Digital Social Science

Innovative

Article

The Digital Shield and the Sovereign State: A Legal Analysis of Cybersecurity, Data Privacy, and the DPDPA 2023 in India

Aman Kumar Jha*, Sujal Chhajed and Tanishk Bhawsar

National Law Institute University, Kerwa Dam Road, Bhopal-462044, India
sujalchhajed.bscllb@nliu.ac.in (S.C); tanishkbhawsar.bscllb@nliu.ac.in (T.B)
* Correspondence: amankumarjha.bscllb@nliu.ac.in (A.K.J)

Abstract: India's economy is developing rapidly due to digitization, changing the way citizens interact with the government and improving the way services are delivered. However, significant cybersecurity issues are identified in India's digital system, demanding new ways to protect citizens' "informational privacy". This study explores the evolution of Indian (privacy) law by significant courts' decisions; starting with *M.P. Sharma* (1954) and ending with the *K.S. Puttaswamy v Union of India* (2017) that established the right to privacy as part of the fundamental rights framework established through Article 14, 19, and 21 of the Constitution. Accordingly, a close analysis of the Digital Personal Data Protection Act 2023 ("The DPDPA") is reported exploring the conflict between state interests and individual liberties and specifically the broad exemptions provided to government agencies pursuant to Section 17 of the DPDPA. It is these same exemptions that some persons believe will enable unchecked government surveillance on an equivalent basis as the "Going Dark" debate related to encrypted data. The paper will focus on the technical aspects of how the laws and regulations defining end-to-end encrypted systems, zero-trust security models (pursuant to CERT-In's requirements to report breaches within six hours), and the requirements to report breaches/other incidents within six hours can be interpreted and enforced. Comparisons will be made to the General Data Protection Regulation (GDPR) of the European Union and how there are gaps in the Indian framework that do not ensure regulatory independence and/or facilitate cross-border data transfers. Ultimately, while DPDPA 2023 may represent an important moment in Indian legal history, its success or failure will depend more on the operational independence of the Data Protection Board than on the harmonization of legal requirements with the changing nature of cybersecurity.

Keywords: right to privacy; DPDP act 2023; state surveillance; cybersecurity and data fiduciary obligations; end-to-end encryption

Citation: Aman Kumar Jha, Sujal Chhajed and Tanishk Bhawsar. 2025. The Digital Shield and the Sovereign State: A Legal Analysis of Cybersecurity, Data Privacy, and the DPDPA 2023 in India. *Digital Social Sciences 2(1)*, 23-27. https://doi.org/10.69971/dss.2.1.2025.37

1. Introduction

Data has transformed into a crucial economic asset that promotes innovation and governance, meanwhile putting consumers at risk of violating their privacy, having their identity stolen, and facing cyber threats (Joshi 2023). Digital change in India has resulted in the Aadhaar system being ubiquitous and rapid growth of digital public infrastructure, resulting in the reconfiguration of the social contract between citizens and the state. The country's cybersecurity infrastructure contains significant vulnerabilities, which require a fundamental transformation of the legal and constitutional legal framework.

India's privacy law has been slow to develop because the courts did not accept privacy as a separate right under the Constitution. In M.P. Sharma v. Satish Chandra, a Supreme Court judge looked only at the literal meaning of the Constitution when deciding the case. He determined that the Constitution doesn't explicitly state a right to privacy, so the rights of the individual are secondary to the right of the state to conduct searches or seizures.1 The Supreme Court made the same judgment in Kharak Singh v. State of Uttar Pradesh stating that while unauthorized entry into one's residence is an infringement of one's personal liberty, it does not mean that a right to privacy is a fundamental right guaranteed by the Constitution.[2]

1 *M.P. Sharma v Satish Chandra* 1 SCR 1077.
2 *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295.

In 2017, the landmark ruling by K.S. Puttaswamy against the union of India provided a conclusive resolution to this long-standing trajectory of historical injustices. This nine-judge bench ruling, unanimously overturned six previous decisions and reaffirmed that the right to privacy is part of the right to life and personal liberty under Article 21 of the Constitution.[3] Further, the right to privacy is constitutionally protected as one of three components of the 'Golden Triangle' composed of the Fundamental Rights of Articles 14, 19 and 21.

The Puttaswamy ruling was not made in isolation. Anxiety emerged about an increase in centralized databases and on-state surveillance abilities. A major catalyst for a legislative response was the catastrophic vulnerabilities of the Aadhaar framework. In January 2018, it was noticed that unauthorized agents were able to access the sensitive demographic information (such as name, address and date of birth) of more than 1 billion Indian citizens, for as little as ₹500 (Yechury 2018). This highlighted weaknesses in the biometric ecosystem, and emphasized the "going dark" issue. Law enforcement agencies have legal authority to intercept communications but do so without the appropriate technical ability due to the growth of encryption technologies. Contrarily, the government has too much access to its citizens' data but provides insufficient protections for it (Dixit 2018).

The digital personal data protection act was created from judicial decisions about privacy laws and the need for cybersecurity measures. The act codifies the right to privacy in the Puttaswamy judgement and establishes a framework to create an informed consent-based process, use personal information, and limit the amount of personal data (Kumar 2025). The cybersecurity becomes more sophisticated ranging from an attack on encrypted WhatsApp communications to the state-sponsored use of spyware such as Pegasus, versus protecting the state's ability to carry out its national security responsibilities (Sohrab 2025). This study analyses the digital personal data protection act, 2023 in conjunction with the IT Act regarding a sufficient "digital shield" between a digital user and a national state versus the impact of the broad exemptions in the Digital Personal Data Protection Act, 2023.

2. Privacy, Sovereignty, and the Cryptographic Challenges in India

India's cybersecurity laws derive their foundations from the privacy rights of individuals and the government's responsibility to provide law and order and to ensure national security. The right to privacy is based on the Puttaswamy decision[4] and is an express right under Article 21 (right to life and personal liberty) of the Constitution.[5] The right to privacy has been embedded in the Constitution as an integral part of one's ability to live a private and independent life. However, the Constitution states that all fundamental rights, as described in the Constitution, are not absolute and are subject to reasonable limitation. Article 19(2) allows for restrictions on an individual's freedom of speech and expression, as determined by the State, to protect the sovereignty and integrity of India, and ensure the security of the State.[6]

The constitutional balance has been, tested most recently with the development of cryptography (Dixit 2018). In today's world of securing online commercial sales, ATM networks and instant messaging through services such as WhatsApp - there is no more powerful tool for maintaining the Constitution's guarantee of an individual's "zone of privacy" than encryption. However, law enforcement refers to a phenomenon called "going dark" to the widespread implementation of strong, end-to-end encryption. Law Enforcement has experienced a reduction in the ability of the State to intercept or gain access to communications;[7] therefore credentialing authority to conduct surveillance on a person is now virtually impossible through mathematical means.

India's encryption discussion resembles to that occurring internationally, especially in the US and the EU where security agencies are unable to investigate and prosecute criminals and terrorists as encrypted communications are untraceable.[8] The "going dark" argument claims that if the State does not have access to a method of bypassing the encryption (a "backdoor"), it will be unable to prevent many types of crimes and terrorist acts.[9] The binary argument privacy versus security is flawed because creating weaker encryption to facilitate law enforcement will ultimately weaken the overall national security framework[10] that the legislation is meant to protect by providing access for foreign nations and cybercriminals to critical digital assets.

Legal concepts surrounding access to data are muddled by "Third Party Jurisprudence". Traditionally, any time someone gives information to a third party (for example, bank or an internet service provider), they have been considered to waived their reasonable expectation of privacy with respect to that information. However, with the advent of modern encryption, this concept has been challenged. When a user sends an encrypted message to another user through an encrypted messaging app or email, the third party that provides the messaging service (referred to as the Data Fiduciary in the DPDPA 2023) is just acting as a messenger and does not hold the "keys" to decrypt the data.

Accordingly, the attempts by the State to create laws requiring all data to be traceable or decrypted run directly against the fact, from a mathematical perspective. It is impossible to decrypt or trace encrypted data for the "good guys" without also decrypting or tracing it for the "bad guys." The major constitutional challenge to DPDPA 2023 will therefore be reconciling the State's emergency powers,[11] which have historically been interpreted liberally under the Constitution, with the technical irreversibility of cryptographic standards.

3. The DPDPA 2023 and the Architecture of Control

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

4 Justice K.S. Puttaswamy n(5).

5 Constitution of India, art 21.

6 Constitution of India, art 19(2).

7 ibid.

8 ibid 8-9.

9 ibid 3.

10 ibid 23.

11 Constitution of India, Part XVIII (Emergency Provisions).

Changes in the Constitution of India regrading protecting privacy through the *Puttaswamy*[12] ruling, and through the DPDPA in 2023, represents a significant step in India's overall cybersecurity governance. Article 21 of the Constitution guarantees Indians their right to 'life and personal liberty', and the DPDPA serves as statutory machinery meant to ensure that Indian citizens can exercise their fundamental rights within the digital space.[13] However, a detailed examination of DPDPA indicates that there are two strands of understanding inherent within i. One imposes significant regulatory burden on private companies and the other gives the Indian Government/every level of government the ability to completely ignore conformity and compliance, thereby possibly re-defining the balancing or weighing of 'individual rights and legitimate State interests'.

The DPDPA removes the previous categorization of "Body Corporate" that existed under the Information Technology Act, 2000,[14] and replaces it with the definition of "Data Fiduciary", which is defined as an entity that makes decisions about how to process personal data. This term establishes an implied relationship of trust between the Data Fiduciary and the individuals whose data is being processed,[15] similar to the fiduciary duty under equity law. As a result of the new DPDPA framework, there is a requirement for Data Fiduciaries to have appropriate technical and organizational measures in place to ensure compliance with the DPDPA, including reasonable security safeguards for the protection of personal data from the risk of a data breach (i.e. loss/unauthorized access).

Most importantly, the DPDPA requires that organizations report all personal data breaches to the Data Protection Board of India (DPBI) to both the DPBI and the affected Data Principals. This creates a dual accountability mechanism.[16] However, as it relates to cybersecurity professionals, there is no clear definition in the DPDPA around what constitutes reasonable security safeguards. Unlike the EU's General Data Protection Regulation (GDPR), which has inexpensive technologies such as pseudonymization and encryption that would not be cost-prohibitive to implement; the DPDPA has few technology-related requirements, allowing all organizations to define the reasonable security safeguards they must implement, which may lead to conflicts with the zero trust architectures being used by many private sector organizations to mitigate the concerns with going dark, or where data becomes unavailable to those accessing the system, including system administrators.

Section 17 of the DPDPA[17] gives the Central Government the authority to exempt its agencies from the requirements of the Data Protection Act, for sovereignty and integrity of India, state security, friendly relations with foreign countries, and maintenance of public order. This is similar to the Constitution's Article 19(2) which allows reasonable limits on freedom of speech and expression.[18]

The fact that the State is exempt from some of the consent and purpose limitations could potentially result in the violations of the proportionality test as set out by Puttaswamy[19] because Section 17 makes it possible for government entities to operate outside of the "data privacy" framework that they purport to create. It presents challenges because, pursuant to Article 12 of the Constitution [20], "the State" includes the Government of India, the Parliament of India, the Government of each State, and the Legislatures of each State as well as any other local or otherwise in the territory of India. Therefore, if "the State" is excluded from having to comply with privacy obligations, the protections offered under Article 21[21] to citizens vis-à-vis the State may effectively be rendered illusory.

In a crypto context, the inability for citizens to have their information protected from governmental access by virtue of the government's ability to obtain that information unchecked under Section 17 leads to a direct conflict with end-to-end encryption protocols.[22] The going dark debate has traditionally been framed as a binary choice between privacy and security but a backdoor for the government is also a backdoor for malicious actors, which ultimately undermines the "security of the State" as articulated in Article 19(2) as grounds for restriction.[23] Accordingly, the DPDPA's exemptions can weaken the national security of India by discouraging organisations from adopting strong encryption standards that are needed to protect critical information infrastructure.

4. The GDPR Benchmark versus The Indian Reality

When measuring the effectiveness of any modern data protection regime, there will always be a benchmark established by the EU's GDPR) known as the "gold standard."[24] With the DPDPA 2023 representing India's unique claim of "sovereignty over data," comparing these two systems reveals that there are major differences between them philosophically and structurally regarding how privacy principles, such as data minimization and cross-border transfers, are applied.

The main principle of the GDPR is data minimization allowing only collect and process the minimum amount of data needed to provide service(s) to individuals.[25] In Europe, many checks are imposed on companies that breach this principle, such as

12 *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1, [180]–[181], [297]–[298].

13 Constitution of India, arts 21.

14 The Information Technology Act, 2000, s 43A.

15 The Digital Personal Data Protection Act 2023, s 7.

16 The Digital Personal Data Protection Act 2023, s 18.

17 The Digital Personal Data Protection Act 2023, s 17.

18 ibid 12.

19 ibid 19.

20 Constitution of India, arts 12.

21 ibid 20.

22 Indian Computer Emergency Response Team (CERT-In), Directions under s 70B of the Information Technology Act 2000 (28 April 2022), cl 4.

23 Constitution of India, arts 19(2).

24 Ben Wolford, 'What is GDPR, the EU's new data protection law?' *gdpr.eu,* https://gdpr.eu/what-is-gdpr/, accessed on 10 February, 2026.

25 Regulation (EU) 2016/679 (General Data Protection Regulation), arts 5(1)(c).

WhatsApp. The EU may determine that a company is partially compliant if it does not comply with the data minimization requirement and will require ongoing regulatory scrutiny of that company's data collection practices.

The 2023 DPDPA implements comparable terminology for "purpose limitation".[26] However, the practical application is limited by qualification of the "legitimate uses" rule and the broad exemptions available to the State. The EU framework invalidates data transfers by dominant market participants if privacy protective measures are not met.[27] Conversely, the Executive Branch of Government at the State level has a discretion in deciding if it is in the interests of sovereignty and security to maintain data beyond the need for legitimate purposes.

Law regarding cross-border information transfer is particularly salient, The GDPR's Chapter V governs such matters specifically Article 44 to 50.[28] Under these provisions, personal protections are not diminished when transferring personal data to a third country - necessitating a strict protocol for any such transfers (as established by the EU). Following the invalidation of the privacy shield, EU and US companies were compelled to depend on "standard contractual clauses" (SCCs) to comply with their responsibilities. These SCCs are subject to continuous litigation which adds further uncertainty for all future compliance between these two jurisdictions.[29]

The Digital Personal Data Protection Act in India applies a "blacklist" approach to cross-border transfers of data. Under this legislation, the government may only restrict cross-border transfers to specific countries by order of the central government. Cross-border transfers of data will be allowed by default. The GDPR, however, adopts a "whitelist" or adequacy-based approach. For an expert observer, this represents a significant departure from a restrictions-based approach to data transfer from a rights perspective in the European Union to a geopolitics-based restrictions approach in India. Under the Constitution, the State may restrict the right to freedom of expression for the purpose of maintaining "friendly relations with foreign States" under Article 19(2).[30] This will allow the State's executive branch to either grant permissions for data flows into or out of India or to impose restrictions on those flows while not necessarily having to conduct the technical adequacy assessments used in the European model.

Enforcement context shifts radically from the GDPR. By having separate supervisory authorities adjudicate violations of the GDPR, there is an attempt of independence from the government. However, in India, since the Data Protection Board depends on the center to appoint its members, this doubt its ability to act against the State. Still, the Constitution should provide solace. The Constitution's Articles 32 and 226[31] authorize the Supreme Court and High Courts, to issue writs (including habeas corpus, mandamus, and certiorari) to enforce fundamental rights. Therefore, although the statutory board doesn't have the institutional independence of European boards, the constitutional courts have the "authority to issue directions and orders" to overrule an executive's abuse of power, thus serving as the ultimate protector of the "digital shield."[32]

Encryption is one of the most effective tools at an individual's disposal to maintain their privacy. Therefore, the New Encryption Policy should require stringent encryption standards for all major sectors (e.g., banking, health care, defense) rather than requiring "back doors," which "violate the laws of mathematics" and undermine the integrity of the nation's information systems. The Data Protection Board may impose a very strict policy on the practice of "metadata minimization" so that the principle of purpose limitation is followed. Data Fiduciaries must follow best practices in cybersecurity for publishing "clear data retention schedules," which must be developed to balance the need for forensic traceability against the need for privacy protection. Data Fiduciaries and Organizations must implement "automated stripping tools" on document types to remove embedded log information and revision histories that would unnecessarily expose sensitive information. Additionally, the introduction of a mandatory requirement for all significant Data Fiduciaries to conduct a "metadata minimization audit". A critical vulnerability identified in current practice, for platforms like WhatsApp, is the storage of backups in unencrypted or server-side encrypted formats on third-party clouds. To mitigate this, regulations under the DPDPA should mandate "end-to-end encrypted cloud backups" where encryption keys are "generated and stored exclusively under organizational [or user] control". This ensures that even if a cloud provider is subpoenaed or breached, the data remains unintelligible, thereby curing the "Third Party" defect. To make sure that the exemptions under Section 17 do not make Article 21 meaningless, there needs to be a provision for "procedural safeguards" by the constitutional courts. There should be a requirement for judicial pre- or post-approval of any interception or decryption order issued for the purpose of "defending the sovereignty and integrity of India" so they can satisfy the proportionality test.

5. Conclusions

The analysis of the Digital Personal Data Protection Act, 2023 and the Constitution of India shows a constantly changing legal landscape. The DPDPA 2023 creates a "sovereign paradox" through Section 17, by granting a broad exemption of liability to the government for its processing of personal data and holding Data Fiduciaries accountable as required by Puttaswamy. This broad exemption granted to the State, the DPDPA 2023 preserves the vulnerabilities associated with Third-Party Jurisprudence. It cures by allowing the State access to citizen data processed by DATA Fiduciaries without any judicial oversight. The "going dark" creates a significant problem that cannot be addressed by legislative solutions alone. The privacy and security dichotomy is a false premise as weakening encryption to allow law enforcement agency access will ultimately create new vulnerabilities that adversaries and cybercriminals can exploit. Therefore, for a "Digital Shield" for India, there is need to be not only a legal document, but also a harmonization of statutory mandates with cryptographic realities. There is an urgent need for the government to create a New

---

26 The Digital Personal Data Protection Act 2023, s 6.

27 Regulation (EU) 2016/679 (General Data Protection Regulation), arts 45.

28 Regulation (EU) 2016/679 (General Data Protection Regulation), arts 45.

29 Bundeskartellamt v Meta Platforms Inc (Case C-252/21) EU:C: 2023:537, [118]– [123].

30 ibid 30.

31 Constitution of India, arts 32, 226.

32 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18) EU:C:2020:559 ('Schrems II'), [94]–[101], [168]–[176].

National Encryption Policy that updates the proposals made in 2015. Any new policy on encryption must reflect recent changes in legal and constitutional thought since the landmark decision handed down by the Supreme Court in Puttaswamy.

References

Dixit, Pratik Prakash. 2018. Conceptualizing interaction between cryptography and law. *NUJS Law Review* 11: 327-359. https://nujslawreview.org/wp-content/uploads/2019/01/11.3-Pratik-Prakash-Dixit-CONCEPTUALISING-INTERACTION-BETWEEN-CRYPTOGRAPHY-AND-LAW.pdf

Joshi Sidharth. 2023. Analysis of Right to Informational Privacy with respect to DPDPA 2023. *International Journal of Law Management and Humanities* 6: 3705-3718. https://doij.org/10.10000/IJLMH.118361

Kumar, Dharmendra. 2025. The Right to Privacy Under Article 21: Implications of the DPDP Act, 2023 for Data Protection in India. *International Journal of Leading Research Publication* 6: 1-8. https://www.ijlrp.com/research-paper.php?id=1702

Kumar, P Vasantha. 2024. Cybersecurity and data privacy: legal and ethical dimensions in the digital age. *International Journal of Multidisciplinary Research in Science and Business* 1: 11-12. https://edwin.co.in/egj/index.php/ijmrsb/article/view/1186

Sohrab, Khan Nazma. 2025. Privacy in the age of digital surveillance: analyzing Whatsapp's policy and cybersecurity implications. *Journal of Information Systems Engineering and Management* 10: 937-965. https://doi.org/10.52783/jisem.v10i40s.7543

Yechury, Sitaram. 2018. Rs 500 for billions Aadhaar details 10 minutes. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361