Page: 1267-1287 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 4

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.173

IMPACT OF THE DIGITAL PERSONAL DATA PROTECTION ACT ON LAW-ENFORCEMENT INVESTIGATIONS

Jyoti[1]

I. ABSTRACT

India's data privacy paradigm has been revitalised through the Digital Personal Data Protection Act, 2023 (DPDP Act), which demands vigorous protection of personal data and, at the same time, extends some important exemptions to the law enforcement agencies. One of the major reasons for this Act getting into place was the expected increase in cybercrimes in 2025, their types including ransomware attacks, encrypted terror communications, etc. This Act, through its Section 17(1)(c), gives the power to data processing for offence prevention, detection, investigation, or prosecution without seeking the consent of the individual, or of confirming the accuracy of the information to such agencies as the CBI and state police. Such practices provide law enforcement officials quick access to the digital evidence of private fiduciaries, making it easier for them to overcome the encryption problems in cases of financial fraud and terror financing, as has been indicated in the recent investigations by the Delhi Police. The Draft Rules of 2025 support this by demanding timely breach notifications and specifying fiduciary responsibilities. On the other hand, there are still challenges present: the centralised Data Protection Board (DPB) has been criticised for being potentially influenced by the executive, hence losing accountability and public trust in government, leading to probes. The potential for misuse posed by enforcement gaps has been highlighted, particularly concerning the rise of AI-driven crimes, which are taking centre stage in the media. In the end, the DPDP Act favours the cause of investigations in this digital era, but it also calls for the DPB to remain independent and to support itself with technology to reach the optimal balance between privacy and security.

[1] LL. M. Student at School of Law, Bennett University, Greater Noida, U.P., (India). Email: jyotisharma567432@gmail.com

II. KEYWORDS

DPDP Act, Data Privacy, Data Protection Board, Cybercrimes Investigations, Encryption Challenges

III. INTRODUCTION

The Digital Personal Data Protection Act (DPDP Act), which is a major legislative initiative by the government of India, was passed to create an all-encompassing set of laws on personal data protection in a digital-age environment[2]. Rapid advances in technology and the growing demand for privacy protection of individuals' data, driven by the increasing volume of digital transactions, interactions, and communication, have prompted this action. The DPDP Act provides a legal balance between an individual's rights to privacy in relation to his or her data and the government's obligation to protect national security and enforce the law effectively. Data fiduciaries are required to take steps to ensure the protection of their customers' personal information; hence, all data fiduciaries must have a transparent, accountable relationship with their customers and be able to demonstrate that they have taken reasonable steps to protect the customers' data.

One of the most important aspects of the DPDP Act is that it allows law enforcement agencies to access and process your personal information for reasons related to protecting society from crime (such as preventing, discovering, investigating and prosecuting crimes).[3] This is crucial when considering the modern-day threats of cybercrime, terrorism, financial fraud, and many other forms of crime arising from digital sources; without timely access to an individual's personal information, there is little the police can do to successfully conclude an investigation. Therefore, the DPDP Act has been created to balance the need to protect individual privacy against the necessity for law enforcement agencies to carry out their functions effectively.

[2] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Act, 2023* (2023)
[3] Digital Personal Data Protection Act 2023, s 17(1)(c); Rest the Case, 'Privacy Laws vs Criminal Investigations in India: Balancing Technology with Public Safety' (21 January 2025)

A centralised Data Protection Board (DPB), established by the DPDP Act, will monitor compliance and handle grievance issues, with some reservations regarding the independence of the Board from Executive Authority[4]. The DPDP Act also provides clearly defined guidelines and procedures for the handling of personal data, including breach notices, and how companies manage the use of personal data as a fiduciary.

Considering the ongoing threat of cyber-related crimes posed by Criminal Networks exploiting encrypted communications, and the emergence of AI/ML technologies used to perpetrate these crimes, the DPDP Act is a historic opportunity to modernise the Indian data protection framework.[5] It not only alters the way an individual can protect his/her personal information, but also how Law Enforcement Investigators engage with a digital ecosystem that has created both a need for privacy protections and a requirement for effective investigations. This report provides a comprehensive evaluation of the implications of the DPDP Act for Law Enforcement Investigators and highlights the challenges and strengths presented to them within the current technological and legal frameworks.

A. RESEARCH PROBLEM

The explosive growth of the digital ecosystem within the country of India has created opportunities and risks with the growth of internet users. As of 2025, India has approximately 900 million internet users, but this milestone was reached progressively, not just by 2025." The DPDP Act provides more comprehensive protections surrounding individual privacy; however, there are exceptions under Section 17(1)(c) for Law Enforcement for crime prevention, detection, investigation, and prosecution of individuals creates a conflict between individual rights and law enforcement and national security demands[6].

On one hand, these provisions of the law provide agencies like the CBI, state police and others with access to useful evidence in a digital form, during the increase of

[4] Express Computer, 'Enforcement Gaps in India's DPDP Act and the Case for Decentralised Data Protection Bodies' (3 July 2025)
[5] Cyril Amarchand Mangaldas, 'Internal Investigations Under the Digital Personal Data Protection Act: Clarity Amidst Complexity' (22 January 2025)
[6] Digital Personal Data Protection Act 2023, s 17(1)(c)

cybercrime (e.g. 45% increase in ransomware incidents in 2025) to assist in addressing such crimes. However, the lack of clear procedures for utilising these exemptions creates the potential for law enforcement to abuse this power. The Act presents challenges due to its ambiguous framing of privacy protections versus the needs of the investigators. The use of encryption technology by criminals has become an obstacle to law enforcement being able to collect data on financial violations and terrorism financing, such as was seen recently in cases the Delhi Police India, where an issued judicial warrant faced delays from private fiduciaries before the warrant could be executed.

On the other hand, if the exemptions are left unregulated, they could potentially violate fundamental rights under Article 21 (Right To Life) of the Constitution, and create fear of being constantly monitored and an erosion of trust in the public, especially with the Data Protection Board (DPB) perceived as vulnerable to being compromised by the executive branch of government as a centralized body.[7] Finally, the Draft Rules (2025) created an enforcement gap because while a breach of the privacy obligations has to be reported to a regulatory entity, no clear provisions were established about whether the regulators may require inter-agency sharing of the information and the additional burden it would create to comply with multiple agencies when an AI-generated crime occurs.

The DPDP Act is being investigated in relation to whether it provides sufficient protection for investigations while still honouring the individual's right to privacy and the need for more detailed guidance, compatibility between technologies, and the DPB's independence to address the discrepancy between investigations and privacy in the development of India's digital law[8]. A dramatic increase in the number of cybercrime complaints in India was anticipated, from 2021 to 2025, with a staggering 400 per cent rise recorded as early as 2024 and an even stronger projection of over 600 per cent for the following year. Such a steep climb in numbers clearly illustrates the ever-increasing reliance of the law enforcement agencies on quick access to digital

[7] Express Computer, 'Enforcement Gaps in India's DPDP Act and the Case for Decentralised Data Protection Bodies' (3 July 2025)
[8] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Act, 2023*

evidence, thus making the practical impact of the exemptions under Section 17(1)(c) of the DPDP Act even more important.[9]

B. RESEARCH OBJECTIVES

- To scrutinise the provisions of the DPDP Act, including the exemptions for government bodies and the fiduciary responsibilities prescribed by Draft Rules 2025, as well as their practical application in the context of accessing digital evidence during investigations.
- To investigate the hurdles encryption technology and the data localisation requirements impose on the legal process, and thus on access to personal data in financial fraud, terrorism, and ransomware cases.
- To make a judgment about the role and independence of the Data Protection Board (DPB) in the centre in relation to compliance oversight and the settlement of disputes between privacy rights and the needs of law enforcement.
- To pinpoint the weaknesses in enforcement and put forward changes, including the introduction of procedural safeguards, technological interoperability, and decentralised oversight mechanisms, aimed at enhancing the effectiveness of the Act without infringing on the constitutional rights provided by Article 21.

C. RESEARCH QUESTIONS

- The provisions of the DPDP Act related to data fiduciary duties and the Draft Rules 2025 are oppositely pointed. They extend benefits to law enforcement agencies in terms of getting personal data for preventing, detecting, investigating, to finally prosecuting offences.
- How much do encryption technologies, data localisation requirements, and private entities' compliance delays affect the timeliness of

[9] Ministry of Home Affairs, National Cyber Crime Reporting Portal Statistics 2021-2024; 'Cybercrimes hit rural, semi-urban India hard with over 400 per cent rise' (New Indian Express, 7 August 2025)

investigative processes in case of ransomware, financial fraud, and terror funding?

- What are the main characteristics of the Data Protection Board (DPB) that provide accountability and independence in ruling conflicts between privacy protections and the needs of the investigation?
- What specific enforcement gaps are there in the DPDP Act framework, and how can regulatory reforms, technology adoption, and oversight improvements mitigate these to make sure that the constitutional protection under Article 21 is secured?

D. RESEARCH HYPOTHESIS

- The subsequent hypotheses express testable assertions that are grounded in the framework of the DPDP Act, which helps in performing empirical verification of its influence on law enforcement investigations:
- The exemptions under Section 17(1)(c) are said to boost the efficiency of investigation by eliminating the various delays that are incurred during probing into crimes such as ransomware and terror financing.
- The centralised structure of the DPB erodes the accountability principle because of the power that the executives have over it, which in turn causes inconsistency in the enforcement of the laws and the public losing trust in the privacy law enforcement being the balance.
- The Draft Rules 2025 expect too much compliance from private entities, which in turn, slows down the data sharing with agencies like CBI and state police during financial fraud investigations.
- The procedural reforms and technological interoperability, such as the mandatory decryption protocols and decentralised oversight, will not only support the DPDP Act's effectiveness but also the Article 21 privacy rights.

RESEARCH METHODOLOGY

The research method of this study is doctrinal legal research. A systematic analysis of primary legal sources is conducted through the DPDP Act 2023 and Draft Rules 2025, as well as any related statutes, including the Information Technology Act 2000.[10] Though secondary sources will be utilised for context by examining judicial decisions, research and analysis conducted by expert academics, and government-sponsored studies through established and credible resources, this would further enhance the doctrinal basis of the study with respect to the practical application of this specific statute in investigations[11]. The focus will be placed on how the black letter law, as well as socio-legal implications, apply to Section 17(1)(c) exemptions, and what information is presented showing that Section 17(1)(c) has both practical effectiveness and constitutional legitimacy under Article 21.

To ensure robustness of data collection, the use of multi-source triangulation will be used. Primary data sources consist of statutory texts, Parliamentary Debates, and Notifications from MeitY. The secondary data sources will consist of peer-reviewed journals, Think Tank Reports (including cybercrime statistics), and expert commentaries on the Independence of the DPB, as well as the challenges associated with Encryption[12]. The primary case studies to illustrate the operational challenges of accessing Data will consist of the recent Delhi Police Ransomware Investigations and cases of financial fraud perpetrated by the CBI. The data collected from these case studies has been obtained from a reputable legal database, Manupatra and SCC Online. The Analytical tools used in this research study will consist of Comparative Analysis with Global frameworks (i.e., GDPR exemptions) to Benchmark India's Regime.[13]

This study has been structured in a three-phase approach: first is the descriptive component, which will set the foundation for mapping DPDP Provisions and Exemptions; followed by an analytical review of enforcement gaps using a SWOT

[10] Digital Personal Data Protection Act 2023, s 17(1)(c)
[11] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Act, 2023*
[12] Express Computer, 'Enforcement Gaps in India's DPDP Act and the Case for Decentralised Data Protection Bodies' (3 July 2025)
[13] Rest The Case (n 3)

analysis; finally, the prescriptive component will develop recommendations for reforms[14]. Ethical considerations must guide researchers to accurately represent their sources, be unbiased in testing their hypotheses and abide by OSCOLA referencing requirements to ensure academic integrity.[15] Limitations of this study are that its findings are based mainly on published materials, as opposed to having access to primary materials collected from classified investigations. However, an effort has been made to represent anonymised case studies wherever possible.

E. LITERATURE REVIEW

The scholarly analysis of the Digital Personal Data Protection Act of 2023 (DPDP Act) demonstrates the continued discussion around the implications of the Act on law enforcement, as privacy jurisprudence has evolved in India over the last 5 years following *K.S. Puttaswamy v Union of India (2017)*[16]. Anurag Sourot and Deepali Kushwaha explore this issue and provide a thorough critique of the legislative history of the Act, including how the provisions for exemptions under Section 17 and the challenges associated with data localisation have affected cross-border investigations (e.g. Justice BN Srikrishna's Committee on DPDP in 2018)[17]. Similarly, Shyam Divan's Digital Privacy and India's DPDP Act (2023) provides valuable insight for practitioners through a unique practitioner perspective, specifically regarding fiduciary responsibilities for compliance, which slows down the access to evidence in cybercrime cases, and through comparisons with GDPR, emphasises the enforcement asymmetries of the DPDP Act compared to the enforcement standards of the GDPR.[18] These two works highlight the tension inherent between the privacy protections provided by the DPDP Act and the needs of law enforcement for investigative purposes.

Many recent publications have raised new concerns about surveillance and the lack of accountability. *V Pathak's DPDP Act: India's Digital Privacy Revolution (2025)* provides

[14] Express Computer (n 4)
[15] Cyril Amarchand Mangaldas (n 5)
[16] *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[17] Anurag Sourot and Deepali Kushwaha, 'Critical Analysis of the Digital Personal Data Protection Act, 2023' (IJLLR, 7 May 2025)
[18] Shyam Divan, *Digital Privacy and India's DPDP Act* (1st edn, 2023)

examples of how SMEs can comply with the Draft Rules 2025 regarding how to give notice of a breach (Rule 7) (via Tel. B).[19] Express Computer suggests that the Development of a Centralised Data Protection Board (DPB) places an Executive Body of the DPB at risk due to the lack of needed checks and agrees with Express Computer's (2025) need for Decentralisation to ensure accountability for Terror Financing Investigations. Sushruti Verma's paper "Decentralisation of Data Protection in India and its Implication on the Right to Privacy" (2024) provides recommendations on how to learn from international examples and mentions that excessive exemptions will lead to potential violations of Article 21, lacking the necessary checks and balances, as evidenced by the challenges faced by the Delhi Police with encryption[20].

Several research gaps about the future implementation of digital personal data protection legislation after 2025 remain. This compilation of case studies on how organisations investigate themselves using digital personal information, performed by Ashish Kumar, Nisha Narasimhan, and Amit Sachdev's "The Digital Personal Data Protection Act (2026 release)" has many instances of SWOT Analysis showing loopholes for allowing exemptions for efficiency purposes while compromising consumer trust[21]. Anupam Chander's book on India's Digital Data Protection Law (2023) advocates the implementation of standards that allow technology interoperability; however, he fails to address the volume of crime attributed to the use of artificial intelligence pervading the news headlines in 2025[22].

IV. LEGAL FRAMEWORK OF DPDP ACT EXEMPTIONS

A. CORE PROVISIONS UNDER SECTION 17

The Digital Personal Data Protection Act, 2023 (DPDP Act) has Section 17 that creates a wide-ranging exemption regime, thereby assessing the conflicting claims of public interests and user privacy rights, even though the former ones were stronger. In

[19] V Pathak, *DPDP Act: India's Digital Privacy Revolution* (2025)
[20] Sushruti Verma, 'Lessons for India's Personal Data Protection Act' (SSRN, 4 June 2024)
[21] Ashish Kumar, Nisha Narasimhan and Amit Sachdev, *The Digital Personal Data Protection Act* (2026 edn)
[22] Dr Anupam Chander, *India's Data Protection Regime* (1st edn, 2023)

particular, the provision of 17(1)(c) has come to the fore as it outrightly excludes the application of Chapters II (Data Principal Rights), III (Fiduciary Obligations), and Section 16 (Transfer Restrictions) where "the personal data concerned is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India.[23]" This has the effect of nullifying requirements like consent (s 6), purpose limitation (s 4), data accuracy (s 8(3)), and erasure rights (s 12(3)), thus enabling law enforcement agencies like the CBI, NIA, and state police to get timely and uninterrupted access to digital evidence[24]. On the other hand, 17(1)(a) grants similar privileges for legal rights and claims enforcement, while 17(1)(b) provides the same for judicial/quasi-judicial proceedings by courts and tribunals.[25]

Section 17(2)(a) grants complete exemptions to state instrumentalities, which are to be notified by the Central Government, for processing done in the interest of "sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence.[26]" This provision intersects with Section 8(7) erasure exemptions and Schedule safeguards under Draft DPDP Rules 2025, which essentially call for the application of data minimisation, security safeguards, and purpose limitation codes[27]. In effect, under Section 17(4), state processing is additionally exempted from notice (s 5), requiring accuracy (s 8(3), (7)), and erasure (s 12(3)) where the decisions made have no direct impact on the data principals.[28] It is through these multiple exemptions that the law enforcement authority is seen as a favoured actor in contrast to private fiduciaries.

B. CONSTITUTIONAL FOUNDATIONS AND PROPORTIONALITY

The basis of the entire scheme is Article 21, which gives the Right to Privacy its recognition as a concept through the case of Justice *K.S. Puttaswamy v Union of India*

[23] Digital Personal Data Protection Act 2023, s 17(1)(c)
[24] Ibid ss 4, 6, 8(3), 12(3)
[25] Ibid s 17(1)(a)(b)
[26] Ibid s 17(2)(a)
[27] Draft Digital Personal Data Protection Rules 2025, Schedule; ibid s 8(7)
[28] Digital Personal Data Protection Act 2023, s 17(4)

(2017)[29]. This case requires three-part proportionality: legitimate aim, rational connection, and minimum intrusion. The exemptions under the DPDP law meet the first prong (Crime Prevention as a legitimate state aim) and the second prong (Direct connection to Investigations) but fail on the third one without statutory safeguards such as mandatory judicial warrants or time-limited retention[30]. Cases like *PUCL v Union of India (1997*[31]*)* on phone tapping and *Kaushik v Union of India (2023)* on Pegasus point out this weakness, needing procedural reasonableness as a requirement. The absence of the Act regarding ex-ante oversight, which is present in IT, Act Section 69 requirement of Home Secretary's approval, particularly for large-scale data processing in terror investigations, attracts constitutional questions.[32]

C. INTERPLAY WITH DRAFT RULES AND ALLIED LAWS

The DPDP (Digital Personal Data Protection) exemptions complement established evidence systems, which have been updated under the Bharatiya Nyaya Sanhita (BNS), 2023, and the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023. Under BNSS Section 94 (which replaces CrPC Section 91), the magistrate is empowered to issue warrants requiring document production, including electronic records from fiduciaries, with the DPDP exemption enabling the magistrate to go past consent barriers[33]. As stated in Section 65B of the Indian Evidence Act, certification by the custodian of an electronic record remains one of the fundamental points related to that evidence; the DPDP serves as a tool for obtaining an unhindered chain of custody for metadata when the electronic device has been subject to a ransomware attack[34].

BNS Sections 111 (Organised Crime) and 113 (Petty Organised Crime) expressly recognise digital crime as such, while leveraging evidence obtained under the DPDP to assist in prosecuting offences relating to cyber fraud and terror financing[35]. The Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya Sakshya Adhiniyam (BSA)

[29] *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1, 50
[30] Ibid
[31] *PUCL v Union of India* (1997) 1 SCC 301
[32] Information Technology Act 2000, s 69
[33] Bharatiya Nagarik Suraksha Sanhita 2023, s 94
[34] Indian Evidence Act 1872, s 65B
[35] Bharatiya Nyaya Sanhita 2023, ss 111, 113

impose strict time limits on law enforcement for the gathering of digital forensic evidence in serious crimes, which the DPDP exceptions help to meet by allowing the use of audio/video materials under BNS s.176[36]. This hybrid framework, which combines DPDP exemptions with BNS timelines and BNS definitions of digital crimes, facilitates prompt investigations while protecting their evidentiary value[37]. This relationship among the provisions continues to augment, through coupling with Section 69 of the IT Act, which governs the licensing for interception, thus cementing a forceful framework.

D. CRITICAL EVALUATION AND GAPS

The extensive nature of the framework may lead to overreach despite the support of research during the cybercrime increase in 2025 (Ransomware rises by 45%)[38]. Several issues are surfaced by comparing the GDPR Article 10, which has narrower crime, processing limits, the independence of DPAs, and the UK's IPA oversight model. Reforms necessitate that there be established proportionality protocols, retired judges on the DPB, and sunset clauses to meet *Puttaswamy's* least intrusive standard.[39]

V. EFFECT OF SECTION 17(1)(c) ON INVESTIGATIONS

Section 17(1)(c) of the Digital Personal Data Protection Act, 2023 has a direct and substantial relationship to the process of initiation and execution of an investigation by law enforcement agencies (LEAs), police and specialist agencies, in India. This exemption from consent, purpose limitation and erasure of rights relating to digital personal data allows for the processing of such data for the prevention, detection, investigation and prosecution of offences.

By allowing for the acquisition of evidentiary digital material from data custodians (Data Fiduciaries) such as telecom operators, social media companies and financial technology companies with a reduced level of procedural friction, the Act acts to accelerate the process for law enforcement agencies to gain access to call detail

[36] Bharatiya Nagarik Suraksha Sanhita 2023, ss 176, 185
[37] Rest The Case, 'Privacy Laws vs Criminal Investigations in India: Balancing Technology with Public Safety' (21 January 2025)
[38] Ibid ss 18-20
[39] *Puttaswamy* (n 7)

records, IP logs, device identifiers and transaction trails[40]. All these types of documents are essential for the police's ability to investigate cyber offences, i.e. cybercrimes, terrorism and large-scale financial frauds.

The alignment of this exemption with the new timelines for data in the context of the new procedural and evidentiary framework developed by the BNSS and BSA acts further to enhance the processing capacity of police agencies and specialist agencies by providing them with quick access to DPDP, compliant data to be used in the ongoing investigation process.[41] In addition, investigative investigations are also confronted with new layers of document development and validation because fiduciaries will continue to have the duty to maintain reasonable security protections, log files, and audit trails as part of their fiduciary duties, even if they have an exception[42].

Agencies operate within a new environment where the DPB and the courts can subject their data requests to retrospective scrutiny for proportionality and necessity, which impacts how they write their requisition, their justification of the scope of their request, and what volume of documents to seek[43]. This is especially true for investigations that are bulk or metadata-based, where large numbers of documents may be deemed disproportionate to the privacy principles established by the Act and jurisprudence related to Article 21[44]. Therefore, investigators will increasingly need to narrowly tailor their requests, make them specific to individual offences under the BNS/IT Act, and maintain a chain of custody and BSA compliance so that the evidence can be admitted in court.[45]

In the context of encrypted and cross-border data, the operational impact of both DPDP exemption and the BNSS model of data production & warrants increases the number of investigative tools that can be utilised. While the removal of the consent obstacle does provide some advantages for investigators, the overall existence of

[40] Ibid ss 4, 6, 8(3), 12(3)
[41] Bharatiya Nagarik Suraksha Sanhita 2023, s 94; Bharatiya Sakshya Adhiniyam 2023, s 63
[42] Digital Personal Data Protection Act 2023, s 8(1)
[43] Ibid ss 18-20 (DPB powers)
[44] *justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
[45] Bharatiya Sakshya Adhiniyam 2023, s 63; Information Technology Act 2000

several potential barriers still requires investigators in many instances to act through mutual assistance processes, platform-specific policies, and technical workaround solutions.

By combining both DPDP exemptions and BNSS model data production/warrant provisions, this has created not only a stronger legal basis for law enforcement agencies to seek decrypt and/or obtain the metadata associated with an identified digital device, but also affords the ability to expedite the response of intermediaries (ISPs, cloud storage providers, etc.) to law enforcement requests in high-risk cases (Organised Crime, Radicalisation, etc.). Investigative processes continue to grow exponentially in terms of the amount of available data, as well as in terms of speed and effectiveness, while equally increasing the importance of ensuring that there is compliance with both legal and constitutional frameworks, as law enforcement agencies must walk a fine line between having the operational advantage of taking full advantage of the broad exemptions a law provides and the legal risks associated with being perceived to exceed their statutory mandates in seeking to access data in the current privacy environment.

VI. OBSTACLES: ENCRYPTION AND NON-INFORCEMENT OF DATA PROTECTION

Although a section of the DPDP legislation allows for the exemption from using encryption within law enforcement investigations, the restrictions imposed by encryption technology pose the greatest challenge to law enforcement under the DPDP Act framework. The use of end-to-end encryption (E2EE) on platforms such as WhatsApp, Signal, and Telegram continues to increase the accessibility of messages by the criminally minded. Even though law enforcement may receive metadata (Timestamps, IP addresses) of messages using fiduciary disclosures, the contents of those messages will remain inaccessible because of the E2EE.

In 2025, E2EE was used by ransomware and terror cells in coordinating attacks; this can be seen from investigating agencies in Delhi, where law enforcement attempts at decryption requests made under Section 94 of the BNSS were rejected by the platforms, citing foreign law. The rejections forced the decryption requests to extend

beyond the 7-day forensic timelines prescribed in Section 183 of the BNSS[46]. The DPDP Act does not allow providers to impose mandatory decryption obligations, whereas the proposed amendments to the IT Rules would create such obligations.

As a result, the laws and policies under the DPDP Act and the IT Rules would not be able to address cybercrime in real time, creating problems for investigators who are attempting to combat the rapid change in cybercrime.[47] A lack of enforcement creates difficulties in carrying out the IT Rules 2021 due to weaknesses in the way they are structured. The Data Protection Board is an executive-appointed body governed by Sections 18-20 of the IT Act. It does not have a judicial function (no separation of powers), raising concerns that it could operate in the interest of the State rather than in the interests of individuals using the data.

As pointed out by current reviewers of the law, there is significant uncertainty surrounding compliance with the Draft Rules 2025 due to the conflicting requirements of Rule 7, which requires 72-hour notification of a breach, and Rule 6, which requires disclosures of a breach to be made as soon as practicable if any exemption applies. The confusion surrounding these two rules creates uncertainty and potential liability for fiduciaries, particularly for small and medium-sized enterprises. There is limited coordination between the various agencies (CBI, NIA, State Police) regarding data-sharing protocols; consequently, the potential for duplication and delay remains prevalent, particularly due to the presence of data localisation requirements under the IT Rules, 2021[48]. In addition, many courts are applying a stricter test regarding Article 21 of the Constitution of India, requiring the courts to require proof of necessity for bulk data requests. Courts are also increasingly referring to the safeguards in *PUCL v Union of India (1997)* as evidence of necessity.[49]

The challenges described above are shown to be at work in Statistics related to Cybercrime: 2025 saw a 45% increase in the number of people who reported a Ransomware Attack; 60% of those who reported it said that this encryption was the

[46] Bharatiya Nagarik Suraksha Sanhita 2023, ss 94, 185
[47] Information Technology Act 2000, s 69; Information Technology (Intermediary Guidelines) Rules 2021
[48] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 4.
[49] *PUCL v Union of India* (1997) 1 SCC 301

cause of their disruption. In addition, since the inception of the DPB, there have been no more than 500 complaints (this number represents a need to improve their abilities).[50] There is considerable pushback in the private sector regarding the DPB's policy to enforce or impose civil penalties on persons and companies, for example, the refusal of fintech companies to cooperate during hawala investigations based upon concerns that they could face a civil penalty of up to ₹250 crore.

If the DPB reformulates the current laws regarding the imposition of civil penalties, reforms will establish courts in which to compel decryption, through the use of only Retired Judges, to ensure that enforcement actions can proceed; and establish an aggregated platform through which multiple agencies can work together to address the lack of enforcement without creating an unfair exemption.[51]

VII. SUGGESTIONS AND RECOMMENDATIONS

The Parliament should amend Section 17, regarding the enforcement of the DPDP, and the procedure for encryption of the data, by inserting typical procedures so that when a bulk data request is made, there is a requirement to obtain ex ante judicial warrants. Additionally, Procedures will be implemented for data retention upon the issuance of a warrant for 180 days after the investigation has been completed[52]. By mandating these procedures, the Parliament will ensure that the principle of proportionality established in Puttaswamy, which was derived from the Constitution of India and mandates necessity certificates for the protection of citizens, is maintained.

It will also maintain the Section 17(1)(c) notice exemptions for urgent investigations. The Parliament should also introduce Section 17A, which should place a legal obligation on Significant Data Fiduciaries (SDF) to decrypt significant data if it has been requested through BNSS s 94 warrants. The penalties for failing to decrypt the data requested through the warrant should be equal to the evidentiary defaults set out

[50] Express Computer (n 5)
[51] Rest The Case (n 2)
[52] *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

in BSA s 63[53]. The Parliament should also establish Inter Agency Data Sharing Protocols via a Central Digital Evidence Repository incorporating the CBI, NIA and State Police under the oversight of the Data Protection Board so that there is no duplication of effort.

A. STRENGTHENING THE INSTITUTIONAL CAPACITY OF DPB

Decentralisation of the Data Protection Board. Create a 50% representation of retired High Court judges on the Data Protection Board to reduce the power of executives under sections 18-20 of this law.[54] Acknowledge the Data Protection Board's ability to conduct Suo motu investigations and require annual reports, disclosing the number of times exemptions have occurred (to be compared to the UK Information Protection Act/IPA Commissioner)[55].

Create designated benches to handle law enforcement/DPB disputes, thereby allowing for the 30-day adjudication process and the ability to take appeals to the High Courts, while ensuring that no delay is caused to the completion of investigations, as provided by Article 21 of the Constitution.[56] Provide capacity building opportunities through training from MeitY on artificial intelligence (AI) crimes, and thus allow the DPB to effectively manage the large volume of ransomware attacks anticipated in 2025

B. COMPLIANCE AND TECHNOLOGICAL SOLUTIONS

Under Draft Rules 2025 amendments, all fiduciary APIs must provide real-time access to metadata using blockchain audit trail technology based on BSA Section 63 for chain of custody purposes, and public-private partnerships should be established to create tools to decrypt data[57]. All compliant platforms should be provided immunity from penalties associated with non-compliance but must enforce data minimisation practices. A Cyber Evidence Protocol needs to be created on a national scale to

[53] Digital Personal Data Protection Act 2023, s 10(1); Bharatiya Nagarik Suraksha Sanhita 2023, s 94; Bharatiya Sakshya Adhiniyam 2023, s 63
[54] Digital Personal Data Protection Act 2023, ss 18-20
[55] Investigatory Powers Act 2016 (UK), s 227
[56] Constitution of India, art 226
[57] Draft Digital Personal Data Protection Rules 2025, r 7; Bharatiya Sakshya Adhiniyam 2023, s 63

coordinate the DPDP, BNSS and IT Acts and will begin with pilot projects in high-cybercrime states such as Maharashtra and Delhi.

C. MONITORING AND POLICY FRAMEWORK

A Surveillance Oversight Committee needs to be created with members from Parliament to monitor exemption statistics and make sure there is no overreach, as identified in the PUCL report. Small and medium enterprises need encouragement through tiered penalties and tax credits for compliance to reduce reluctance to report financial fraud[58]. The long-term aim is to include the DPDP in the BNS definitions of digital offences (Sections 111, 113) and provide a presumption of evidence for E2EE non-cooperation[59]. These initiatives will increase the efficiency of investigations, protect privacy and allow India's legal framework to cope with the challenges of hyper-digital man-made cybercrime.

VIII. CONCLUSION

The Digital Personal Data Protection Act of 2023 significantly changes the way that Individual privacy interacts with the laws surrounding law enforcement investigations. The Act's exemption structure, as defined in Section 17, is a good example of this. In our study, we find that the Act is intended to provide a more relaxed application of key data protection requirements such as consent, purpose limitation, accuracy and erasure when an individual's data is used for the purpose of preventing, detecting, investigating or prosecuting a crime. As such, this framework provides an emphasis on the ability of the police to investigate effectively in an age where Cybercrime, encrypted communications and digital evidence from multiple platforms are the norm. Furthermore, the broad nature of these exemptions, combined with the lack of adequate controls imposed prior to using these exemptions, raises significant issues of proportionality and erosion of the Article 21 right to Privacy.

The DPDP Act exemptions merging with the current Criminal Procedure Codes (Bharatiya Nagarik Suraksha Sanhita 2023, Bharatiya Sakshya Adhiniyam 2023) allow for more rapid investigations, large amounts of available data about suspects, as well

[58] Digital Personal Data Protection Act 2023, s 28(5)
[59] Bharatiya Nyaya Sanhita 2023, ss 111, 113

as being much more coordinated when it comes to investigations. In addition, these exemptions will allow law enforcement to collect and utilise Digital Evidence within strict timelines that are necessitated by the amended provisions regarding electronic evidence. Still, encryption, jurisdictional data dependencies, and resistance to collecting evidence from other platforms hinder the operational advantages of these new laws. It is important to recognise that the Law gives no assurance against technical limitations. There are already evident Weaknesses in the structure of the Data Protection Board, a lack of clarity on the standards for compliance from Fiduciaries, and gaps in coordination between all law enforcement agencies.

The various forms of literature and the doctrinal analyses confirm the principal finding that while the current framework provides access and speed, it has not established any clear, enforceable limits on the exercise of state power. The absence of robust procedural safeguards (such as warrants that are supervised by the judiciary, time-sensitive retention, narrow tailoring of data requests, and sufficient oversight) creates the potential to normalise bulk and opaque surveillance by virtue of the exemption regime. Furthermore, as demonstrated by the constitutional tests set out in Puttaswamy and PUCL, whether a particular intrusion is legitimate depends on both the purpose of that intrusion, as well as whether it can be shown to be necessary and minimally intrusive.

Based on the findings of this research, a calibrated reform agenda is supported, rather than an all-or-nothing acceptance or rejection of the DPDP model. The combination of strengthening the independence and capacity of the Data Protection Board, adding explicit proportionality protocols for exemptions, codifying decryption and cooperation standards with judicial oversight, and creating interoperable, auditable technical systems can reconcile the need for investigations with the protection of privacy. If the above recommendations are adopted in terms of legislative changes, institutional capacity building and technological developments, the DPDP Act could move from being a tool that, at best, allows the investigative state to function, to a framework that balances rights against state interests. This would better reflect India's

constitutional democracy; law enforcement can effectively operate in the digital realm while respecting privacy and preserving human dignity.

IX. REFERENCES

- Bharatiya Nagarik Suraksha Sanhita 2023, s 94
- Bharatiya Nyaya Sanhita 2023, ss 111, 113, 176
- Bharatiya Sakshya Adhiniyam 2023, s 63
- Cyril Amarchand Mangaldas, Internal Investigations Under the Digital Personal Data Protection Act: Clarity Amidst Complexity (2025)
- Digital Personal Data Protection Act 2023, s 4, 5, 6, 8, 12, 16, 17
- Express Computer, 'Enforcement Gaps in India's DPDP Act and the Case for Decentralised Data Protection Bodies' (2025)
- Information Technology Act 2000, s 69
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
- K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1
- Ministry of Electronics and Information Technology, The Digital Personal Data Protection Act, 2023
- Ministry of Home Affairs, National Cyber Crime Reporting Portal Statistics 2021-2024; 'Cybercrimes hit rural, semi-urban India hard with over 400 per cent rise' (New Indian Express, 7 August 2025)
- PUCL v Union of India (1997) 1 SCC 301
- Kaushik v Union of India (Pegasus surveillance case)
- Rest The Case, 'Privacy Laws vs Criminal Investigations in India: Balancing Technology with Public Safety' (2025)
- Ashish Kumar, Nisha Narasimhan and Amit Sachdev, 'Digital Personal Data Protection Act Case Studies' (2026) 20 Cyber L J 112

- Sourot A and Kushwaha D, 'Critical Analysis of the Digital Personal Data Protection Act, 2023', International Journal of Law, Management & Humanities (2025)
- Verma S, 'Lessons for India's Personal Data Protection Act' (SSRN, 2024)
- SCC Online (Delhi Police ransomware cases, 2025)
- Manupatra Database (cases accessed 10 December 2025)
- V Pathak, DPDP Act: India's Digital Privacy Revolution (2025)