread disputes, India should continue developing sector specific guidance and regulatory standards that work alongside the DPDP Act while remaining consistent

[39] Digital Personal Data Protection Act 2023, s 17; *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
[40] Digital Personal Data Protection Act 2023; General Data Protection Regulation (Regulation (EU) 2016/679).
[41] Digital Personal Data Protection Act 2023; Sai Krishna Associates, 'Navigating the Intersection of Data Protection and Consumer Protection Laws in India'.
[42] Grant Thornton Bharat, Data Protection Act 2023's Impact on Consumer Businesses, The Way Forward; Khanna and Associates, 'DPDP Act Compliance for Businesses'; Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'.

with constitutional principles.[43]

Finally, privacy should not be viewed only as a legal issue. It is equally an issue of public trust. Every time an individual uses Aadhaar, makes a UPI payment, stores a document on DigiLocker, books a flight, shops online, or interacts with an AI powered service, they place trust in the organisation handling their personal information. Protecting that trust is ultimately the objective of every data protection framework. The success of the DPDP Act will therefore depend not only on the rights it creates, but also on whether citizens, businesses, and public institutions continue to believe that India's digital ecosystem is secure, transparent, and accountable.[44]

CONCLUSION

India's digital transformation has changed the way people live, work, communicate, and access public services. Personal data now plays an important role in almost every aspect of daily life, from digital payments and healthcare to education, e commerce, and governance. As technology continues to evolve, protecting personal information is no longer only a question of privacy. It has become a question of constitutional rights, consumer confidence, responsible business practices, and public trust.

The DPDP Act, 2023 is an important milestone in India's journey towards a comprehensive data protection framework. It recognises rights for Data Principals, creates responsibilities for Data Fiduciaries, and provides a legal foundation for regulating the collection and processing of digital personal data. At the same time, the broad exemption powers granted to the Government continue to raise legitimate constitutional concerns. The Supreme Court in Justice K.S. Puttaswamy, Retd. v. Union of India made it clear that privacy is a fundamental right, but it also recognised that this right may be restricted where there is a lawful, necessary, and proportionate reason for doing so. The real challenge therefore is not deciding whether exemptions should exist, but ensuring that they remain subject to adequate safeguards, transparency, and accountability.

The comparison with the GDPR shows that strong privacy protections and effective governance are not mutually exclusive. Although India should not simply copy the European model, it can learn from its emphasis on independent oversight, transparency, accountability, and

[43] General Data Protection Regulation (Regulation (EU) 2016/679); KPMG India, 'Cleared for Take Off, Privacy in Aviation'.

[44] Digital Personal Data Protection Act 2023; General Data Protection Regulation (Regulation (EU) 2016/679); Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader'.

effective remedies. At the same time, India's own digital ecosystem presents unique challenges. Digital Public Infrastructure, artificial intelligence, digital commerce, cryptocurrency platforms, cloud computing, and cross border data flows require a framework that is flexible enough to encourage innovation while continuing to protect individual rights.

The future of data protection in India will depend on much more than legislation alone. Courts will continue to interpret constitutional principles, regulators will shape compliance standards, businesses will develop stronger privacy practices, and citizens will become increasingly aware of their digital rights. As new technologies continue to emerge, the law must evolve alongside them without losing sight of the constitutional values that protect individual dignity and personal liberty.

Ultimately, the success of the DPDP Act will not be measured only by the number of penalties imposed or the volume of compliance achieved. It will be measured by whether people continue to trust the digital systems they use every day. Every Aadhaar authentication, every UPI payment, every online purchase, every digital health record, and every interaction with an AI powered service depends on that trust. Protecting personal data is therefore not only about complying with the law. It is about protecting the relationship between citizens, businesses, and the State in an increasingly digital society. If that trust is maintained, the DPDP Act will become more than a data protection law. It will become one of the foundations of India's digital future.

BIBLIOGRAPHY

Constitutional Provisions

- Constitution of India: https://www.indiacode.nic.in/bitstream/123456789/19150/1/constitution_of_india.pdf

Statutes

- Digital Personal Data Protection Act, 2023: https://www.indiacode.nic.in/handle/123456789/22037
- General Data Protection Regulation (Regulation (EU) 2016/679): https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Information Technology Act, 2000: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Cases

- Gobind 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 (Aadhaar-5J.) v Union of India (2019) 1 SCC 1.
- Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295.
- People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.
- R. Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.

Government and Committee Reports

- Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, 2018): https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
- PRS Legislative Research, The Digital Personal Data Protection Bill, 2023, Legislative Brief: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

Professional Publications and Online Resources

- Economic Times Telecom, 'DPDP Act to Boost Consumer Confidence and Position India as a Digital Economy Leader': https://telecom.economictimes.indiatimes.com/news/policy/dpdp-act-to-boost-consumer-confidence-and-position-india-as-a-digital-economy-leader/127376868
- Forbes India, 'Can WhatsApp Read Your Messages': https://www.forbesindia.com/article/news/can-whatsapp-read-your-messages/2993170/1
- Grant Thornton Bharat, 'Data Protection Act 2023's Impact on Consumer Businesses, The Way Forward': https://www.grantthornton.in/insights/blogs/data-protection-act-2023s-impact-on-consumer-businesses-the-way-forward/
- Khanna and Associates, 'DPDP Act Compliance for Businesses': https://khannaandassociates.com/blog/dpdp-act-compliance-for-businesses/
- KPMG India, 'Cleared for Take Off, Privacy in Aviation': https://kpmg.com/in/en/insights/2026/02/cleared-for-take-off-privacy-in-aviation.html
- K&S Partners, 'Data Protection and Privacy Risks in E Commerce': https://ksandk.com/data-protection-and-data-privacy/e-commerce-privacy-risk/

- K&S Partners, 'Penalties and Adjudication under India's DPDP Act, 2023': https://ksandk.com/data-protection-and-data-privacy/penalties-adjudication-under-indias-dpdp-act-2023/
- Legal Service India, 'Click, Cart and Rights, Consumer Protection in India's E Commerce Era': https://www.legalserviceindia.com/Legal-Articles/click-cart-and-rights-consumer-protection-in-indias-e-commerce-era/
- Lloyd Law College, 'Data Protection Laws and Their Impact on E Commerce': https://www.lloydlawcollege.edu.in/blog/data-protection-laws-impact-ecommerce.html
- Sai Krishna Associates, 'Navigating the Intersection of Data Protection and Consumer Protection Laws in India': https://www.saikrishnaassociates.com/navigating-the-intersection-of-data-protection-and-consumer-protection-laws-in-india/
- Tsaaro Consulting, 'DPDP GDPR Divergence Map, A Practitioner's Comparative Analysis': https://tsaaro.com/blogs/dpdp-gdpr-divergence-map-a-practitioner-s-comparative-analysis