
WHEN THE STATE BECOMES THE EXCEPTION: EXECUTIVE POWER AND CONSTITUTIONAL PRIVACY UNDER DPDP ACT,2023

Aswathy S Nair, B.A. LL.B., The Kerala Law Academy Law College, Thiruvananthapuram

Harsha M, B.Com. LL.B., The Kerala Law Academy Law College, Thiruvananthapuram

ABSTRACT

Executive exemption and information calling power under the DPDP Act has the effect of placing the State outside the very obligation it creates for others. The paper tries to examine whether these powers given to the Central Government are sufficiently safeguarded to satisfy the constitutional standard that governs any interference with right to privacy. For that the present statutory framework and its evolution across earlier drafts of data protection legislation, along with DPDP rules is examined. The paper also evaluates the framework focusing on the rule making power given to the Central Government, the grounds on which State instrumentalities may be exempted, and the manner in which information may be called for from data fiduciaries and intermediaries. The recognition of privacy as fundamental right has developed through years of judicial interpretation, moving from denial of any standalone right to eventual acceptance of it as important aspect of personal liberty, along with a structured method for testing whether State interference with such right is justified. The study concludes by analysing whether the exemption power and the information calling power meet this standard of sufficient safeguard, and finds that both presently fall short, this being now a matter of ongoing constitutional litigation

Keywords: Digital Personal Data, Executive discretion, Proportionality, State exemption

I. INTRODUCTION

From being treated as outside the scope of protected rights to being recognised as part of the right to life under Article 21, privacy in India has gone through a slow and uneven transformation. For decades, courts were unwilling to accept privacy as an independent right, arguing that its absence from the constitutional text was a deliberate choice, and that statutory procedure need not be tested for fairness. This narrow reading gave the legislature and executive considerable power over how they dealt with personal information. Over time this position shifted and a structured method for testing whether any restriction placed on the right is legitimate, necessary, and proportionate was developed. This background is directly relevant to how the Digital Personal Data Protection Act, 2023 is examined, because the Act was enacted after this proportionality standard was already in place, yet its own design raises the question of whether that standard has actually been carried through. The Act imposes detailed obligations of consent, security and accountability upon data fiduciaries, but it also allows the Central Government to exempt its own instrumentalities from these very obligations, and separately gives it power to call for information from data fiduciaries and intermediaries with little indication of what limits, if any, apply to that power. Both provisions place considerable authority in the hands of the executive, the same body the Act is otherwise meant to hold accountable.

This paper seeks to address whether the exemption power and the information calling power conferred upon the executive under the DPDP Act, 2023 are sufficiently safeguarded to satisfy the constitutional requirement governing interference with right to privacy. For this, the statutory design of these powers, their drafting history across earlier versions of the legislation, the rules made to implement them, and the extent to which an independent institution exists to check their exercise, are examined in turn.

II.CONSTITUTIONAL FOUNDATION OF INFORMATIONAL PRIVACY IN INDIA

2.1 PRIVACY BEFORE PUTTUSWAMY

Over the last six decades, the Indian Constitution did not provide for a standalone right to privacy. In *M.P Sharma v Satish Chandra*¹, the argument presented by petitioner was that the search-and-seizure power under Section 94 and 96 of the Code of Criminal procedure violated

¹ M.P. Sharma and Others vs. Satish Chandra, District Magistrate, Delhi, and Others, AIR 1954 SC 300

their rights under Article 19(1)(f) of the Constitution and that the compulsory production of documents in accordance with search warrants was equivalent to compelled self-incrimination under Article 20(3) and amounted to an unreasonable search, unlike the protections afforded under the U.S. Fourth Amendment. The Supreme Court dismissed this analogy and it was held that the Indian Constitution does not provide any express protection for the right to privacy and that framers, being fully aware of such protections abroad, chose not to include such a provision into Part III. On this basis, the Court upheld the validity of search and seizure under the Code of criminal procedure and it was held that such statutory powers, subject to their own procedural safeguards, do not necessitate a constitutional right to privacy. The judgement in *Kharak Singh v State of UP*² affirmed this principle. Together, these two cases provided the basis for subsequent privacy claims in India to be made indirectly through the narrower lens of Article 19 or 21.

2.2 THE EVOLUTION OF ARTICLE 21

Article 21 of the Constitution provides that no one shall be deprived of his life or personal liberty except in accordance with “procedure established by law” rather than American “due process of law” under which American courts have the power to strike down laws they find unjust and arbitrary, giving judiciary power over legislature and executive. Under the interpretation given in *A.K Gopalan v State of Madras*³ the courts limited themselves to seeing whether a law existed and was it followed procedurally without considering if it was fair, just or reasonable. This gave the legislature more deference. However, the decision in *Maneka Gandhi v Union of India*⁴ marked a crucial departure from this position. The Supreme Court held that the ‘procedure established by law’ under Article 21 should not be arbitrary or oppressive. This evolution of Article 21 shows how judiciary’s interpretive power has developed over time⁵.

2.3 JUSTICE K.S. PUTTASWAMY v UNION OF INDIA

Like separation of powers, the Right to Privacy is not explicitly written into the Constitution. A nine-judge bench of the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*⁶

² *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295

³ *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27

⁴ *Maneka Gandhi v. Union of India*, AIR 1978 SC 597

⁵ M.P. JAIN, INDIAN CONSTITUTIONAL LAW, 861, (9th ed., Lexis Nexis 2024)

⁶ *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors*, AIR 2017 SC 4161

commonly referred to as *Puttaswamy I* overruled the decision in *M.P. Sharma and Kharak Singh*, holding that the right to privacy is fundamental to the right to life and personal liberty guaranteed under Article 21, along with Articles 14 and 19. Both decisional and informational privacy were recognised by the Court as aspects of this right, and State interference with it must satisfy standard of justification.

In *Puttaswamy II*, the Supreme Court applied the proportionality test to answer the specific question of whether the Aadhaar scheme's biometric data collection was a legitimate restriction on individual's privacy. In doing so, the Court moved from simply declaring the right to implementing a method for testing government restriction on it.

2.4 PROPORTIONALITY TEST

By virtue of Article 13, read with Article 32 and 226, the judiciary can strike down laws that violate Fundamental Rights and review executive action for constitutionality. The proportionality test can be said to be the approach the Courts now uses to perform that review. Earlier Indian courts often used the "reasonableness" or "arbitrariness" test grounded in Article 14 to review restrictions on rights. The four-part proportionality analysis makes judicial review more structured and predictable and ensures that any limitation on privacy is justified by legitimate state, with the restriction being necessary and maintaining a proportionate balance between individual right and state interest.

This proportionality framework that was developed in *Puttaswamy* strengthens the right to privacy enshrined in Article 21 since it offers a systematic procedure for evaluating the legality of any restrictions on the objectives state. By incorporating this framework into Article 21, the Court has created a jurisprudential link between the fact that recognition of privacy is a fundamental right and a framework which allows states to assess the permissibility of restriction.⁷

III.THE DPDP ACT AND THE ARCHITECTURE OF STATE POWER

3.1 OBJECTIVE AND SCOPE OF THE ACT

The DPDP Act regulates the processing of digital personal data within India, and also extends

⁷ Rishika Sahgal, Proportionality Review and Economic and Social Rights in India, 8 Indian law review, 207 (2024)

to processing outside India when it is connected with offering goods or services to individuals residing in India. This can be compared to EU's General Data Protection Regulation, although DPDP Act has narrower scope since it covers only digital personal data and excludes non-digitised records and data processed for personal or domestic purposes.

The Act pursues the dual objective of safeguarding individual rights and promoting economic interest. It seeks to maintain individual autonomy by means of consent and notice requirements and establishes obligation for data fiduciaries to ensure the responsible processing of individual's data. The Act prescribes obligations concerning data security, breach notification and regulatory compliance, seeking to strengthen accountability within the digital ecosystem. It further provides for the Data Protection Board of India for addressing violations and enforcing the statutory framework.⁸

3.2 DELEGATION OF RULE MAKING POWER TO CENTRAL GOVERNMENT

Section 40 of the DPDP Act confers the power to make rules entirely to the Central Government. Sub-section (1) confers the general power to make rules, by notification, for the purpose of giving effect to the objects of the Act, while sub-section (2), without prejudice to the said general power, enumerates twenty-five specific provisions on which rules may be framed, together with a residuary power to make rules for 'any other matter'. Furthermore, the Act confers power to issue eleven types of notifications and four miscellaneous powers under Chapter IX, some of which are coercive in nature.

This framework is significant when compared with the Personal Data Protection Bill introduced in December 2019 and withdrawn in 2022. The 2019 Bill provided for the conferral of certain legislative powers to the Data Protection Authority of India, the statutory regulatory authority created under the Bill. Unlike the 2019 Bill, the DPDP Act does not delegate any rule making powers to the Data Protection Board of India created under Section 18. Across different countries, data protection laws delegate rule making authority to the regulatory bodies tasked with implementing the data protection regime because of their specialized expertise and practical experience in regulation. Such an arrangement enhances legislative design and effectiveness of data protection laws. Since the legislation applies to both state and private actors ensuring that the regulators make the rules further strengthen its independence. The

⁸ The Digital Personal Data Protection Act, No. 22 of 2023, Indian code (2023)

concentration of decision-making power in the Central Government sits uneasily with Section 28(1), which separately described the Board as an independent body, raising the question of why the body that was supposed to embody that independence had no say over the rules it would enforce.⁹

IV. SECTION 17: STATE EXEMPTION AND EXPANSION OF EXECUTIVE DISCRETION

4.1 NATURE OF SECTION 17

The Act, while marking an important step towards establishing a legal framework for data protection in India, is substantially circumscribed by the extent of exemption available to the state. Section 17 provides for several exemptions from the Act's obligations. Its provisions raise some constitutional concerns regarding the balance between individual privacy and legitimate State interest.

4.2 ANALYSIS OF SECTION 17(1)(c) and 17(2) OF DPDP ACT

Section 17(1)(c) exempts certain processing activities from key obligations under the Act if such processing is undertaken for the "prevention, detection, investigation or prosecution of any offence or contravention of any law". While such law enforcement exemptions are recognized across data protection frameworks, the wording "any offence or contravention of any law" widens the ambit of the provision extending its application beyond serious criminal offences to include minor statutory contraventions.¹⁰

In contrast, Section 17(2) empowers the Central Government to exclude any notified instrumentality of the State from the operation of the Act on grounds of sovereignty, integrity, security, friendly relations with foreign States, public order or preventing incitement to any cognizable offence relating to any of these. The grounds specified in the Section prima facie pursue legitimate constitutional objectives, as Article 19(2) itself permits restrictions on freedom of speech and expression in the interests of sovereignty, security of the State, and

⁹ Malavika Raghavan, Rulemaking for Data Protection: Implementing India's Digital Personal Data Protection Act, 2023, Indian Journal of Law and Technology Blog (2024), <https://www.ijlt.in/post/rulemaking-for-data-protection-implementing-india-s-digital-personal-data-protection-act-2023>.

¹⁰ Bharat Manwani & Abhiraj Rana, The Right to (Pry)-vacy: Understanding India's Dystopian Data Protection Legislation, N.Y.U.J. Int'l L & Pol. Blog (Feb. 12, 2024), <https://nyujilp.org/the-right-to-pry-vacy-understanding-indias-dystopian-data-protection-legislation/>.

public order. However, these broadly framed grounds have also historically enabled extensive executive interpretation and discretion as these terms are vague and flexible. Justice B.N Srikrishna, who chaired the committee that authored India's earlier draft data protection bill, has observed that such language raises the basic question of what 'sovereignty of nation' means, a criticism that captures how open ended and undefined the exemption is. Nothing in Section 17 itself defines or limits the scope of these terms, establishes a clear threshold for their application, or requires the government to place on record reasons demonstrating that the processing by a particular instrumentality genuinely falls within these grounds. The practical effect is that once a state fiduciary is notified, it does not need to comply with key obligations under the Act. The provision does not expressly require a proportionality assessment, prescribe a sunset period for such exemptions, or establish an independent mechanism for reviewing their exercise.¹¹

Both provisions exhibit substantial overlap, notably in relation to law enforcement and security related processing. The provision is designed to give the government an opportunity to place entire agencies outside the Act's reach on discretionary grounds. When read together, the provisions may create a two-tiered data protection framework in which the State instrumentalities enjoy fewer statutory constraints than private data fiduciaries.

4.3 A COMPARATIVE READING WITH EARLIER BILL DRAFT

In contrast to previous drafts, there is clear evidence of progressive weakening of safeguard around the government's exemption granting authority. The Draft Data Protection Bill of 2018 confined exemptions to processing that was "authorised by law and as per the procedure established by law" thus grounding the invocation of this authority in a specified statutory basis and prescribed procedure, despite its shortcomings. The Personal Data Protection Bill of 2019 however relaxed this condition to some extent by allowing the Central Government to grant exemptions "by order" to specified agencies, while requiring such exemptions to be necessary or subject to certain procedural safeguards. But the DPDP Act, 2023 removes both of these protections, and the exemptions are granted by way of notification with no necessity condition or procedural safeguards. This gradual erosion, from requiring legal authority and necessity to

¹¹ Yash Verma, State Exemptions Under the Digital Personal Data protection Act, 2023: Testing Section 17(2)(a) Against the Proportionality Standard, 8 Indian J.L. & Legal Research (July 8, 2026), <https://www.ijllr.com/post/state-exemptions-under-the-digital-personal-data-protection-act-2023-testing-section-17-2-a-agai>

unrestricted notification power, is not just a change in successive drafts but reflects an expansion of executive discretion. The lack of procedural limitation when considered with Section 17(2) expansive grounds of “sovereignty, security, integrity, and public order” leaves the exemption power effective upon notification. The Central Government is not required to show proportionality, necessity, or compliance to any defined procedure before exempting itself or its instrumentalities from the provision of Act. This shows a reversal of safeguards provided in the 2018 and 2019 drafts. Instead of analysing Section 17 alone, this development over time shows that the Act marks a transition towards increasingly unaccountable executive power.¹²

The executive which is responsible for overseeing data processing of private entities can relax those same obligation for itself. Together, these provisions result in a two-tier data protection framework, one that binds private enterprises and ordinary data fiduciaries, and another where state enjoys limited oversight. Rather than balancing individual privacy and legitimate state interests, Section 17 favours state, creating the risk of unregulated data collection and surveillance by state fiduciaries.

4.4 APPLYING THE PROPORTIONALITY STANDARD

When assessed in the light of the proportionality standard, Section 17 only fulfils the first requirement of legality. Even though the exemption power derives from a duly enacted statute, the presence of a legitimate state interest cannot be assumed solely from the specification of grounds such as security, sovereignty, and public order. The provision does not mandate the government to show that the exemption is for legitimate state objective. The necessity condition is also weakened by the design of the exemption process. As the notification power is implemented without further approval procedure, there is no compulsory review to see whether exempting a whole State instrumentality from the Act, instead of specific condition, is required to achieve the objective. The balancing requirement is also compromised by the absence of procedural safeguards. As the provision lack periodic review and recording of reasons for allowing an exemption, it limits the scope for assessing whether the exemption remains justified over time and whether individual’s privacy interests are balanced against the State interests.¹³

¹² Anirudh Burman, Understanding India’s New Data Protection Law, Carnegie India (October 2023), <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law>.

¹³ Supra note [11]

4.5 THE DPDP RULES, 2025

The grounds provided in Section 17(1) parallels to those recognised in Article 19(2) of the Constitution, which have provided a basis for broad executive interpretation. The provision does not require the exemption to be limited, require recording of reason or independent overview and from the notification by Central Government alone, the exemption takes place. The DPDP Rules of 2025 does not cure this limitation. Rule 23 leaves the procedural requirements regulating government access to future notification instead of prescribing them within the Rule. The Second Schedule is limited to technical security safeguard and does not specify proportionality conditions or call for established link between an exempted activity and its stated objective. The Software Freedom Law Centre highlighted that the framework does not expressly include the proportionality and necessity condition laid down in Puttaswamy and the lack of independent oversight and judicial warrants restricts the individual from vindicating their privacy rights against the State processing. This is now the subject of ongoing litigation¹⁴. In *Chandresh Jain v. Union of India*, the Delhi High Court issued notice to the Central Government based on a PIL challenging Sections 17 to 21, 23, 29, 33, 34, 36, 37, and 44 of the Act, along with corresponding Rules on grounds of excessive executive control and sweeping State exemptions.¹⁵ A separate writ petition was filed by Venkatesh Nayak, an RTI activist, at the Supreme Court under Article 32 challenging Sections 17(1)(c), 17(2), 33(1), 36, and 44(3) of the Act, along with Rules 17 and 23(2) of the DPDP Rules, arguing that these provisions violates Articles 14, 19(1)(a), and 21 of the Constitution.¹⁶

V. SECTION 36 OF DPDP ACT: THE GOVERNMENT'S POWER TO CALL FOR INFORMATION

5.1 NATURE AND SCOPE

Section 36 of the DPDP Act, 2023 stipulates that the Central Government, for the purposes of the Act, can direct the Board and any intermediary or data fiduciary to provide such information as it may call for. The provision gives Central Government a direct statutory way of obtaining

¹⁴ Yatharth Chakravarty, The Structural Hole In India's Data Protection Law, Live Law (June 6, 2026), <https://www.livelaw.in/articles/digital-personal-data-protection-act-state-processing-without-consent-proportionality>.

¹⁵ *Chandresh Jain v. Union of India*, Delhi High Court (February 18, 2026), reported in Bhavini Srivastava, Delhi High Court Seeks response on PIL Against Digital Personal Data Protection Act, Bar & Bench (February 18, 2026), <https://www.barandbench.com/news/delhi-high-court-seeks-centres-response-on-pil-against-digital-personal-data-protection-act>.

¹⁶ *Venkatesh Nayak v. Union of India*, W.P. © no. 177/2026 (SC filed February 2, 2026)

the records maintained by the data processing entities instead of providing such power exclusively to the board.¹⁷ There is also inconsistency between the provision and the Bill's explanatory notes on clauses which described clause 36 as empowering the Board to call for information from any data fiduciary¹⁸. But in the enacted provision the power lies with the Central Government, extend to intermediaries and includes the Board among the entities that should furnish the information. This shift from the stated legislative intent redirects the power from a specialised regulator to the executive. Information under Section 36 is not defined. It may include audit logs, compliance reports, data-transfer details, breach records, security protocols, internal policies and anything the government may consider important for accountability, transparency and regulatory oversight. It is not clear what kind of information the government can gather. The phrase “for the purposes of this Act” is wide enough to support any request concerning data governance and the provision does not impose any limitation on the frequency of such demands. It is only provided that the request must satisfy the Act's objectives and should not be arbitrary.

Adherence to Section 36 is mandatory. Unreasonable delay, failure to comply or providing misleading information may result in legal action and penalties under other provisions of the Act, as Section 36 does not expressly prescribe such penalties. But at the same time, the Act also incorporates certain procedural safeguards, including opportunity for representation aimed to prevent arbitrary or excessive demands, even though the effectiveness of these safeguards in practice has yet to be examined once the Board is fully in effect.¹⁹ Section 36 does not operate by itself. It must be read with Section 37, under which the Central Government on receipt of a written reference from the Board intimating the imposition of monetary penalty on a data fiduciary in two or more instances and after giving an opportunity of being heard to such a data fiduciary, may, upon a direction of the Central Government, block access to information in the interest of the general public. Thus, Section 36 serves as a means for obtaining relevant facts, while Section 37 provides a means of acting upon them.²⁰ This seems to provide the government, subject to due process and the right to be heard, the power to direct intermediaries or agencies to block information in the public interest. This link is further strengthened by its relation with Information Technology (Procedure and Safeguards for Blocking for Access of

¹⁷ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 36 (India).

¹⁸ The Digital Personal Data Protection Bill, 2023, Bill No. 113 of 2023, Notes on Clauses, cl. 36, https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital%20Personal%20Data%20Protection%20Bill,%202023

¹⁹ Id note 16

²⁰ Digital Personal data Protection Act, 2023, No. 22 of 2023, S.37 (India)

Information by Public) Rules, 2009.²¹

The development of rules around this section is also worth noting. The DPDP Rules, 2025, along with the Seventh Schedule now lay down the purposes for which information may be obtained from intermediaries or Data Fiduciaries and the authorised person who may collect such information. The Draft Rules had tied this information sharing requirement to Section 36 of the DPDP Act, but in the final version, despite the obligation to give information remaining the same, the reference to Section 36 has been removed from the DPDP Rules. This can be seen as an important development as it may indicate that the government intends to ground the information gathering requirement more firmly in rule-based and purpose specific criteria instead of leaving it to open ended language used in Section 36.²²

The implementation time period is also important to understand Section 36. The Ministry of Electronics and Information Technology, on 14 November 2025, issued notifications bringing the DPDP Act and DPDP Rules into force with phased timelines and established the Data Protection Board in the National Capital Region with four members. Three dates, 13 November 2025, 13 November 2026, and 13 May 2027, were notified for commencement of provisions, with the substantive provisions of the Act and Rules coming into force in 18 months. This is important for Section 36 because it determines when the Central Government's information calling power becomes fully operative and when the machinery needs to exercise that in a structured way.²³

Finally, Section 36 must also be assessed in the contest of the Act's broad exemption power and India's constitutional privacy jurisprudence. The Act empowers the government to exempt its own agencies from its safeguards and it may collect and process an individual's personal data without complying with those safeguards, creating a risk of misuse. Section 36 read along with these exemptions raises concern due to the information demanding power with limited purpose specification and exemption of government fiduciaries from the very obligations it imposes on others.²⁴

²¹ Information Technology (procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, G.S.R. 781 (E) (India)

²² Digital Personal Data Protection Rules, 2025, G.S.R. 846 (E), r. 23 & Seventh Schedule (India, notified by the Ministry of Electronics and Information Technology (November 13, 2025)

²³ ed @ 19

²⁴ Supra note 16

5.2 SUPREME COURT CHALLENGES

The argument that Section 36 authorizes government to collect data without the data principal being informed is not simply inferential. Rule 23(2) of the DPDP Rules, 2025 implement Section 36 by mandating that a data Fiduciary or intermediary not disclose to the data principal that such information was provided to the government when the grounds of sovereignty, integrity or security of the State are invoked²⁵. The petitioners before the Supreme Court have argued that Section 36 creates a non-transparent government surveillance by obliging entities to provide any data that the Centre require and this gives the state unchecked power.²⁶

Writ petitions filed by RTI activist Venkatesh Nayak, the Reporters' Collective and journalist Nitin Sethi ²⁷ and by the National Campaign for People's Right to Information²⁸ challenge Section 36 read with Rule 23 of the DPDP Rules and Section 44(3) which rewrote Section 8(1)(j) of RTI Act. On 16 February 2026, bench comprising of Chief justice of India Surya Kant, Justice Joymalya Bagchi and Justice Vipul M. Pancholi issued notice to the Centre and referred the matter for further consideration.

VI THE DATA PROTECTION BOARD

6.1 COMPOSITION AND POWER

The Data Protection Board is a regulatory body established under the DPDP Act,2023 for implementing the data protection framework. The Board is comprised of a chairperson and other Members as appointed by the Central Government. The Chairperson and Members shall hold office for a term of two years and are eligible for reappointment. The board is empowered to inquire into breaches, adjudicate matters placed before it and impose penalties for non-compliance. It may also issue directive compelling data fiduciaries to undertake corrective actions. Penalties provided in the Act may extend to Rs 250 crore for specified breaches, making the Board an important enforcement authority under the data protection framework.²⁹

The Board plays a significant function in handling data breaches. When a breach occurs, the data fiduciary is required to notify the Board in compliance with the procedure provided under

²⁵ Digital Personal Data Protection Act,2023, No.22 of 2023, S 36 (India)

²⁶ Supra note 15

²⁷ The Reporters Collective Trust v. Union of India, W.P. (C) No. 211 of 2026

²⁸ National Campaign for People's Right to Info. v. Union of India, W.P. (C) No. 212 of 2026

²⁹ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.18-19 (India).

the DPDP Rules. The DPDP Rules, 2025 prescribed a 72-hour time limit from the time the data fiduciary becomes aware of the breach, while also giving the possibility of extension upon a written request from the data fiduciary. The Board is also empowered to hear complaints and references with respect to contraventions of the DPDP Act. The Board therefore deals with a wide range of violations, including failure to obtain consent, data security, compliance with requirements imposed on data fiduciaries and the exercise of rights by data principal. Although the framework presents the Board as an independent body, its design raises questions regarding the extent of its independence. The Central Government's position in appointing the Chairperson and members along with their limited tenure and eligibility for reappointment, may impact the Board's institutional autonomy. Since the Board exercises important investigative, adjudicatory and penal powers adequate safeguards for its independence is important to ensure impartial enforcement and to maintain public trust in the data protection framework.³⁰

Under Section 18, the Board exercise as an independent online body with its proceedings conducted fully online. It operates as an online mechanism for resolving complaints.³¹ Rule 19 of the DPDP Rules provides the procedures governing the Board's meetings, including quorum, voting, recusal in cases of conflict of interest, and emergency decision making through circulation or by the Chairperson. Thus, not every decision requires the full Board to sit together, as the Rules permit decisions to be taken by fewer members or by circulation in urgent matters.³²

6.2 JURISDICTION OF THE BOARD

The jurisdiction of the Board may be invoked by complaints from data principal, breach notifications or information received from other sources. In addition, the Board can also act *Suo motu*, allowing it to take actions without waiting for a formal complaint. It may call for information from data fiduciaries and conduct inquiries into alleged contraventions. Under Section 27, the Board may order discontinuation of unlawful processing and issue corrective orders. It also has authority to impose penalties separately or in addition to the corrective measures.³³ In important cases involving a significant risk of data loss or continuing breach, it

³⁰ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.19, S.21 (India).

³¹ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.18 (India).

³² Digital Personal Data Protection Rules, 2025, GSR 846 (E) rule 19 (India).

³³ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.27 (India).

may issue interim orders pending final adjudication. Under Section 28(7), the Board can exercise certain powers similar to those of a civil court and these include summoning and enforcing the attendance of persons, requiring the discovery and production of documents, receiving evidence through affidavits, and issuing commissions for the examination of witnesses or documents.³⁴

The Board's power to impose penalties is subject to the restrictions provided in Schedule I. The Board does not have rule making authority. It performs adjudicatory and enforcement functions rather than exercising broad powers associated with sectoral regulator. Even though the inquiries are required to be completed within six months from the date of the complaint, the period may be extended for another three months by recording reason. The Board is also required to follow the principles of natural justice, including providing an opportunity of hearing and recording reasons in writing³⁵. Section 39 restricts civil courts from entertaining suits or proceedings in respect of matters that comes under the Board's statutory jurisdiction. This gives the Board a degree of exclusivity over disputes assigned to it under the Act. Judicial decisions have also directed parties to pursue the statutory remedy before the Board rather than approaching the civil court directly.³⁶ A limitation arises with respect to Section 17, which provides exemptions for specified government agencies. When an exemption applies, the Board's power to scrutinise the relevant processing of personal data is restricted. Thus, although the Act establishes a broad jurisdiction, its practical reach is shaped by statutory exemptions.³⁷

6.3 EXECUTIVE CONTROL OVER APPOINTMENT AND REMOVAL OF MEMBERS OF BOARD

Under Section 19, the Central Government can appoint the Chairperson and Members of the Board through selection committees. A separate committee, chaired by the Cabinet Secretary, recommends candidates for the position of Chairperson, while a committee chaired by the Secretary of the Ministry of Electronics and Information Technology recommends candidates for members of board.³⁸ This appointment mechanism may affect the institutional independence of the Board, particularly when considered alongside of Central Government's

³⁴ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.28(7) (India).

³⁵ Digital Personal Data Protection Act, 2023, No. 22 of 2023, sch. 1 (India).

³⁶ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.38 (India).

³⁷ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.17 (India).

³⁸ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.19 (India).

broad exemption powers under Section 17.³⁹ Section 21 provides that the Chairperson or a member may be removed only on specified grounds. The concerned person must also be given an opportunity to be heard before removal. These safeguards provide a degree of protection and prevent the Central Government from removing Board members solely at its discretion.⁴⁰

6.4 LIMITATION

Despite the framework, the Board's adjudicatory powers are not yet operational. The Board was legally established with effect from 13 November 2025 with its composition fixed at chairperson and four Members. However, as of the latest reporting in July 2026, no Chairperson or Members were appointed with the recruitment process starting only in May 2026. Consequently, despite the institutional and appellate framework being legally in place, the Board is not currently exercising its adjudicatory jurisdiction in practice.⁴¹

VII CONCLUSION

Providing executive the power to exempt itself and to call for information should only be allowed by keeping individual privacy and State interest in balance. But under the DPDP Act this balance remains unresolved. The safeguard that would ordinarily accompany such power like requirement to show necessity, a limit on duration, an obligation to record reasons is largely absent which means the power is capable of being exercised on notification alone. The grounds on which exemption may be granted are the grounds the Constitution itself recognises as legitimate, so the underlying objective is not without basis, but in practice these same broad grounds allow entire State instrumentalities to be placed outside statutory oversight without the Government having to justify the decision in any particular case. Comparing this with earlier drafts of the legislation where exemption was tied more closely to necessity or specific statutory authorisation, shows that the present design is a choice made in drafting rather than something the subject matter makes unavoidable. This raises a fair question, whether complete exemption of an entire instrumentality, rather than a condition narrowly tied to the processing actually involved, is necessary at all. There is a deeper structural problem underlying both provisions, the Central Government controls the grant of exemption, the exercise of the information calling power, and also the appointment of members to the very body that might

³⁹ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.17 (India).

⁴⁰ Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.21 (India).

⁴¹ Ministry of Electronics & Info. Tech., Circular No. F. No. 2(1)/2026-Pers.I (May 6, 2026) (India), <https://www.meity.gov.in/static/uploads/2026/05/cd481c027470b420b4cb85fb40a91c53>

otherwise be expected to review both. This concentration of authority is itself a source of the insufficiency this paper has tried to identify and addressing it should come before any narrower fix. Setting clearly defined grounds for exemption, requiring reasons to be recorded and made available for review, fixing a limited duration subject to renewal, and insulating the reviewing body's appointment from the government it is meant to oversee, would together move the framework closer to the safeguard the Constitution demands.

In short, exemption and information gathering power under the DPDP Act should not operate as an ordinary tool of administration. It should be granted only after careful scrutiny, tested against the same standard of necessity and proportionality the Constitution requires of any interference with privacy and treated as a measure of last resort rather than the default position from which executive power proceeds.