IN THE HON'BLE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (C) NO. 275 of 2026

(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

[PUBLIC INTEREST LITIGATION]

IN THE MATTER OF:

GEETA SESHU & ANR …PETITIONERS

VERSUS

UNION OF INDIA & ORS. …RESPONDENTS

IA NO. 66957 OF 2026

APPLICATION SEEKING EX-PARTE INTERIM RELIEF

{PAPER BOOK}

{FOR INDEX KINDLY SEE INSIDE}

==========

ADVOCATE FOR THE PETITIONERS:

PARAS NATH SINGH

Dated the 19th February 2026

==========

INDEX

RECORD OF PROCEEDINGS

S.NO.	PARTICULARS	DATES
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		

Index

S. No	Particulars of documents	Page number of parts to which its belongs		Remark
		Part - I [Contents of Paper Book]	Part - II [Contents of fine alone]	
(i)	(ii)	(iii)	(iv)	(v)
1.	Listing proforma	A1 – A2	A1 – A2	
2.	Cover page of paper book		A3	
3.	Index of Record of Proceedings		A4	
4.	Limitation Report of Proceedings		A5	
5.	Defects list		A6	
6.	Note sheets			
7.	Synopsis and List of Dates	**B- Q**		
8.	Writ Petition along with Affidavit	1 - 108		
9.	Appendix: Article 32 of the Constitution of India	109		
10.	**ANNEXURE P-1** A true copy of representation/comments nil dated sent by the Petitioner No. 2 to the Respondents	110-140		

11.	**ANNEXURE P-2** A true copy of the Digital Personal Data Protection Act, 2023 notified on 11.8.2023	141-161		
12.	**ANNEXURE P-3** A true copy of the Digital Personal Data Rules 2025 issued vide Notification No. G.S.R. 846 (E) dated 13.11.2025	162-179		
13.	**ANNEXURE P-4** A true copy of the Report titled "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", by Justice B.N. Srikrishna Committee	180-392		
14.	**ANNEXURE P-5** A true copy of the Personal Data Protection Bill, 2018	393-459		
15.	**ANNEXURE P-6** A true copy of the Personal Data Protection Bill, 2019	460-516		
16.	**I.A. No. of 2026** Application for ad-interim relief	517-521		
17.	Vakalatnama along with copy of Board Resolution	522-524		
18.	Filing Memo	525		

A1

PROFORMA FOR FIRST LISTING

SECTION:

This case pertains to (Please tick/ check the correct box):

☐	Central Act: (Title)	The Constitution of India
☐	Section :	Article 32
☐	Central Rule : (Title)	……N.A.
☐	Rule No(s)	……..N.A.
☐	State Act: (Title)	……N.A.
☐	Section :	……N.A.
☐	State Rule : (Title)	……N.A.
☐	Rule No(s):	……N.A.
☐	Impugned Interim Order : (Date)	……N.A
☐	Impugned Final Order /Decree : (Date)	NA
☐	High Court : (Name)	NA
☐	Names of Judge(s):	NA
☐	Tribunal/Authority : (Name)	

1.	Nature of the matter	☐ ☐	**CIVIL**
2.	a) Petitioner/Appellant		**GEETA SESHU**
	b) Email I.D.		……N.A.
	c) Mobile phone number:		……N.A.
3.	a) Respondent No.		**Union of India**
	b) Email I.D.		N/A
	c) Mobile phone number:		N/A
4.	a) Main category classification		1807
	b) Sub classification :		18
5.	Not to be listed before:		-N.A.-
6(a).	Similar disposed of matter with citation, if any and case Details		No Similar Disposed Matter
6(b).	Similar pending matter with case details		WP(C) No.177 of 2026 WP(C) No.212 of 2026
7.	**Criminal Matters**:		
	a) Whether accused /convict has surrendered:		NA
	b) FIR No Date	NA	
	c) Police Station:	NA	

A2

d) Sentenced awarded NA

e) Period of Sentence undergone including period of detention/ custody undertaken: NA

f) Whether any earlier case between the same parties is filed NA

g) Particulars of the FIR and Case NA

h) Whether any bail application was preferred earlier and decision thereupon

8. **Land Acquisition Matters:** .....N/A
   a) Date of Section 4 notification : .....N/A
   b) Date of Section 6 notification : .....N/A
   c) Date of Section 17 notification .....N/A

9. **Tax Matters**: State the Tax effect: .....N/A

10. **Special Category**: (first petitioner/ appellant only):
    ☐ Senior citizen > 65 years ☐ SC/ST ☐ Woman /child
    ☐ Disabled ☐ Legal ☐ Aid case ☐ in custody

11. Vehicle Number (in case of Motor Accident Claim matters) : **N/A**

12. Whether there was/is litigation on the same point of law, if yes, details thereof: **NO**

Date:

B

SYNOPSIS

1. The Petitioners herein are constrained to approach this Hon'ble Court under Article 32 of the Constitution of India as against to the Digital Personal Data Protection Act, 2023 (*hereinafter referred to as the* **"DPDP Act"**) and its corresponding Digital Personal Data Protection Rules, 2025 (*hereinafter referred to as the* **"DPDP Rules"**) (*collectively referred to as the* **"DPDP Laws"**). The present petition challenges the DPDP Laws as a constitutional regression from the fundamental right to privacy recognised by this Hon'ble Court in ***Justice K. S. Puttaswamy (Retd.)* v. *Union of India*** 2017 (10) SCC 1 (*hereinafter referred to as* **"Puttaswamy"**). While enacted under the ostensible objective of protecting personal data, the DPDP Laws in effect legalize disproportionate State surveillance, create a compensation vacuum for citizens, dilute the Right to Information, erode the ability of journalists to practice their profession, and establish a data protection regulator that is structurally dependent upon the Executive.

2. The Petitioners submit that the DPDP Laws depart materially from the principles recommended by the **Committee of Experts under the Chairmanship of Justice B.N. Srikrishna** (*hereinafter referred to as the* **"B.N. Srikrishna Committee Report"**), disregard the doctrine of proportionality, and violate Articles 14, 19(1)(a), 19(1)(g), 21, and 21A of the Constitution of India. The DPDP Laws provide unchecked exemptions for the State, permit indefinite retention, remove the individual's right to compensation for data breaches, erode the ability of journalists to engage in independent and impartial reporting, and concentrates adjudicatory power in a non-independent Data Protection Board of India (*hereinafter referred to as the* **"DPB"**).

C

3. The present Petition seeks the striking down of unconstitutional provisions as the primary relief, along with consequential directions to restore constitutional safeguards, judicial oversight, and effective remedies. For the better perusal of this Hon'ble Court, the Petitioners' contentions have been categorised into five prongs, namely, (i) Lack of Exemptions for Journalistic Purposes (ii) Constitutionality of the Data Processing by the State and the Overbroad Powers to Exempt Instrumentalities of the State, (iii) Compensation Vacuum, (iv) Lack of Independence of the Data Protection Board (DPB), and (v) Surveillance. The said categorisation is detailed hereinafter:

(I) Lack of Exemptions for Journalistic Purposes:

4. This chapter challenges the lack of journalistic exemptions under the DPDP Laws, which in effect, prevents journalists from carrying out their work in an independent manner and erodes the fourth pillar of democracy.

5. The fourth pillar of democracy needs to have the freedom to engage in reporting that is unbiased, informative and of public importance. The nature of journalism today requires the usage of technology and collaboration with concerned citizens, researchers, civil society organizations and similar stakeholders for the processing and analysis of documents and data.

6. The DPDP Laws in their current form do not provide any exemptions for the processing of data for journalistic purposes. Due to the current iteration of the DPDP Laws that have been brought into effect, journalists and similar stakeholders will be categorized as Data Fiduciaries due to their collection of data and personal details in the ordinary course of their duties. Journalists and similar

D

stakeholders would now need to undertake onerous data protection compliances in the discharge of their duties whenever they process any data or personal details. Additionally, since data fiduciaries require the consent of data principals in order to process their data, journalists will no longer be able to report on stories that are unfavourable to data principals without first providing their notice of the intended use of their personal data and seeking that data principal's consent, effectively stifling the ability to provide fair and impartial reportage. Further, data principals can now retroactively retract their consent for the processing of their personal data and seek the erasure of the personal data stored with journalists, which can include published reportage and private notes containing data, which in turn limits the ability of the public to conduct post facto verification of the underlying data of published reportage.

7. Significantly, Parliament was aware of this issue, having created carve-outs for data processing requirements for information used for journalistic purposes. The Personal Data Protection Bill, 2018, the Personal Data Protection Bill, 2019 and the Joint Parliamentary Committee's Report, 2021 made specific exemptions from data compliance requirements for the use of data for journalistic purposes. Even at the international level, the EU GDPR's Article 85 and the Brazilian LGPD's Article 4 have codified exemptions from data processing compliance requirements for data and information that is used for journalistic purposes, further highlighting the DPDP Laws' deviation from the norm.

8. In the absence of any exemptions for the use of data for journalistic purposes, the DPDP Laws in their current form violate the

E

fundamental right of journalists to carry on their profession under Article 19(1)(g) of the Constitution.

(II) Constitutionality of the Data Processing by the State and the Overbroad Powers to Exempt Instrumentalities of the State:

9. This chapter challenges the constitutional validity of Sections 7(c) and 17(2)(a) of the DPDP Act. Under these provisions, the State possesses unchecked powers to direct Data Fiduciaries to undertake personal data processing of Indian citizens in a legal vacuum — in which none of the data protection principles prescribed under the DPDP Laws will be applicable to such processing. Furthermore, the DPDP Laws empower the Central Government with unfettered discretion to bypass the data protection principles outlined in the DPDP Act and the DPDP Rules. Additionally, data protection standards established under the Second Schedule of the DPDP Rules create a parallel framework that is unenforceable, allowing the State to obviate data protection principles such as lawful processing, fairness, transparency, informed consent, purpose limitation, data minimisation, storage limitation and reasonable security safeguards.

10. Section 7(c) of the DPDP Act outlines certain legitimate uses, where one of the uses allows a Data Fiduciary to process personal data for the State and any of its instrumentalities for provisioning or issuing to the Data Principal such subsidy, benefit, service, certificate, licence or permit — as prescribed under Rule 5 of the DPDP Rules.

11. Under the garb of certain legitimate uses, Section 7(c) allows the State to obviate data protection requirements for lawful processing and consent if a Data Principal has previously consented to such

F

data processing. Irrespective of the legitimate interests of the State or a Data Fiduciary, any data processing must be subject to the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation, and reasonable security safeguards outlined in the DPDP Laws. Section 17(2)(a) of the DPDP Act allows the Central Government unfettered discretion to exempt any of its instrumentalities from the application of the provisions of the DPDP Laws.

12. The DPDP Laws eliminate the crucial balance between protecting the fundamental right to privacy and the legitimate interests of the State. Instead of subjecting the State's power to process personal data to the constitutional limits, the DPDP Laws exacerbate the underlying privacy risks of mass surveillance programmes. In the absence of judicial oversight and any other procedural safeguards, the DPDP Laws fail the standards of necessity and proportionality by allowing the State to accumulate an indefinite (in terms of variety and quantity) amount of sensitive personal data through mass surveillance programmes. Furthermore, it not only obviates the established principles of the DPDP Act but also lacks clear and enforceable standards to prevent extraneous data processing by the State.

(III) Compensation Vacuum:

13. This chapter challenges the constitutional validity of the repeal and omission of Section 43A of the Information Technology Act, 2000 (*hereinafter referred to as the* **"IT Act"**), and the consequent failure of the DPDP Act to provide any equivalent or effective civil

G

remedy to individuals whose personal data is unlawfully processed or breached.

14. Section 43A represented the only statutory embodiment of a compensatory privacy remedy in Indian law prior to the DPDP regime. It imposed liability on body corporates for failure to implement reasonable security practices and entitled affected individuals to compensation for wrongful loss or wrongful gain. Though limited and fragmented, it constituted a crucial rights-restorative mechanism and a deterrent against negligent data handling.

15. The DPDP Laws under Section 33 dismantle this remedial architecture entirely. While the DPDP Act Schedule introduces a penalty-centric framework with fines running into hundreds of crores, such penalties are payable exclusively to the Consolidated Fund of India through Section 34 of the DPDP Act. The data principal whose privacy is violated receives no compensation, restitution, or restoration, even in cases involving identity theft, financial fraud, reputational harm, or dignitary injury.

16. This shift from a rights-based compensatory model to a State-centric penalty model creates a constitutionally impermissible vacuum. A fundamental right to privacy, recognised under Article 21, cannot be rendered remediless through legislative design. The absence of compensation particularly undermines the enforcement of privacy rights against both private and State actors, weakens deterrence, and prioritises State's fiscal considerations over individual dignity.

17. This chapter therefore contends that the repeal of Section 43A, without the enactment of a comparable or superior civil remedy,

H

violates Article 21, fails the doctrine of proportionality, and represents a regressive rollback of privacy protections in India's constitutional framework.

(IV) Lack of Independence of the Data Protection Board (DPB)

18. This chapter challenges the constitutional validity of Rules 17, 18, and 21 along with the Fifth and Sixth Schedules to the DPDP Rules, and Section 24 of the DPDP Act. The DPDP Act establishes the DPB as a statutory adjudicatory body empowered under Chapter VI of the DPDP Act to inquire into contraventions, adjudicate complaints, issue binding directions, and impose monetary penalties. As per the judicial pronouncement of this Hon'ble Court in ***Rojer Mathew* v. *South Indian Bank Limited represented by its Chief Manager and Others*** (2020) 6 SCC 1, "*50. ...the procedure of appointment and conditions of service of members must be akin to judges...*"

19. However, the DPDP Laws do not prescribe a transparent or judicially insulated appointment mechanism, do not confer administrative autonomy upon the DPB, and do not provide statutory safeguards to ensure independence from executive influence. The DPDP Laws vest pervasive control over the constitution, appointment of members, staffing, service conditions, and functioning of the DPB, with the Central Government:

- Rule 17 of the DPDP Rules provides that the Search-cum-Selection Committee for appointment of the Chairperson and Members of the DPB is constituted by the Central Government, and that appointments are made by the Central Government on the basis of such recommendations.

- Rules 18 and 21 of the DPDP Rules further place the salaries, allowances, and service conditions of the Chairperson, Members, officers, and employees of the DPB under executive control. The Fifth Schedule subjects the Chairperson and Members to the Central Civil Services (Leave) Rules, 1972 and the Central Civil Services (Classification, Control and Appeal) Rules, 1965, assimilating them into the executive civil-service framework.

- Rule 21 read with the Sixth Schedule restricts the DPB's ability to appoint officers and staff by requiring prior approval of the Central Government and limiting recruitment primarily to deputation from government-controlled entities. Residual and undefined service conditions are required to be referred to the Central Government, whose decision is final. Section 24 of the DPDP Act provides for the same prior approval requirement from the Central Government.

20. Under the DPDP Act, the Central Government and its instrumentalities are classified as Significant Data Fiduciaries, and complaints against them may be adjudicated by the DPB under Section 27 of the DPDP Act. Consequently, the Central Government could be a litigating party to proceedings before the DPB while simultaneously retaining decisive control over its appointments, staffing, and service conditions. Such an institutional arrangement raises concerns regarding the independence and impartiality of the adjudicatory framework, particularly in cases involving the Central Government. There is a catena of decisions from this Hon'ble Court requiring that executive control must be

removed for tribunals to be independent, especially if the government is contemplated to be a litigation party before the tribunal.

21. In contrast, established data protection regimes in comparative jurisdictions expressly secure the independence of data protection authorities through statutory provisions. This includes the European Union under the General Data Protection Regulation (*hereinafter referred to as the* "**EU GDPR**"), Brazil under the *Lei Geral de Proteção de Dados* (LGPD) (General Data Protection Law) through the National Data Protection Authority (ANPD), and the State of California under the California Privacy Rights Act through the California Privacy Protection Agency. In each of these regimes, independence of the data protection authority is institutionally recognised and protected through legislation, particularly in relation to appointments, tenure, staffing, and freedom from executive influence.

22. Further, the scheme governing the DPB, multiple statutory tribunals and quasi-judicial bodies in India incorporate judicial oversight as part of their constitution and appointment processes either through mandatory consultation with the Chief Justice of India, or through the inclusion of a member of the Judiciary in the Selection Committee. Further, these tribunals often include both judicial and technical members to ensure judicial oversight is balanced with technical expertise, and their parent statutes often prescribe minimum years of experience and require prior judicial office for key positions. By contrast, Section 19(3) of the DPDP Act prescribes broad and undefined eligibility criteria for the Chairperson and Members of the DPB, without mandating judicial experience, minimum years of professional practice, or

demonstrable expertise in privacy and data protection law. The constitution and appointment mechanism itself is primarily effectuated through delegated legislation under Rule 17 of the DPDP Rules, rather than being comprehensively detailed in the parent statute.

(V) Surveillance:

23. This Chapter challenges the constitutional validity of Section 36 of the DPDP Act, along with its enabling provisions under Rule 23 and the Seventh Schedule of the DPDP Rules. These provisions grant the Central Government the power to compel the DPB, any Data Fiduciary or an intermediary, to furnish information that may be called for, and create a parallel regime of *de facto* interception and surveillance in India. The provisions lack sufficient legal and procedural safeguards to protect individual civil liberties, and thus create a chilling effect on the right to freedom of speech in the country. The provisions lack the basic requirements of oversight, guardrails to prevent abuse, and any statutorily imposed timelines for deletion of records, and negate the idea of privacy as a whole.

24. The provisions are violative of this Hon'ble Court's judgment in ***People's Union for Civil Liberties (PUCL)* v. *Union of India***, (1997) 1 SCC 301, (*hereinafter referred to as* **"PUCL"**) where this Hon'ble Court held that the "*occurrence of any public emergency*" or "*in the interest of public safety*" are the *sine qua non* for interception. The impugned provisions fly explicitly in the face of the judgment, making no mention of the only two constitutionally permissible conditions, i.e., public order and the interest of public safety, held permissible for conducting interception. The DPDP Laws instead place reliance on "*the interest of sovereignty and integrity of India or security of the State*", which were held to be

L

explicitly invalid conditions for interception, barring the presence of situations of violations of public order and public safety.

25. The provisions are also violative of the right to privacy and fail the proportionality standard as laid down in ***Puttaswamy***. This Hon'ble Court held that where the State intends to infringe upon the right to privacy or aims to interfere, the interference must pass the proportionality test. The test states that (1) The action must be sanctioned by law; (2) The proposed action must be necessary in a democratic society for a legitimate aim; (3) The extent of such interference must be proportionate to the need for such interference; (4) There must be procedural guarantees against abuse of such interference.

26. The DPDP Laws' provisions fail on multiple counts. First, by permitting state action without establishing the existence of mandatory pre-conditions of a public emergency or public safety conditions as laid down in the PUCL judgment, the provisions fail to meet the first criteria, i.e., a threshold requirement of legality. Further, the Central Government is granted overbroad and unchecked power to compel any Data Fiduciary or an intermediary to hand over information on the grounds of "the interest of sovereignty and integrity of India or security of the State". This power is neither democratic nor legitimate in the absence of situations demanding emergent actions or having the element of public safety concerns. Without adequate safeguards or limiting guidelines, these grounds are inherently broad and vague, leaving them susceptible to potential misuse. Therefore, the provisions do not meet the second limb of the proportionality test. Notably, Section 69 of the IT Act, read with the Information Technology (Procedure for Safeguards for Interception, Monitoring and

M

Decryption of Information) Rules, 2009 (*hereinafter referred to as the* **"Interception Rules, 2009"**) prescribe similar measures for interception and surveillance, with detailed safeguards and procedures to ensure that such interception and surveillance does not carry on unchecked. However, the DPDP Laws override an existing parallel framework in the Interception Rules, 2009 that is heavily guarded by safeguards; essentially creating a method of interception with close to no oversight which encourages arbitrary state action. Importantly, no safeguards similar to the Interception Rules, 2009 are prescribed under the impugned provisions of the DPDP Laws. Emphasisingly, it is also pertinent to note that the existence of Interception Rules, 2009 *ipso facto* do away with the necessity prong of *Puttaswamy* test, thereby making the requirement of impugned provisions of the DPDP Laws obsolete and illegal in the eye of the law.

27. In the absence of legality, necessity, proportionality, or procedural safeguards, the provisions also fail all four prongs of the Puttaswamy test and are therefore liable to be struck down on the grounds that they are violative of Article 21 and the Right to Privacy guaranteed thereunder. The existence of Section 36 of the DPDP Act is solely incumbent of it being subject to the Section 69 of IT Act read with the Interception Rules, 2009, wherein all the tests and safeguards are necessarily followed under Section 36 as well.

28. Hence, the instant writ petition

LIST OF DATES

DATES	PARTICULARS

17/10/2000	The Information Technology Act, 2000 (IT Act) came into force vide Notification No. G.S.R.788(E) issued by the Ministry of Information Technology, Government of India. The IT Act laid the foundational legal framework for electronic commerce and cyber offences in India.
05/02/2009	Section 43A was introduced into the IT Act through the Information Technology (Amendment) Act, 2008, creating a civil compensation regime for failure to protect sensitive personal data.
11/04/2011	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were notified vide Notification G.S.R. 313(E) issued by the Ministry of Communications and Information Technology ("**MeitY**"), operationalising Section 43A.
31/07/2017	The B.N. Srikrishna Committee of Experts on a Data Protection Framework for India was constituted by the Union of India in the wake of this Hon'ble Court's judgment in *Justice K.S.Puttaswamy (Retd.) v. Union of India and Ors*, 2017 (10) SCC 1.
27/07/2018	The B.N. Srikrishna Committee released its Report titled 'A Free and Fair Digital Economy - Protecting Privacy and Empowering Citizens.' The Report made recommendations on various issues such as: • The establishment of a Data Protection Agency in the nature of a high-powered, sector-agnostic, independent national body corporate with the following functions: (1) monitoring and enforcement; (2) legal affairs,

O

	policy and standard setting; (3) research and awareness; and (4) inquiries, grievance handling and adjudication. • The creation of a system for selecting members of the Data Protection Authority in a fair and transparent manner, especially as it was expected that government agencies will be regulated as data fiduciaries under the data protection law, with a selection committee consisting of a judicial representative as well as a subject matter expert in addition to officials from the Central Government. • The setting up of a separate and independent Adjudication Wing for the Data Protection Authority consisting of Adjudicating Officers with subject-matter expertise, and of a dedicated appellate tribunal set up to hear and dispose of any appeals from the orders of the Data Protection Authority and the orders of the Adjudicating Officers. • The strict adherence of the data protection law to the judgment of the Hon'ble Supreme Court in *Puttaswamy*, and with adequate safeguards, to enable an exemption to the processing of personal or sensitive personal data only if it is proportionate and necessary in the interest of the security of the state and is pursuant to a law that meets the test of constitutionality. • The design of the current legal framework in India is responsible for according a wide remit to intelligence and law enforcement agencies. At the same time, it lacks sufficient legal and procedural safeguards to protect individual civil liberties. Much intelligence-

P

	gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammeled rise of a surveillance society. There is no general law in India today that authorises non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are carrying out activities of such a nature without statutory authorisation (for example, solely through executive authorisation), such activities would be illegal as per the Puttaswamy judgment as they would not be operating under law. • The creation of a law to deal with the question of oversight of intelligence gathering, providing for both parliamentary oversight as well as judicial approval of all requests for non-consensual access to personal data, so that the data protection principles may be implemented effectively. • The inclusion of exemptions from data processing obligations for journalistic activities due to the onerous obligations this would place on journalists and the possibility that mandating consent would result in unfavourable accounts against data principals not being published. The B.N. Srikrishna Committee also released the draft of the Personal Data Protection Bill, 2018 on the same day.
11/12/2019	The Personal Data Protection Bill, 2019 ("**2019 Bill**") was introduced in the Lok Sabha. The Bill was referred to a Joint Parliamentary Committee on the same day.

Q

16/12/2021	The Joint Parliamentary Committee submitted its Report on 2019 Bill, and renamed it to the Data Protection Bill, 2021.
03/08/2022	The Data Protection Bill, 2021 was withdrawn by the Central Government.
18/11/2022	The Digital Personal Data Protection Bill, 2022 was published by MeitY.
11/08/2023	The Digital Personal Data Protection Act, 2023 was enacted, repealing the application of Section 43A of the IT Act without providing an equivalent compensatory remedy.
13/11/2025	The Digital Personal Data Protection Rules, 2025 were notified by the Central Government, along with a phased notification of certain provisions of the Digital Personal Data Protection Act, 2023.
19.02.2026	Hence, the present Writ Petition.

IN THE HON'BLE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (C) NO. 275 of 2026

(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

[PUBLIC INTEREST LITIGATION]

IN THE MATTER OF:

Geeta Seshu

...Petitioner No. 1

Software Freedom Law Center, India

...Petitioner No. 2

VERSUS

Union of India
Through its Secretary
Ministry of Law and Justice,
Shastri Bhawan, New Delhi - 110001 **...Respondent No. 1**

Ministry of Electronics and Information Technology (MeitY)
Through Secretary (Electronics and Information Technology),
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003 **...Respondent No. 2**

Ministry of Home Affairs
Represented through Home Secretary,
North Block,
New Delhi - 110001 **...Respondent No. 3**

A WRIT PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA SEEKING ISSUANCE OF AN APPROPRIATE WRIT, ORDER OR DIRECTION, FOR QUASHING AND SETTING ASIDE SECTIONS 7, 17(2)(a), 24, 36, 44(2)(a) AND 44(3) OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND RULES 5, 6, 17, 18, 21 AND 23, AND THE SECOND, FIFTH, SIXTH AND SEVENTH SCHEDULES OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025, TO THE EXTENT CHALLENGED HEREIN, AND FOR ISSUANCE OF APPROPRIATE DIRECTIONS INCLUDING A WRIT IN THE NATURE OF MANDAMUS TO SECURE THE PROTECTION AND ENFORCEMENT OF FUNDAMENTAL RIGHTS GUARANTEED UNDER PART III OF THE CONSTITUTION OF INDIA.

To,
THE HON'BLE CHIEF JUSTICE OF INDIA AND
HIS COMPANION JUSTICES OF THE HON'BLE SUPREME COURT OF INDIA.

HUMBLE PETITION OF THE
PETITIONERS ABOVE-NAMED

MOST RESPECTFULLY SHOWETH:

1. PRELIMINARY SUBMISSIONS

1.1. The instant writ petition in the public interest is being filed under Article 32 of the Constitution of India seeking an appropriate writ, order, or direction to:

a) Strike down Sections 7, 17(2)(a), 24, 36, 44(2)(a) and 44(3) of the Digital Personal Data Protection Act, 2023, to the extent challenged herein;

b) Strike down Rules 5, 6, 17, 18, 21 and 23 and the Second Schedule, Fifth Schedule, Sixth Schedule and Seventh Schedule of the Digital Personal Data Protection Rules, 2025, to the extent challenged herein;

c) Strike down Section 17(2)(a) of the Digital Personal Data Protection Act, 2023, insofar as it empowers the Central Government to exempt any of its instrumentalities from the application of the provisions of the DPDP Act and the DPDP Rules;

d) Strike down Section 44(2)(a) of the Digital Personal Data Protection Act, 2023, insofar as it extinguishes the right of affected persons to seek compensation or civil remedy for unlawful processing of personal data and/or data breach;

e) Issue an appropriate writ, order or direction, quashing and setting aside Section 44(3) of the Digital Personal Data Protection Act, 2023 insofar as it dilutes the right to information of the citizens of India.

f) Strike down Section 24 of the Digital Personal Data Protection Act, 2023 read with Rules 17, 18 and 21 and the Fifth and Sixth Schedules of the DPDP Rules, 2025, insofar as they relate to the

constitution, appointment, service conditions and functioning of the Data Protection Board of India;

g) Issue a writ in the nature of mandamus directing the Respondents to frame and notify a constitutionally compliant mechanism for appointment, tenure and service conditions of the Data Protection Board of India, ensuring its independence from executive control;

h) Strike down Section 36 of the Digital Personal Data Protection Act, 2023 read with Rule 23 and the Seventh Schedule of the DPDP Rules, 2025;

i) Issue a writ in the nature of mandamus directing the Respondents to incorporate and notify a specific and proportionate exemption under the DPDP Act and DPDP Rules for processing of personal data for journalistic, editorial, investigative and public interest reporting purposes, including protection of journalistic sources.

2. DETAILS OF THE PARTIES AND DECLARATIONS BY THE PETITIONER:

2.1. That, Petitioner No. 1 is a Senior Journalist and a co-founder of the Free Speech Collective. She is a citizen of India. The present Petitioner No. 1 herein furnishes details with respect to the present PIL, which are as follows: PAN details: Aadhaar Number: Email: Mobile No.

Annual Income around INR and it is also submitted that there is no criminal, civil, or revenue litigation pending against Petitioner No. 1 before before this Hon'ble Court or any other Court.

2.2. That, Petitioner No. 2 is a society registered under the Societies Registration Act, 1860, bearing registration number dated 03/03/2010, that works for the promotion and protection of digital rights and digital freedoms. The present Petitioner No. 2 herein furnishes details with respect to the present PIL, which are as follows: PAN details: Contact No. Annual Income between INR and it is also submitted that there is no criminal, civil, or revenue related litigation pending against the Petitioner No. 2 before this Hon'ble Court or any other Court.

2.3. That Petitioner No. 2 relies on donations from Indian philanthropists, institutional donors, small donations from individual professionals like lawyers, engineers, journalists, and corporate social responsibility funds of corporations.

2.4. That Petitioner No. 2 has broad experience addressing threats to human rights in the digital realm, working alongside civil society organizations and other stakeholders across the globe. Petitioner No. 2 is the sole Indian organization to be inducted in IFEX (International Freedom of Expression and Exchange), the largest network of global free expression organizations consisting of 100 member

organisations, spanning 70 countries, and committed to collaboration and transformative advocacy. In 2022, Petitioner No. 2 was given Special Consultative Status from the Economic and Social Council of the United Nations (ECOSOC). Since its inception in 2010, Petitioner No. 2 has done a range of work from litigating to protect digital freedoms to conducting empirical research which could lead to policy change. The Petitioner No. 2 is duly represented through its Treasurer, who has been authorised by the Governing Board of the Society.

2.5. Respondent No. 1 is the Union of India, represented through the Ministry of Law and Justice, which is responsible for making rules essential for legislative affairs and is concerned with the enactment and implementation of laws affecting the fundamental rights of citizens, including the Digital Personal Data Protection Act, 2023.

2.6. Respondent No. 2, the Ministry of Electronics and Information Technology (MeitY), is the nodal ministry of the Central Government responsible for formulating and implementing policies relating to information technology and digital governance in India. Respondent No. 2 is also the administrative ministry responsible for the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, including their implementation and enforcement.

2.7. Respondent No. 3, the Ministry of Home Affairs, is responsible for matters relating to internal security,

public order, law enforcement coordination, and national security. Respondent No. 3 is also concerned with the functioning of law enforcement and security agencies which process personal data, and is therefore a necessary party in view of the impugned provisions of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 which enable broad State processing of personal data and exemptions in favour of government instrumentalities.

2.8. It is stated that all the Respondents are 'State' within the meaning of Article 12 of the Constitution of India and thus the Writ Petition against them is maintainable.

CAUSE OF ACTION

2.9. The cause of action arose when the Respondents notified the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 on 11.08.2023 and 13.11.2025 respectively.

2.10. Even though the Digital Personal Data Protection Act, 2023 was passed by Parliament on 11/08/2023, it was formally brought into force only on 13.11.2025, once the Digital Personal Data Protection Rules, 2025 were brought into effect, with its provisions being brought into effect in a phased manner over an 18-month period.

NATURE OF INJURY

2.11. The nature of injury caused to the public is the violation of fundamental rights of the citizens under Articles 14, 19(1)(a), 19(1)(g), 21 and 21A of the Constitution of India.

2.12. The Petitioners have no personal gain, private motive, or any such reason whatsoever in filing the present Writ Petition, and the same is in the Public Interest. The Petitioners are approaching this Hon'ble Court with clean hands, and the sole intention is to address the larger public concern.

2.13. There is no civil, criminal, or revenue litigation involving the Petitioners that has or could have a legal nexus with the issues involved in the present Public Interest Litigation.

2.14. It is submitted that the Petitioners also participated in the consultative process and offered their comments in response to the draft Digital Personal Data Protection Rules, 2025. That the Petitioners have the requisite locus to file the present public interest litigation. It is further submitted that there is no other effective and expeditious alternative remedy available to the Petitioners except by filing the present petition under Article 32 of the Constitution of India. A true copy of representation/comments sent by the Petitioner No. 2 to the Respondents is annexed herewith and marked as **ANNEXURE P-1 (Pg.No. 110 to 140)**

3. FACTS LEADING TO THE PRESENT PETITION

3.1. That the Petitioners herein are a journalist and civil society organization respectively who are aggrieved

by the unconstitutional nature of certain provisions of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") and its corresponding Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") (collectively, "**DPDP Laws**"). A true copy of the Digital Personal Data Protection Act, 2023 notified on 11.8.2023 is annexed herewith and marked as **ANNEXURE P-2 (Pg.No. 141 to 161)**. A true copy of the Digital Personal Data Rules 2025 issued vide Notification No. G.S.R. 846 (E) dated 13.11.2025 is annexed herewith and marked as **ANNEXURE P-3 (Pg.No. 162 to 179)**

3.2. That, in 2017, this Hon'ble Court recognized the fundamental right to privacy in its seminal ***Puttaswamy*** judgment.

3.3. The judgment acted as the impetus for the Union of India to establish the B.N. Srikrishna Committee, comprising ten experts in the field of data and privacy laws. The B.N. Srikrishna Committee published its report on 27/07/2018 wherein it made recommendations on various issues such as:

A. The establishment of a Data Protection Authority in the nature of a high-powered, sector-agnostic, independent national body corporate with the following functions: (1) monitoring and enforcement; (2) legal affairs, policy and standard setting; (3) research and awareness; and (4) inquiries, grievance handling and adjudication.

B. The creation of a system for selecting members of the Data Protection Authority in a fair and transparent manner, especially as it was expected that government agencies will be regulated as data fiduciaries under the data protection law, with a selection committee consisting of a judicial representative as well as a subject matter expert in addition to officials from the Central Government.

C. The setting up of a separate and independent Adjudication Wing for the Data Protection Authority consisting of Adjudicating Officers with subject-matter expertise, and of a dedicated appellate tribunal set up to hear and dispose of any appeals from the orders of the Data Protection Authority and the orders of the Adjudicating Officers.

D. The strict adherence of the data protection law to the judgment of the Hon'ble Supreme Court in *Puttaswamy*, and with adequate safeguards, to enable an exemption to the processing of personal or sensitive personal data only if it is proportionate and necessary in the interest of the security of the state and is pursuant to a law that meets the test of constitutionality.

E. The design of the current legal framework in India is responsible for granting broad authority to intelligence and law enforcement agencies. At the same time, it lacks sufficient legal and procedural safeguards to protect individual civil

liberties. Much intelligence-gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammeled rise of a surveillance society. There is no general law in India today that authorises non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are carrying out activities of such a nature without statutory authorisation (for example, solely through executive authorisation), such activities would be illegal as per the Puttaswamy judgment as they would not be operating under law.

F. The creation of a law to deal with the question of oversight of intelligence gathering, providing for both parliamentary oversight as well as judicial approval of all requests for non-consensual access to personal data, so that the data protection principles may be implemented effectively.

G. The inclusion of exemptions from data processing obligations for journalistic activities due to the onerous obligations this would place on journalists and the possibility that mandating consent would result in unfavourable accounts against data principals not being published. A true copy of the Report titled "A Free and Fair

Digital Economy Protecting Privacy, Empowering Indians", by Justice B.N. Srikrishna Committee is annexed herewith and marked as **ANNEXURE P-4 (Pg.No. 180 to 392)**

3.4. That the present Petition has been filed after the Petitioners herein have approached the concerned authorities on numerous occasions and sent several representations seeking clarifications regarding the concerns with DPDP Laws.

(I) Lack of Exemptions for Journalistic Purposes

3.5. The field of journalism today requires the usage of technology for the processing and analysis of documents and data. The journalistic profession generally involves carrying out investigations and research that collect, store, process and publish sensitive data that is of public importance. Journalists also frequently work with concerned citizens, civil society organizations and other stakeholders who help them in the collection and sometimes processing of this sensitive data, which can result in important investigations that hold power to account.

3.6. The DPDP Laws in their current form do not provide any exemptions for the processing of data for journalistic purposes. Section 2(i) of the DPDP Act defines a "Data Fiduciary" as "*any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data*". Section 4 of the DPDP Act allows a person to process

the personal data of a Data Principal either (a) for which the Data Principal has given their consent; or (b) for certain legitimate uses. Section 5, in turn, requires that the data fiduciary give notice to the data principal of the personal data and the purpose for which it is being processed. Section 7 of the DPDP Act provides a list of the legitimate uses for which a Data Fiduciary may process a Data Principal's personal data, which does not include journalistic or public purpose.

3.7. Given the nature of their work, under the current iteration of the DPDP Laws, journalists, media organizations and similar stakeholders will be categorized as Data Fiduciaries by default, due to their collection and processing of data and personal details in the ordinary course of their duties. Media organizations, journalists and similar stakeholders would now need to undertake onerous data protection compliances in the discharge of their duties whenever they process any data or personal details.

3.8. Additionally, as set out above, since journalistic or public purposes are not specified as one of the legitimate uses under the DPDP Act, data fiduciaries require the consent of data principals in order to process their data. Resultantly, journalists, media organizations and similar stakeholders will no longer be able to report on issues that are unfavourable to Data Principals without obtaining that Data Principal's affirmative consent first, effectively stifling the ability of journalists and concerned

citizens to provide fair and impartial reportage on issues of public importance.

3.9. Further, the ability granted to data principals to retroactively withdraw their consent to the processing of their data under Section 12 of the DPDP Act imperils any reportage that may portray the data principal in a negative light, effectively violating journalists and similar stakeholders' fundamental right of free speech and expression under Article 19(1)(a) and their fundamental right to carry on their profession under Article 19(1)(g).

3.10. Significantly, Parliament was aware of this issue, having created carve-outs for data processing requirements for information used for journalistic purposes.

3.11. The Personal Data Protection Bill, 2018, expressly included a reservation for the use of data for journalistic purposes. The proposed Section 47 of the Personal Data Protection Bill, 2018 excluded the applicability of the obligations imposed by the other provisions for journalistic purposes, barring the proposed Sections 4 (fair and reasonable processing) and 31 (security safeguards).

3.12. The Personal Data Protection Bill, 2019 and the Joint Parliamentary Committee's Report, 2021 made similar specific exemptions from data compliance requirements for the use of data for journalistic purposes, subject to compliance with the Personal Data Protection Bill, 2019 and its accompanying rules, the code of ethics issued by the Press Council

of India or any statutory media regulatory organization.

3.13. Even at the international level, the EU GDPR's Article 85 and the Brazilian LGPD's Article 4 have codified exemptions from data processing compliance requirements for data and information that is used for journalistic purposes, further highlighting the DPDP Laws deviation from the norm. Article 85 of the EU GDPR states that:

> "*Processing and freedom of expression and information*
>
> 1. *Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.*
> 2. *For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.*
> 3. *Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.*"

3.14. Similarly, Brazil's LGPD states as follows:

> "*Article 4. This law shall not apply to the processing of personal data that:*
>
> *...*
>
> *II. is carried out exclusively for:*
>
> a. *journalistic or artistic purpose...*"

3.15. Section 17 read with Part 2 of the First Schedule of Singapore's Personal Data Protection Act, 2012 permits news organizations to collect, use and disclose personal data about an individual without their consent when it relates to news activity.

3.16. In the absence of any exemptions for the use of data for journalistic purposes, the DPDP Laws in their current form violate the fundamental right of journalists to carry on their profession under Article 19(1)(g) of the Constitution. Further, the lack of these exemptions also violate the right to freedom of speech and expression of journalists and similar stakeholders as enshrined under Article 19(1)(a) of the Constitution.

3.17. That the Petitioners have no other equally efficacious remedy and are thus invoking the jurisdiction of this Hon'ble Court under Article 32 of the Constitution of India to vindicate their fundamental rights under Articles 14, 19(1)(g), 21, and 21A.

(II) Constitutionality of the Data Processing by the State and the Overbroad Powers to Exempt Instrumentalities of the State

3.18. In 2017, this Hon'ble Court in ***Puttaswamy*** recognised the right to privacy as a fundamental right

under Article 21 of the Constitution. The Hon'ble Court established the proportionality test to determine the constitutionality of privacy-infringing measures — where a State measure interferes with the right to privacy, it is only constitutional when it satisfies the requirements of: (i) legality, the measure is authorised by statute; (ii) legitimate goal, the measure pursues a proper purpose; suitability, (iii) the measure takes meaningful steps towards achieving the proper purpose; (iv) necessity, the measure is the least rights-restrictive measure amongst equally effective alternatives; (v) proportionality, the measure does not disproportionately impact individual rights; and (vi) procedural safeguards, the measure incorporates meaningful guardrails against possible abuse.

3.19. Section 7 of the DPDP Act outlines certain legitimate uses, where sub-clause (c) prescribes unfettered powers to the State and any of its instrumentalities to process personal data for the performance of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or the security of the State.

3.20. Section 17(2)(a) of the DPDP Act allows the Central Government with unfettered discretion to exempt any of its instrumentalities from the application of the provisions of the DPDP Laws.

3.21. The State possesses unchecked powers to undertake personal data processing of Indian citizens in a legal vacuum, in which none of the data protection principles prescribed under the DPDP Laws will be

applicable to such processing. Furthermore, Section 17(2)(a) empowers the State with unfettered discretion to bypass the data protection principles outlined in the DPDP Act and the DPDP Rules.

3.22. In addition to the lack of procedural safeguards, such expansive powers fail the tests of necessity and proportionality established by this Hon'ble Court in ***Puttaswamy***. Furthermore, the DPDP Laws fail to create an enforceable framework to hold the State accountable for unlawful data processing through mass surveillance programs. Such provisions are liable to be struck down as they violate the fundamental rights and freedom enshrined within Articles 21, 19(1)(a) and 14 of the Constitution.

(III) Compensational Vacuum

3.23. The Information Technology Act, 2000 ("IT Act") was enacted to provide legal recognition to electronic transactions and to address emerging cyber harms. However, for nearly a decade after its enactment, the statute lacked any meaningful mechanism to address harms arising from negligent handling of personal data.

3.24. Recognising this lacuna, Parliament introduced Section 43A into the IT Act through the Information Technology (Amendment) Act, 2008. Section 43A created a civil liability regime whereby any body corporate handling sensitive personal data was required to implement "reasonable security practices and procedures".

3.25. Section 43A provided that where a body corporate failed to maintain such reasonable security practices, resulting in wrongful loss or wrongful gain to any person, it would be liable to pay compensation to the affected individual. This marked the first statutory recognition in Indian law of data breach–linked personal harm.

3.26. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (*hereinafter referred to as the* "**2011 SPDI Rules**") were subsequently notified to operationalise Section 43A. These Rules defined "sensitive personal data", prescribed baseline security standards, and created an enforceable framework for civil claims.

3.27. Although the Section 43A regime was limited in scope and suffered from enforcement deficiencies, it nonetheless served as the sole civil remedial pathway for individuals whose personal data was compromised due to negligence.

3.28. In 2017, this Hon'ble Court, in ***Puttaswamy***, recognised the right to privacy as a fundamental right under Article 21. The Hon'ble Court expressly acknowledged informational privacy and warned against the dangers of unaccountable data processing and surveillance.

3.29. Following the ***Puttaswamy*** judgment, the Justice B.N. Srikrishna Committee of Experts on a Data Protection Framework for India was constituted to recommend a comprehensive data protection framework. The

Committee emphasised that effective remedies, including compensation, were indispensable to the enforcement of privacy rights.

3.30. Despite these recommendations, the DPDP Act consciously omitted any provision analogous to Section 43A. Instead, it introduced a penalty-based framework wherein monetary sanctions are imposed by the Data Protection Board of India and credited entirely to the State.

3.31. With the notification of the DPDP Rules, the DPDP Act has been fully operationalised. Simultaneously, the legacy framework under Section 43A and the 2011 SPDI Rules stands effectively extinguished.

3.32. Under the present regime, an individual whose personal data is leaked, misused, or exposed has no statutory right to claim compensation, regardless of the magnitude of harm suffered. Even large-scale breaches affecting millions of citizens result only in penalties payable to the State treasury.

3.33. This represents a fundamental shift from a victim-centric remedial model to a State-centric enforcement model, wherein the individual data principal is reduced to a mere informant rather than a rights-holder.

3.34. The absence of compensation is particularly grave in cases involving non-material harm such as emotional distress, loss of reputation, loss of autonomy, and fear of future misuse of personal data—harms that are intrinsic to privacy violations.

3.35. The phased implementation of the DPDP Act has further exacerbated this vacuum. During the transition period, individuals are left without the protections of the repealed Section 43A regime and without the benefit of any new compensatory mechanism.

3.36. The cumulative effect of these developments is that the right to privacy, though constitutionally recognised, is rendered practically unenforceable in the absence of a remedy. The data principal bears the harm, while the State appropriates the penalty.

3.37. The Petitioners submit that this remedial void violates Article 21 of the Constitution, undermines the rule of law, and constitutes a regressive dilution of privacy protections that warrants the urgent intervention of this Hon'ble Court.

(IV) Lack of Independence of the Data Protection Board (DPB)

3.38. Prior to the enactment of the DPDP Act, India did not have a comprehensive data protection statute or a single, unified data protection regulator. Governance of personal data was undertaken through a fragmented framework consisting of sector-specific regulators like the TRAI, for example.

3.39. The Justice B.N. Srikrishna Committee, in its Report, had recommended the enactment of a comprehensive data protection law accompanied by the establishment of a statutory, independent Data Protection Authority (DPA), which was proposed to be a single, sector-agnostic central regulatory body vested with wide

powers for investigation, monitoring, imposition of penalties, and adjudication of violations. It was further recommended that the DPA must be insulated from executive interference through some statutory safeguards, including the creation of a system for selecting members of the Data Protection Authority in a fair and transparent manner, especially as it was expected that government agencies will be regulated as data fiduciaries under the data protection law, with a selection committee consisting of a judicial representative as well as a subject matter expert in addition to officials from the Central Government.

3.40. The Personal Data Protection Bill, 2019 incorporated some of the Committee's recommendations by proposing a statutory Data Protection Authority consisting of a Chairperson and multiple Members, and possessing a wide gamut of powers under Sections 49(2)(a)-(o) of the Bill, as well as the power of search and seizure.

3.41. However, the Selection committee that would appoint the Chairperson and the Members to the DPA was populated entirely by officials from the Central Government, and the Joint Parliamentary Committee Report, 2021, suggested that members of the selection committee should also include: (i) the Attorney General of India, (ii) an independent expert from fields such as data protection, information technology, or cyber laws, and (iii) Directors of an IIT and an IIM, or include judicial representatives,

highlighting the need for independence as mentioned in the B.N. Srikrishna Committee Report.

3.42. This is in line with established data protection regimes in comparative jurisdictions, which expressly secure the independence of data protection authorities through statutory provisions. This includes the European Union under the EU GDPR, Brazil under the Lei Geral de Proteção de Dados LGPD) (General Data Protection Law) through the National Data Protection Authority (ANPD), and the State of California under the California Privacy Rights Act through the California Privacy Protection Agency. In each of these regimes, independence of the data protection authority is institutionally recognised and protected through legislation, particularly in relation to appointments, tenure, staffing, and freedom from executive influence.

3.43. In August 2023, Parliament enacted the DPDP Act. The DPDP Act departed materially from the earlier legislative drafts by replacing the proposed "Data Protection Authority" with a body titled the "Data Protection Board of India" as a statutory body and assigns to it certain adjudicatory and enforcement functions, including the power to inquire into specified contraventions and impose monetary penalties in defined circumstances. Unlike the PDP Bill, 2019 and the Srikrishna Committee's recommendations, the DPDP Act does not provide detailed statutory safeguards concerning the independence of the DPB.

3.44. To the contrary, the DPDP Act read with the DPDP Rules vests pervasive control over the constitution, appointment of members, staffing, service conditions, and functioning of the DPB, with the Central Government:

A. Rule 17 of the DPDP Rules provides that the Search-cum-Selection Committee for appointment of the Chairperson and Members of the DPB is constituted by the Central Government, and that appointments are made by the Central Government on the basis of such recommendations.

B. Rules 18 and 21 of the DPDP Rules further place the salaries, allowances, and service conditions of the Chairperson, Members, officers, and employees of the DPB under executive control. The Fifth Schedule subjects the Chairperson and Members to the Central Civil Services (Leave) Rules, 1972 and the Central Civil Services (Classification, Control and Appeal) Rules, 1965, assimilating them into the executive civil-service framework.

C. Rule 21 read with the Sixth Schedule restricts the DPB's ability to appoint officers and staff by requiring prior approval of the Central Government and limiting recruitment primarily to deputation from government-controlled entities. Residual and undefined service conditions are required to be referred to the Central Government, whose decision is final.

Section 24 of the DPDP Act also requires prior approval of the Central Government for the Board to appoint officers and employees.

3.45. Under the DPDP Act, the Central Government and its instrumentalities are classified as Significant Data Fiduciaries, and complaints against them may be adjudicated by the DPB under Section 27 of the DPDP Act. Consequently, the Central Government is a litigating party before the DPB while simultaneously retaining decisive control over its appointments, staffing, and service conditions.

3.46. In contrast to the DPB, multiple statutory tribunals and quasi-judicial bodies in India incorporate judicial oversight in the constitution and appointment of the Chairpersons and Members, through their governing statutes by (i) mandating consultation with the Chief Justice of India for such appointments, or (ii) mandating the inclusion of sitting or former judges in the Search-cum-Selection Committee. Examples include the Central Administrative Tribunal (*hereinafter referred to as the "***CAT***"*), Competition Commission of India (*hereinafter referred to as the* **"CCI"**), National Green Tribunal (*hereinafter referred to as the "***NGT***"*), National Company Law Tribunal (*hereinafter referred to as the* **"NCLT"**), and the National Company Law Appellate Tribunal (*hereinafter referred to as the* **"NCLAT"**).

3.47. Some quasi-judicial bodies like the NCLT, the NGT, and the CAT further ensure judicial oversight through statutory requirements that a judicial member sit on

the tribunal itself along with a technical or expert member.

3.48. The appointment procedure of the DPB also differs from the above-mentioned statutory tribunals and quasi-judicial bodies in that it is effectuated through delegated legislation, under Rule 17 of the DPDP Rules, 2025. For all the above-mentioned tribunals and quasi-judicial bodies except for Judicial and Expert Members of the NGT, the appointments of the Chairperson and Members were effectuated solely through the parent legislation.

3.49. Further, the qualifications listed for the Chairperson and Members of the DPB under Section 19(3) of the DPDP Act, 2023, are sparse and do not prescribe any minimum for years of experience unlike the qualifications listed for the above-mentioned statutory tribunals and quasi-judicial bodies.

(V) Surveillance

3.50. In 2017, this Hon'ble Court, in ***Puttaswamy***, recognised the right to privacy as a fundamental right under Article 21. This Hon'ble Court expressly acknowledged informational privacy and warned against the dangers of unaccountable data processing and surveillance.

3.51. Following ***Puttaswamy***, the Justice B.N. Srikrishna Committee was constituted to recommend a comprehensive data protection framework. The Committee stated that "*there is a vacuum in checks and balances to prevent the untrammeled rise of a*

surveillance society." It further stated that "*Surveillance should not be carried out without a degree of transparency that can pass the muster of the Puttaswamy test of necessity, proportionality and due process. This can take various forms, including information provided to the public, legislative oversight, executive and administrative oversight and judicial oversight. This would ensure scrutiny over the working of such agencies and infuse public accountability*."

3.52. The power to call for information under Section 36 of the DPDP Act is a new addition, when compared to the previous iterations of the draft data protection bills that were considered by the Central Government.

3.53. The previous iterations in fact, highlighted such powers of surveillance as a harm, as can be seen in the Personal Data Protection Bill, 2018, which covered both restrictions suffered due to surveillance, as well as surveillance which would not be expected by Data Principals under the definition of 'harm'. The same was carried forward in the Personal Data Protection Bill, 2019. The Joint Parliamentary Committee Report, 2021, on Data Protection, while commenting on the 2019 Bill specified that the Government's surveillance on data stored in India must be strictly based on necessity as laid down in the legislation, and that the same must be incorporated into the text of the Bill. The Data Protection Bill 2021, consequently included surveillance as a harm identified. A true copy of the Personal Data

Protection Bill, 2018 annexed herewith and marked as **ANNEXURE P-5 (Pg.No. 393 to 459)**. A true copy of the Personal Data Protection Bill, 2019 is annexed herewith and marked as **ANNEXURE P-6 (Pg.No. 460 to 516)**

3.54. There was a marked shift when the DPDP Act was notified, with Section 36 granting powers to the Central Government to require the DPB, any Data Fiduciary, or intermediary to furnish such information as it may call for.

3.55. Rule 23 of the DPDP Rules, which operationalised Section 36, further state that where the disclosure of furnishing of information is likely to prejudicially affect the sovereignty and integrity of India or security of the State, the Central Government may require the Data Fiduciary or intermediary to not disclose such furnishing to the affected Data Principal or any other person except with the previous permission, in writing, of the authorised person.

3.56. The Seventh Schedule of the DPDP Rules elaborated upon the reasons for which information may be required to be furnished:

Sr. No.	Purpose	Authorized Person
1	Use, by the State or any of its instrumentalities, of personal data of a Data Principal in the interest of sovereignty and integrity of India or security of the State.	Such officer of the State or of any of its instrumentalities notified under clause (a) of sub-section (2) of section 17 of the Act, as the Central Government or the head of such

		instrumentality, as the case may be, may designate on this behalf.
2	Use, by the State or any of its instrumentalities, of personal data of a Data Principal for the following purposes, namely: — (i) performance of any function under any law for the time being in force in India; or (ii) disclosure of any information for fulfilling any obligation under any law for the time being in force in India.	Person authorised under applicable law.
3	Carrying out assessment for notifying any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary.	Such officer of the Central Government, in the Ministry of Electronics and Information Technology, as the Secretary in charge of the said Ministry may designate on this behalf.

3.57. The present provisions lack any legislative oversight, executive and administrative oversight and judicial oversight. Further, they introduce opacity, and deny information to affected data principals under Rule 23.

3.58. There exist provisions for similar measures to be carried out under Section 69 of the IT Act, read with Interception Rules, 2009.

3.59. Section 69 of the IT Act and the Interception Rules, 2009 mandate safeguards and procedures to ensure that such interception and surveillance does not carry on unchecked.

3.60. The directions for interception or monitoring or decryptions shall be issued by the competent authority as per Rule 3 of the Interception Rules, 2009. The competent authority as defined under Rule 2(d) means the Secretary in the Ministry of Home Affairs in the case of the Central Government and the Secretary in-charge in the Home Department in the case of the State Government or Union Territory. No person other than the competent authority can issue such orders. However, in unavoidable circumstances, such orders may be issued by an officer not below the rank of Joint Secretary to the Government of India who has been duly authorised by the competent authority.

3.61. Rule 8 of the Interception Rules, 2009 provides that the competent authority shall consider alternative means of acquiring the information before issuing such directions. Rule 10 of the Interception Rules, 2009 prescribes that the directions issued under Rule 3 shall specify the name and the designation of the officer of the authorised agency and the use of the information disclosed.

3.62. Rule 11 of the Interception Rules, 2009 provides that the directions issued shall remain in force for a period not exceeding sixty days, but they can be renewed from time to time for a period not exceeding the total of one hundred and eighty days.

3.63. Rule 22 of the Interception Rules, 2009 provides for the Review Committee and mentions that the Review Committee shall meet once in two months to review the directions issued under Rule 3 and record its

findings whether they are in accordance with Rule 3 read with Section 69(2) of IT Act or not. Where the Committee is of the opinion that the directions are not in accordance with the provisions, it shall set aside the directions and may order the destruction of the copies including the corresponding electronic records of the intercepted or monitored or decrypted information.

3.64. No such safeguards exist under Section 36 of the DPDP Act or the DPDP Rules. The consequent effect is that the provisions violate the Right to Privacy guaranteed under Article 21 of the Constitution, that warrant the the urgent intervention of this Hon'ble Court.

3.65. That the only foreseeable scenario where Section 36 of the DPDP Act read with Rule 23 and Seventh Schedule of the DPDP Rules can exist is where the same is read with and guided by Section 69 of the IT Act read with the Interception Rules, 2009. The lack of safeguards and thorough procedure under the DPDP Laws make it susceptible to abhorrent misuse and leaves the provision up to the whims and fancies of the Central Government.

4. GROUNDS

(I) LACK OF JOURNALISTIC EXEMPTIONS

A. BECAUSE the DPDP Act deliberately fails to provide an exemption for the collection, processing, and publication of data which is processed for journalistic purposes. This results in journalists and

similar stakeholders engaged in collecting, processing and analyzing data being categorized as 'data fiduciaries' as defined under Section 2(i) of the DPDP Act. This, in turn, imposes onerous compliance obligations upon journalists and similar stakeholders under Section 8 and potentially Section 10 of the DPDP Act, and can curtail their ability to report on issues dealing with the data of private or public individuals , since this may constitute personal data. Such measures curtail the abilities of journalists to carry on their profession, violating their fundamental rights under Article 19(1)(g) of the Constitution.

B. BECAUSE Section 7 of the DPDP Act permits the processing of a Data Principal's personal data for a specified list of "legitimate uses", with journalistic or public purposes not featuring on this list. As a result of this, Section 4 of the DPDP Act permits journalists and similar stakeholders to process a Data Principal's personal data only with their affirmative consent. This prevents journalists and similar stakeholders from collecting, processing and disclosing personal data of subjects of investigative reporting, unless they obtain the subject's consent first. Given the necessity of disclosing information of public importance, having to obtain the consent of the subject of the reportage may, in many cases, defeat the very purpose of the reportage itself. Further, if the subject refuses to give their consent for the processing of their personal data, it prevents

journalists from publishing information that can be of significant public importance.

C. BECAUSE Section 5 of the DPDP Act imposes an additional onerous obligation upon journalists and similar stakeholders seeking to collect, process and publish data even if they seek to obtain the consent of a data principal. Section 5(1)(i) of the DPDP Act requires that every request for consent to a data principal would require a data fiduciary to give the data principal a notice informing them of the personal data being processed and the purpose for which the data is being processed. Specifying the purpose for which the data principal's consent is being obtained would prevent journalists and similar stakeholders from being able to process data that may not show the data principal in a positive light in subsequent reporting. While implementing this provision, the DPDP Act effectively neuters the ability of journalists and similar stakeholders to investigate matters of public importance that may show private or public individuals in a negative, albeit truthful, light. Further, at the beginning of an investigation, journalists and concerned citizens may not be in a position to specify a suitably comprehensive "purpose" for processing the data, since the very nature of journalism can result in an investigation uncovering something of a much larger scale than originally envisaged.

D. BECAUSE Section 8 read with Sections 4 and 5 of the DPDP Act imposes onerous obligations on journalists and similar stakeholders who are considered to be data fiduciaries, including (i) giving notice to and obtaining the consent of data principals to process their personal data; (ii) implementing technical and organizational measures to ensure compliance with the DPDP Laws; (iii) ensuring reasonable safeguards to prevent personal data breaches; (iv) inform the Data Protection Board and each affected data principal in the event of a breach; (v) erase personal data when the data principal withdraws their consent or when the specified purpose is no longer being served; (vi) implement a grievance redressal mechanism for data principals; (vii) appoint a Data Protection Officer or a representative to address any questions raised by data principals about the processing of their personal data.

E. BECAUSE journalists and similar stakeholders are also at risk of being categorized as a Significant Data Fiduciary by the Executive under Section 10 of the DPDP Act, based on relevant factors such as (i) the volume and sensitivity of the personal data processed; (ii) risk to the rights of data principals; (iii) potential impact on the sovereignty and integrity of India; (iv) risk to electoral democracy; (v) security of the State; and (vi) public order. Being designated as a Significant Data Fiduciary imposes additional obligations on an individual or

organization such as (i) being required to appoint a Data Protection Officer, (ii) being required to appoint an independent data auditor to carry out data outs; and (iii) undertake measures such as a periodic Data Protection Impact Assessment and a periodic audit.

F. BECAUSE Section 12 of the DPDP Act permits a data principal to seek the deletion of their personal data from processing for which they had previously consented and the data fiduciary is obligated to erase their personal data unless retention is required for the specified purpose or for compliance with any law in force. Further, Rule 8(3) of the DPDP Rules directs a data fiduciary to erase personal data, associated traffic data and other processing logs after one year of processing, unless further retention is required for compliance with any other law. These provisions of the DPDP laws would require journalists and similar stakeholders to delete all information related to personal data, including already published online reportage. Further, forcing the deletion of the personal data on the withdrawal of the data principal's consent or after one year from the date of processing would make archival and subsequent verification of that reportage next to impossible, unless the data collection and processing is repeated from the beginning, which may not always be possible.

G. BECAUSE Parliament itself has considered the importance of including exemptions for data processing for journalistic purposes, as is evidenced by Section 47 of the Personal Data Protection Bill, 2018, Section 36(e) of the Personal Data Protection Bill, 2019 and Section 36(e) of the Data Protection Bill, 2021.

H. BECAUSE the current iteration of the DPDP Act runs contrary to international standards that permit the processing of personal data subject to journalistic purposes. Article 85 of the EU GDPR recognizes this by directing Member States to reconcile the right to personal data protection with the right to freedom of expression and information, including processing for journalistic purposes. In the case of ***Sergejs Buivids*** **v.** ***Datu Valsts Inspekcija*** (National Data Protection Agency, Latvia) (Case C-345/17), the CJEU interpreted 'journalistic purpose' and 'journalism' in a broad manner, including within their fold independent journalists and digital creators if the sole purpose for processing the data was to disclose information, opinions, and comments to the public. Further, the data protection laws of both Brazil and Singapore also include specific exemptions for the collection, processing and disclosure of personal data without obtaining the data principal's consent when dealing with journalistic matters.

(II) CONSTITUTIONALITY OF THE DATA PROCESSING BY THE STATE AND THE OVERBROAD POWERS TO EXEMPT INSTRUMENTALITIES OF THE STATE

I. BECAUSE the extant framework envisaged under the DPDP Laws is violative of the fundamental right to privacy, as recognized by this Hon'ble Court in ***Justice K.S. Puttaswamy (Retd.)*** **v.** ***Union of India,*** (2017) 10 SCC 1. Through the DPDP Laws, the State possesses unchecked powers to direct Data Fiduciaries to undertake personal data processing of Indian citizens in a legal vacuum, in which none of the data protection principles prescribed under the DPDP Laws will be applicable to such processing. Furthermore, the DPDP Laws empower the State with unfettered discretion to bypass the data protection principles outlined in the DPDP Act and the DPDP Rules. Additionally, the data protection standards established under the Second Schedule of the DPDP Rules create a parallel framework that is unenforceable, allowing the State to obviate data protection principles such as lawful processing, fairness, transparency, informed consent, purpose limitation, data minimisation, storage limitation and reasonable security safeguards.

J. BECAUSE Section 7 of the DPDP Act outlines certain legitimate uses, where sub-clause (c) prescribes unfettered powers to the State and any of its instrumentalities to process personal data for the

performance of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or the security of the State..

K. BECAUSE Section 7(c) of the DPDP Act unduly expands the power of the State to collect, process and retain an indiscriminate amount of personal data of Indian citizens. Under the garb of certain legitimate uses, Section 7(c) allows the State to obviate data protection requirements for lawful processing and consent if a Data Principal has previously consented to such data processing. Irrespective of the legitimate interests of the State or a Data Fiduciary, any data processing must be subject to principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation and reasonable security safeguards outlined in the DPDP Laws. Further, the Second Schedule prescribes data protection standards that are at best vague and do not contain any effective procedural safeguards. In absence of sufficient guardrails, the Data Principal has no legal avenue to challenge arbitrary or extraneous data processing by the State and any of its instrumentalities. In the *Puttaswamy* judgment, this Hon'ble Court had forewarned the necessity of safeguards in human rights and data protection frameworks and its possible implications on technology-facilitated mass surveillance,

> *"122 The flip side is the concern over the abuse of new technology, including biometrics, by the State and private entities by actions such as surveillance and large-scale profiling. This is particularly acute, given the fact that technological advancements have far outpaced legislative change. As a consequence, the safeguards necessary to ensure protection of human rights and data protection are often missing. The lack of regulatory frameworks, or the inadequacy of existing frameworks, has societal and ethical consequences and poses a constant risk that the concepts of privacy, liberty and other fundamental freedoms will be misunderstood, eroded or devalued."*

L. BECAUSE Section 17(2)(a) of the DPDP Act allows the Central Government unfettered discretion to exempt any of its instrumentalities from the application of the provisions of the DPDP Laws.

M. BECAUSE the extant framework eliminates the crucial balance between protecting the fundamental right to privacy and the legitimate interests of the State. Under Section 17(2)(a) of the DPDP Act, State possesses unfettered discretion to exempt any of its instrumentalities from the data protection obligations envisaged under the Act and the Rules. In the *Puttaswamy* judgment, this Hon'ble Court had held that –

> *"180 While it intervenes to protect legitimate state interests, the state must nevertheless put into place a robust regime that ensures the fulfilment of a three-fold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). They emanate from the procedural*

and content-based mandate of Article 21. The first requirement that there must be a law in existence to justify an encroachment on privacy is an express requirement of Article 21. For, no person can be deprived of his life or personal liberty except in accordance with the procedure established by law. The existence of law is an essential requirement. Second, the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness. Legitimacy, as a postulate, involves a value judgment. Judicial review does not re-appreciate or second guess the value judgment of the legislature but is for deciding whether the aim which is sought to be pursued suffers from palpable or manifest arbitrariness. The third requirement ensures that the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law. Hence, the three-fold requirement for a valid law arises out of the mutual inter-dependence between the fundamental guarantees against arbitrariness on the one hand and the protection of life and personal liberty, on the other. The right to privacy, which is an intrinsic part of the right to life and liberty, and the freedoms embodied in Part III are subject to the same restraints which apply to those freedoms."

N. BECAUSE the DPDP Laws allow the State unfettered powers to operate and potentially expand

the scope of mass surveillance programs. Such programs can be deployed to collect massive amounts of sensitive personal data, based on vague grounds such as 'in the interests 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'. As per this Hon'ble Court's order in ***Manohar Lal Sharma (Pegasus Spyware)*** **v.** ***Union of India***, (2023) 11 SCC 401, the State cannot resort to expansive surveillance regimes and such measures would be subject to judicial review. In light of binding precedents, this Hon'ble Court had held that:

> *"49. ...It is a settled position of law that in matters pertaining to national security, the scope of judicial review is limited. However, this does not mean that the State gets a free pass every time the spectre of "national security" is raised. National security cannot be the bugbear that the judiciary shies away from, by virtue of its mere mentioning. Although this Court should be circumspect in encroaching upon the domain of national security, no omnibus prohibition can be called for against judicial review."*

O. BECAUSE the DPDP Laws fail to address the underlying privacy risks of mass surveillance programmes that do not adhere to the constitutional values of transparency, accountability and fairness. In the absence of judicial oversight, the DPDP Laws fail to restrict the State's power to accumulate an indefinite (in terms of variety and quantity) amount

of sensitive personal data through mass surveillance programmes. Furthermore, it not only obviates the established principles of the DPDP Act but also lacks clear and enforceable standards to prevent extraneous data processing by the State. In a Report titled "*A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*", the Justice B.N. Srikrishna Committee had opined that:

> *"The design of the current legal framework in India is responsible for according to a wide remit to intelligence and law enforcement agencies. At the same time, it lacks sufficient legal and procedural safeguards to protect individual civil liberties. Much intelligence-gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammeled rise of a surveillance society. There is no general law in India today that authorises non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are carrying out activities of such a nature without statutory authorisation (for example, solely through executive authorisation), such activities would be illegal as per the Puttaswamy judgment as they would not be operating under law."*

P. BECAUSE the Central Government has executed three major surveillance projects namely Central Monitoring System (**"CMS"),** Network Traffic Analysis (**"NETRA"**) and National Intelligence Grid (**"NATGRID"**), which collectively and

separately seek to spy on the communications of citizens in India. The aforementioned projects allow government agencies to intercept and monitor any and all telecom and internet communications in bulk, furthering the process of construction of a mass illegal dragnet surveillance system by the State. Rather than establishing any substantive legal thresholds to limit arbitrary measures that are violative of the fundamental right to privacy, the DPDP Laws allow the State and any of its instrumentalities to sustain and expand mass surveillance projects like CMS, NETRA and NATGRID. The DPDP Laws fail to satisfy the standards of necessity, proportionality and to establish adequate procedural safeguards to protect Indian citizens from the imminent threat to privacy owing to mass surveillance programmes.

Q. BECAUSE there is no limit to the kind of personal data that can be processed for the performance of any function and under any law or in the interest of "sovereignty and integrity of India or security of the State". The State processes an incalculable amount of personal data of Indian citizens which may variously include, location records, call records, financial transactions, travel records, which can enable mass surveillance of each Indian citizen in real-time. In doing so, it can identify and reveal intimate details about an individual's life — religious affiliations, political beliefs, sexual orientations, health concerns, or personal

relationships. This comes in conflict with the proportionality and necessity standards established in the *Puttaswamy* judgement. Moreover, as outlined above, the provision is unconstitutionally vague as it fails to prescribe adequate procedural safeguards to mitigate the underlying risks of unconstitutional. It also lacks any oversight or accountability mechanism that independently authorizes such data processing from the State and any of its instrumentalities.

(III) THE COMPENSATION VACUUM AND VIOLATION OF THE RIGHT TO A REMEDY

R. BECAUSE the omission of Section 43A of the IT Act, without the inclusion of a corresponding provision in the DPDP Act, for the award of civil compensation to data principals, creates an unconstitutional vacuum in the right to a legal remedy as guaranteed under Article 21. The right to privacy, recognized as a fundamental right in the *Puttaswamy* judgment, is hollow without an effective mechanism for restoration of the *status quo ante* or the provision of damages for its violation. By redirecting all financial consequences of a breach to the Central Government treasury rather than the aggrieved citizen, the legislature has prioritized fiscal deterrence over the fundamental rights of the individual.

S. BECAUSE the repeal of Section 43A extinguishes the ability of individuals to claim damages against

wrongful loss or wrongful gain which occurred by the reason of failure to protect data by an intermediary, which were previously recoverable under the IT Act framework. In contrast, international standards, particularly the EU GDPR under Article 82, as interpreted by the CJEU in *Österreichische Post AG* (C-300/21), explicitly recognize that non-material damage does not need to meet a threshold of seriousness to be compensable. This standard was further reinforced in ***VB* v. *Natsionalna agentsia za prihodite*** (C-340/21), where the CJEU held that the fear of future misuse of personal data following a breach constitutes compensable non-material damage, and in ***Agentsia po vpisvaniyata* v. *OL*** (C-200/23), where the loss of control over personal data for even a short period was deemed sufficient. The Indian framework, by focusing purely on penalties, fails to recognize these inherent injuries.

T. BECAUSE Section 43A of the Information Technology Act, 2000, read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, constituted the only statutory framework in India which recognised an enforceable right of individuals to seek compensation from body corporates for negligent handling of sensitive personal data resulting in wrongful loss or wrongful gain. The said provision embodied the principle that violations of

informational privacy cause both tangible and dignitary harms, and therefore required a compensatory civil remedy. The omission of this framework through the DPDP Act has dismantled a rights-enforcement mechanism that formed a crucial component of privacy protection in India.

U. BECAUSE the DPDP Act replaces the compensatory model under Section 43A with a penalty-centric enforcement structure, where penalties imposed by the Data Protection Board are payable to the State and not to the affected Data Principal. The imposition of a monetary penalty is punitive and regulatory in nature and cannot be treated as an equivalent substitute for a civil compensatory remedy which restores the victim. The DPDP Act does not confer any enforceable right upon an affected Data Principal to claim damages, restitution, or compensation, nor does it empower the Data Protection Board to adjudicate individual claims of harm and award compensatory relief. Consequently, the DPDP framework renders the individual whose privacy has been violated effectively remediless.

V. BECAUSE the right to privacy under Article 21, as recognised by this Hon'ble Court, necessarily requires the availability of effective remedies against unlawful processing, negligent breaches, and wrongful exposure of personal data. A statutory regime which acknowledges privacy harms but

provides no compensatory or restorative relief to affected individuals violates the guarantee of meaningful enforcement of fundamental rights. Further, the DPDP Act creates an arbitrary and unreasonable framework whereby the State becomes the beneficiary of penalties arising out of privacy violations, while the citizen who suffers harm is excluded from relief. Such a design is manifestly arbitrary and violates Articles 14 and 21 of the Constitution.

W. BECAUSE after the recognition of privacy as a fundamental right in ***Puttaswamy***, the State cannot introduce a legislative framework that dilutes existing privacy protections and removes remedies without providing a constitutionally adequate substitute. The omission of Section 43A and the absence of any equivalent compensatory mechanism amounts to a regressive rollback of privacy safeguards. Such a rollback fails the proportionality standard, is not narrowly tailored to any legitimate State purpose, and is inconsistent with constitutional obligations to protect dignity, autonomy, and informational self-determination.

Excessive Delegation and the Standard of Security

X. BECAUSE Section 43A of the IT Act, and the DPDP Act, engage in excessive delegation by permitting the Executive to define the core substantive components of the law, specifically sensitive personal data and reasonable security

practices, through subordinate legislation without sufficient statutory guidelines. This Hon'ble Court has consistently held that the legislature cannot delegate its essential legislative functions, yet the definitions of what data is protected and what security is reasonable have been left entirely to the discretion of the Central Government through the 2011 SPDI Rules and now the DPDP Rules.

Y. BECAUSE Rule 6 of the DPDP Rules introduces a prescriptive and technologically specific set of Reasonable Security Safeguards such as encryption, masking, and virtual tokens, which effectively mandates a State-dictated security architecture for private entities. This rigid approach fails the test of proportionality as it does not account for the varying technical capacities of different data fiduciaries, thereby imposing a disproportionate burden on startups and small enterprises while potentially facilitating state-mandated backdoors into encrypted systems.

Arbitrary Data Retention and the Erosion of Minimization

Z. BECAUSE Rule 6(1)(e) of the DPDP Rules mandates that every Data Fiduciary must retain logs and personal data for a minimum period of one year for the purpose of enabling the detection of unauthorized access, which constitutes a manifest violation of the principle of data minimisation and storage limitation. This mandatory retention period

applies even after the purpose for which the data was collected has been fulfilled, thereby forcing fiduciaries to maintain repositories of data that would otherwise be erased, increasing the surface area for potential breaches and State surveillance.

AA. BECAUSE the mandatory retention of personal data for 365 days after the end of purpose is an arbitrary timeframe that lacks a rational nexus to the objective of cybersecurity, as the risk of breach detection does not universally require a one-year window for every category of data or fiduciary. This requirement is inconsistent with the deemed end-of-purpose concept in the DPDP Act, creating an internal contradiction that leads to legal uncertainty for both the data principal and the fiduciary.

Institutional Lack of Independence and Procedural Fairness

BB. BECAUSE the DPB, as established under the DPDP Rules, is a subordinate office of the Ministry of Electronics and Information Technology (MeitY), lacking the institutional independence required of a specialised adjudicatory body. The Central Government retains complete control over the appointment, tenure, and removal of Board members, which creates a significant risk of institutional bias. This lack of independence is unconstitutional when compared to international standards, such as those established by the CJEU in ***Commission*** **v.** ***Hungary*** (C-288/12) and

Commission* v. *Austria (C-614/10), which ruled that supervisory authorities must perform their duties free from all external influence, specifically political or executive instructions, and that the premature removal of independent heads violates the core principle of independence required for data protection.

CC. BECAUSE the exhaustion of internal remedies requirement under Rule 14, which mandates that a Data Principal must first seek redressal from the Data Fiduciary before approaching the DPB, acts as a procedural barrier to justice. This requirement is particularly onerous when dealing with large-scale digital platforms that utilize automated and opaque grievance systems, thereby delaying the protection of a fundamental right and creating a chilling effect on the enforcement of privacy rights.

The Dilution of the Right to Information

DD. BECAUSE the DPDP Laws arbitrarily dilute the Right to Information Act, 2005, by amending Section 8(1)(j) to remove the public interest override for the disclosure of personal information. This enables public authorities to deny information requests by merely labeling them as "personal data," thereby shielding corruption and administrative irregularities from public scrutiny under the guise of privacy.

Manifest Arbitrariness in Consent and Legitimate Uses

EE. BECAUSE the framework for "deemed consent" or "legitimate uses" under the DPDP Rules is overbroad and vaguely defined, permitting the processing of personal data for purposes that the data principal may never have reasonably expected. The absence of a "legitimate interest" balancing test, as found in the EU GDPR, means that the Indian framework lacks the necessary constitutional safeguards to ensure that the fiduciary's interests do not override the individual's rights, leading to manifest arbitrariness.

FF. BECAUSE the "Consent Manager" framework established under Rule 4 creates a centralized node of failure and a potential instrument for State-directed nudging. By requiring Consent Managers to be India-incorporated entities registered with the DPB, the DPDP Rules facilitate a structure where the State can monitor the aggregate privacy preferences and consent artefacts of the entire population, thereby violating the "anonymity" and "privacy" components of the right to informational self-determination.

Failure of Proportionality in State Access and Surveillance

GG. BECAUSE Section 36 of the DPDP Act and Rule 22 of the DPDP Rules grant the Central Government the power to call for any such information from a Data Fiduciary or intermediary for the purposes of the DPDP Act, without providing for judicial

oversight or independent verification. This power to create "surveillance backdoors" fails the proportionality test. The ECtHR in ***Roman Zakharov* v. *Russia*** (2015) and ***Big Brother Watch* v. *The United Kingdom*** (2021) has held that surveillance regimes lacking independent, preferably judicial, authorisation and oversight are inherently prone to abuse and violate the right to privacy under Article 8 of the ECHR. The absence of such checks in the Indian DPDP Laws constitutes a considerable regression in privacy governance.

Constitutional Infirmity of Phased Implementation

HH. BECAUSE the "Phased Implementation" period of 18 months, as notified by MeitY, creates a "protection holiday" where individuals are left without the safeguards of the legacy IT Act (due to its effective repeal) and the protections of the new DPDP Act (due to the delay in operationalizing fiduciaries' obligations). This gap in the legal framework constitutes a failure of the Central Government to fulfill its positive obligation to protect the fundamental rights of citizens during the transition.

Exclusion of Non-Digital Data and Article 14

II. BECAUSE the DPDP Laws arbitrarily exclude personal data in non-digital form that is not subsequently digitized, thereby creating a discriminatory classification between individuals

whose data is processed digitally and those whose data remains in manual filing systems. This exclusion ignores the importance of confidentiality for all sensitive records, a principle recognized by the ECtHR in ***Z* v. *Finland*** (1997), which held that the disclosure of highly sensitive medical data (HIV status) in a court judgment without cogent reasons violates the right to respect for private and family life, regardless of whether the record was initially digital or manual.

Omission of Data Portability and Economic Freedom

JJ. BECAUSE the DPDP Rules fail to provide for the "Right to Data Portability," a right essential for individual autonomy and for preventing vendor lock-in in the digital economy. The omission of this right strengthens the position of market incumbents and large fiduciaries, thereby infringing upon the economic rights of users and smaller competitors under Article 19(1)(g).

Vagueness in Significant Data Fiduciary Designation

KK. BECAUSE the criteria for designating a Significant Data Fiduciary (*hereinafter referred to as the* **"SDF"**) under the DPDP Act including vague terms like sovereignty and integrity of India and public order grant the Executive unguided power to selectively target specific entities. This lack of specific, objective criteria leads to arbitrary application and political interference.

Infringement on the Rights of the Child

LL. BECAUSE the requirement for verifiable parental consent for all processing of children's data, regardless of the child's age or the nature of the service, is a disproportionate restriction that ignores the "evolving capacities" of adolescents. By effectively preventing minors from accessing even harmless digital services without parental intervention, the DPDP Rules infringe upon the child's right to information and free expression.

Abuse of Algorithmic Transparency

MM. BECAUSE the DPDP Rules, fail to provide a Right to Explanation for automated decision-making (*hereinafter referred to as the* **"ADM"**), which is critical in an era where algorithms determine access to essential services. In the CJEU judgment ***Dun and Bradstreet Austria*** (C-203/22), the court held that data subjects have a fundamental right to receive meaningful information about the logic of ADM in a way that enables them to challenge the outcome. The DPDP Rules, by omitting this right, render the rights to access and correction illusory.

Unconstitutional Burden of Log Retention

NN. BECAUSE the mandatory retention of logs for investigation purposes under Rule 6(1)(e) effectively mandates the creation of a master key for data fiduciaries, as it requires them to keep detailed records of all information retrieval for one year. This

requirement creates a secondary risk of harm to the data principal, as the log itself becomes a target for hackers and state surveillance, without any clear proportionality.

Exclusion of Publicly Available Data

OO. BECAUSE the DPDP Laws exclude from their scope personal data that is made publicly available, which is an overbroad exemption that fails to recognize that public data can still be misused through profiling. This exclusion ignores the contextual integrity of data, where information shared for one public purpose should not be used for unrelated profiling, a principle recognized by the Hon'ble Supreme Court in ***Puttaswamy***.

Barriers to Representative Action

PP. BECAUSE the DPDP Laws do not provide for Representative Actions or class-action suits for data breaches, making it impossible for individuals with small individual losses to collectively challenge a large data fiduciary. This omission facilitates a culture of impunity for systemic security failures and contrasts with evolving standards in the UK following ***Lloyd* v. *Google LLC*** UKSC 27, which, while limiting uniform damages under old statutes, emphasized the inherent value of data and the viability of representative procedures for common interests.

Executive-Led Adjudication and Separation of Powers

QQ. BECAUSE the shift from judicial Adjudicating Officers to an administrative DPB whose members are appointed by the Executive violates the principle of separation of powers. The DPB performs quasi-judicial functions such as imposing massive penalties but lacks the institutional safeguards of the judiciary, making it a "subordinate office" rather than a neutral arbiter.

(IV) LACK OF INDEPENDENCE OF THE DATA PROTECTION BOARD

Executive Interference in Constitution and Functioning of the Data Protection Board

RR. BECAUSE the DPDP Laws establish the Central Government's undue control over the DPB, effectively neutering any semblance of independence. The Central Government controls the constitution of the Search-cum-Selection Committee for appointment of Chairperson and Members of the DPB, as per Rule 17 of the DPDP Rules; the appointment of the Chairperson and Members of the DPB, as per Rule 17 of the DPDP Rules; the provision of salaries and allowances to Chairperson, Members, officers and employees of the DPB, as per Rules 18 and 21 of the DPDP Rules, and the approval of any appointment of officers and employees of the DPB, as per Rule 21 of the DPDP Rules, the same requirement which is found in the language of Section 24 of the DPDP Act as well.

SS. BECAUSE this undue control over the DPB by the Central Government undermines the independence of the Board in carrying out its functions and exercising powers conferred to it under Chapter 6 of the DPDP Act, especially in adjudicating complaints, issuing binding directions, and taking action against government departments. Under the present appointment regime, there is a serious conflict-of-interest as the Central Government and its agencies are Significant Data Fiduciaries against whom complaints may be made under Section 27 of the DPDP Act.

TT. BECAUSE this undue control by the Central Government over the appointment, salaries, and terms and conditions of the members of the DPB is unconstitutional as it violates fundamental constitutional principles of independence of the judiciary and separation of powers. Established judicial precedents of this Hon'ble Court in in ***Supreme Court Advocates-on-Record Association and Another*** **v.** ***Union of India*** (2016) 5 SCC 1, ***Rojer Mathew*** **v.** ***South Indian Bank Limited represented by its Chief Manager and Others*** (2020) 6 SCC 1 (hereinafter **"Rojer Mathew"**) and ***Madras Bar Association*** **v.** ***Union of India*** 2025 INSC 1330 (hereinafter **"MBA-VI"**), clearly hold that executive control must be excluded from the appointment process of bodies performing judicial or quasi-judicial functions as it strikes at the heart of the constitutional core.

UU. BECAUSE in ***Rojer Mathew,*** this Hon'ble Court observed that a party that litigates before the tribunal "should never be a participant in the appointment process of members of the tribunal," and that "the procedure of appointment and conditions of service of members must be akin to judges.":

> *"50. Later, in **Madras Bar Association vs. Union of India (2014)**, whilst striking down the newly-created National Tax Tribunal under the National Tax Tribunals Act, 2005, it was observed that procedure of appointment and conditions of service of members must be akin to judges of the Courts which were sought to be substituted by the Tribunal(s).*
>
> *51. Only persons with professional legal qualifications coupled with substantial experience in law were held to be competent to handle complex legal issues. It was further held that a litigating party (Govt.) should never be a participant in the appointment process of members of the Tribunal. Similarly, a provision for reappointment or extension of tenure is ipso facto prejudicial to the independence of the members of Tribunal. A difference was also drawn between appointments to Tribunals which substituted Courts of first instance and to those which were not subordinate to High Courts."*
>
> *(emphasis supplied)*

VV. BECAUSE this Hon'ble Court in ***Rojer Mathew*** also held that Search-cum-Selection Committees that are dominated by executive nominees with minimal judicial representation violated the doctrine of

separation of powers and undermined the independence of the judiciary and tribunals:

> *"144. (...) Independence of the institution refers to sufficient degree of separation from other branches of the government, especially when the branch is a litigant or one of the parties before the tribunal. Functional independence would include method of selection and qualifications prescribed, as independence begins with appointment of persons of calibre, ability and integrity. Protection from interference and independence from the executive pressure, fearlessness from other power centres – economic and political, and freedom from prejudices acquired and nurtured by the class to which the adjudicator belongs, are important attributes of institutional independence.*
>
> *...*
>
> *152. Composition of a Search-cum-Selection Committee is contemplated in a manner whereby appointments of Member, Vice-President and President are predominantly made by nominees of the Central Government. A perusal of the Schedule to the Rules shows that save for token representation of the Chief Justice of India or his nominee in some Committees, the role of the judiciary is virtually absent.*
>
> *153. We are in agreement with the contentions of the Learned Counsel for the petitioner(s), that the lack of judicial dominance in the Search-cum-Selection Committee is in direct contravention of the doctrine of separation of powers and is an encroachment on the judicial domain. The doctrine of separation of powers has been well recognised and re-interpreted by this Court as an important facet of the basic structure of the Constitution, in its dictum in*

Kesavananda Bharati* v. *State of Kerala, *and several other later decisions. The exclusion of the Judiciary from the control and influence of the Executive is not limited to traditional Courts alone, but also includes Tribunals since they are formed as an alternative to Courts and perform judicial function.*

154. Clearly, the composition of the Search-cum-Selection Committees under the Rules amounts to excessive interference of the Executive in appointment of members and presiding officers of statutory Tribunals and would undoubtedly be detrimental to the independence of judiciary besides being an affront to the doctrine of separation of powers.

...

157. We are of the view that the Search-cum-Selection Committee as formulated under the Rules is an attempt to keep the judiciary away from the process of selection and appointment of Members, Vice-Chairman and Chairman of Tribunals. This Court has been lucid in its ruling in ***Supreme Court Advocates-on-Record Assn.* v. *Union of India (Fourth Judges Case)***, *wherein it was held that primacy of judiciary is imperative in selection and appointment of judicial officers including Judges of High Court and Supreme Court. Cognisant of the doctrine of Separation of Powers, it is important that judicial appointments take place without any influence or control of any other limb of the sovereign. Independence of the judiciary is the only means to maintain a system of checks and balances on the working of Legislature and the Executive. The Executive is a litigating party in most of the litigation and hence cannot be allowed to be a dominant participant in judicial appointments."*

(emphasissupplied)

WW. BECAUSE this observation was further affirmed in ***MBA-VI***, where this Hon'ble Court also relied on ***Supreme Court Advocates-on-Record Association and Another*** **v.** ***Union of India*** (2016) 5 SCC 1 (***Fourth Judges Case***) to emphasize that executive control must be excluded from the appointment process of bodies performing judicial or quasi-judicial functions, and further held that laws that undermine foundational values such as independence, impartiality, and effective adjudication "strike at the core of the constitutional arrangement":

> *"55. The Court further held that since the Executive is often a party to litigation before tribunals, it cannot be permitted to play a dominant role in appointing their members. Drawing from the* ***Fourth Judges Case****, the Court emphasized that executive control must be excluded from the appointment process of bodies performing judicial or quasi-judicial functions. It concluded that the composition of the Search-cum-Selection Committees under the 2017 Rules violated the constitutional scheme, as it diluted judicial involvement and amounted to executive encroachment on the independence of the judiciary.*
>
> *...*
>
> *125. Far from being abstract, these principles are firmly embedded in the text, scheme, and spirit of the Constitution. Judicial independence is inseparable from the guarantee of judicial review, and judicial review itself is the mechanism that ensures*

that all State action (legislative, executive, or judicial) conforms to the Constitution. Similarly, the doctrine of separation of powers is not merely philosophical. It underwrites the very distribution of authority among the three branches of government. It is reflected in Articles 32, 136, 141, 226, and 227 of the Constitution, which vest the judiciary with the power to interpret the law, enforce fundamental rights, and supervise subordinate courts and tribunals. It is also embedded in provisions relating to appointment, tenure, and removal of judges, all of which insulate the courts from executive dominance.

126. Legislative measures concerning the structure, composition, and functioning of tribunals necessarily implicate these constitutional principles because tribunals discharge judicial functions and form part of the larger system of justice administration. When Parliament designs or alters the tribunal system, it must do so in a manner consistent with the constitutional requirements of independence, impartiality, and effective adjudication. A law that undermines these foundational values, such as by enabling executive control over appointments, curtailing tenure arbitrarily, or weakening institutional autonomy, does not merely offend an "abstract principle". It strikes at the core of the constitutional arrangement.

...

132. In the same way, the norms laid down in the tribunal cases, regarding tenure, age limits, selection processes, qualifications, and independence from executive control, are not abstract judicial preferences. They are constitutional requirements distilled from Articles 323-A and 323-B read with the doctrines of separation of powers, independence of the judiciary, and the

> *guarantee of equality under Article 14. These principles therefore furnish the constitutional tests that any legislation on tribunals must satisfy. Where Parliament re-enacts provisions previously struck down without curing the underlying defect, the resulting legislation remains vulnerable to invalidation, not because the Court is imposing its own policy, but because the Constitution itself demands adherence to these structural safeguards."*
>
> *(emphasis supplied)*

XX. BECAUSE the power of the Central Government to appoint various members of the DPB and its personnel, and determine their service terms and conditions, is unconstitutional as it is a Significant Data Fiduciary under the DPDP Act and a litigating party before the DPB against whom complaints under Section 27 of the DPDP Act can be made. By vesting these powers in the Central Government, the Impugned Laws create a structural conflict of interest and a reasonable apprehension of institutional bias, which offends the fundamental natural justice principle of *nemo judex in causa sua*.

YY. BECAUSE the powers vested in the Central Government under Rule 18 and the Fifth Schedule to the DPDP Rules, complete the constitutional subordination of the DPB to the Executive. By subjecting the Chairperson and Members to the Central Civil Services (Leave) Rules, 1972 and the Central Civil Services (Classification, Control and Appeal) Rules, 1965, and by vesting final authority over undefined service conditions in the Central

Government, the Rules assimilate the DPB's Members into the executive civil service hierarchy and undermines the DPB's ability to function independently and process complaints against the Central Government, a Significant Data Fiduciary under the DPDP Act and a litigant before the DPB.

ZZ. BECAUSE Rule 21 of the DPDP Rules, read with the Sixth Schedule vests excessive control over the staffing decisions of the DPB with the Central Government, negatively affecting the independence of the DPB. Rule 21 states that the DPB may appoint officers and staff only with "previous approval of the Central Government," the same language that is found in Section 24 of the DPDP Act. Further, the Sixth Schedule adds the service condition that the DPB may only appoint officers and employees on deputation from the Central Government, a State Government, an autonomous body under the overall control of the Central Government or a State Government, a statutory body, the National Institute for Smart Government, or a public sector enterprise. Further, the Schedule provides for residual, plenary, and unreviewable control over service conditions with the Central Government - as per the Schedule, undefined terms and conditions of service are to be referred to the Central Government alone, whose decision shall be final. As a result, not only is the DPB restricted in its personnel decisions by the Central Government whose approval is necessary, but the Board is also constrained in who it can

appoint as officers and other employees. This has significant negative effects on the DPB's ability to appoint officers and employees with technical, legal, and human rights expertise, all of which are essential for meaningful enforcement of data protection norms.

AAA. BECAUSE this Hon'ble Court has held emphatically in ***Rojer Mathew*** that allowing the executive a controlling authority over diverse facets of tribunals destroys judicial independence which constitutes a basic feature of the Constitution:-

> *"88. ...Determination of the norms of eligibility, the process of selection, conditions of service, and those regulating the impartiality with which the members of the tribunals discharge their functions and their effectiveness as adjudicatory bodies is dependent on their isolation from the executive. By leaving the rule making power to the uncharted wisdom of the executive, there has been a self-effacement by Parliament. The conferment of the power to frame rules on the executive has a direct impact on the independence of the tribunals. Allowing the executive a controlling authority over diverse facets of the tribunals would be destructive of judicial independence which constitutes a basic feature of the Constitution."*
>
> *(emphasis supplied)*

Divergence from Established Global Standards for Independent Data Protection Agencies

BBB. BECAUSE the appointment, staffing, and operational architecture of the DPB under Rules 17, 18 and 21 of the DPDP Rules as well as Section 24 of the DPDP Act departs materially from established norms and minimum standards governing independent data protection authorities, as reflected in contemporary global data protection regimes, thereby rendering the DPB structurally vulnerable to executive influence and regulatory capture.

CCC. BECAUSE across comparative jurisdictions with data protection regimes, the independence of the data protection agency and regulatory body is expressly and institutionally secured through explicit provisions in contrast to the DPDP Laws which centralise power exclusively within the Central Government. Article 52(1) and (2) of the EU GDPR mandate that supervisory authorities act with complete independence and that their members remain free from direct or indirect external influence, while Article 53(1) requires a transparent appointment procedure. Article 52(5) and (6) of the EU GDPR also guarantee that supervisory authorities choose and control their own staff and are provided with separate, public annual budgets to enable independent financial planning:

> *"Art. 52. Independence:*
>
> *1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.*

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53. General conditions for the members of the supervisory authority:

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

> *— their government;*
>
> *— their head of State; or*
>
> *— an independent body entrusted with the appointment under Member State law."*

Similarly, Brazil's National Data Protection Agency (ANPD) is guaranteed technical and operational autonomy under Articles 55-A and 55-D of the General Data Protection Law, *Lei Geral de Proteção de Dados* (LGPD):

> *"Article 55-A. The National Data Protection Authority (ANPD) is hereby created, a government agency of special nature, endowed with technical and decision-making autonomy, with its own assets and its headquarters and jurisdiction in the Federal District.*
>
> *Article 55-D. ANPD's Board of Directors shall consist of five (5) directors, including the Director-President.*
>
> *Paragraph 1. The members of ANPD's Board of Directors shall be chosen and appointed by the President of the Republic, after approval by the Federal Senate, pursuant to Article 52, item III, subitem "f", of the Federal Constitution, and shall hold at least a commissioned position of the Higher Management and Advisory Group - DAS Level 5.*
>
> *Paragraph 2. The members of the Board of Directors shall be chosen among Brazilians with unblemished reputation, higher education level and renowned for their expertise in the specialty field of the positions to which they will be appointed.*

> *Paragraph 3. The term of office of the members of the Board of Directors shall be of 4 (four) years.*
>
> *Paragraph 4. The terms of office of the first members of the Board of Directors shall be of 2 (two), 3 (three), 4 (four), 5 (five) and 6 (six) years, as provided for in the appointment act.*
>
> *Paragraph 5. In the event of a vacancy during the term of office of a member of the Board of Directors, the remaining term shall be completed by the successor.*"

In California, the California Privacy Protection Agency (CPPA) is constituted through a multiparty appointment mechanism under §1798.199.10 of the California Civil Code, and its members are statutorily required to remain free from external influence under §1798.199.15(c). The CPPA also has the power to independently determine staff compensation and appoints its Executive Director under §1798.199.30 of the California Civil Code:

> *"1798.199.10. (a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018. The agency shall be governed by a five-member board, including the chairperson. The chairperson and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the*

areas of privacy, technology, and consumer rights.

1798.199.15. Members of the agency board shall:

(a) Have qualifications, experience, and skills, in particular in the areas of privacy and technology, required to perform the duties of the agency and exercise its powers.

(b) Maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act.

(c) Remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another.

(d) Refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term.

(e) Have the right of access to all information made available by the agency to the chairperson.

(f) Be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil action under this title during the member's tenure or during the five-year period preceding the member's appointment.

(g) Be precluded for a period of two years after leaving office from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the agency if the purpose is to influence an action of the agency.

1798.199.30. The agency board shall appoint an executive director who shall act in accordance with agency policies and regulations and with applicable law. The agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The agency may contract for services that cannot be provided by its employees."

DDD. BECAUSE this manifest departure from established global norms and standards for data protection agencies without any compelling justification, renders the impugned provisions and rules arbitrary and disproportionate under Article 14 of the Constitution of India, as the vesting of comprehensive appointment, staffing, and operational control in the Central Government lacks a rational nexus to the object of effective data protection enforcement when less intrusive and regulatory regimes are available and have been widely adopted across jurisdictions.

Divergence from Constitution and Appointment Practices of other Statutory Tribunals and Quasi-Judicial Bodies

EEE. BECAUSE multiple statutory tribunals and quasi-judicial bodies, in contrast to the DPB, incorporate judicial oversight in the constitution and appointment of the Chairpersons and Members, through their governing statutes by (i) mandating consultation with the Chief Justice of India for such

appointments, or (ii) mandating the inclusion of sitting or former judges in the Search-cum-Selection Committee.

FFF. BECAUSE the Chairperson and Members of the DPB are appointed by the Central Government without any judicial oversight under Rule 17(3) of the DPDP Rules, 2025, in contrast to multiple statutory tribunals and quasi-judicial bodies in India which require mandatory consultation with the Chief Justice of India for the constitution and appointment of their Chairpersons and Members. For example:

A. Section 6(3) of the Administrative Tribunals Act, 1985 requires that the Chairman and every other Member of the CAT be appointed after consultation with the Chief Justice of India by the President.

B. Section 6(2) of the National Green Tribunal Act, 2010, which established the NGT, states that the Chairperson of the NGT is to be appointed by the Central Government in consultation with the Chief Justice of India.

C. As per Section 412 of the Companies Act, 2013, the President of the NCLT and the Chairperson and Judicial Members of the NCLAT are appointed after consultation with the Chief Justice of India.

GGG. BECAUSE even those appointments of Chairpersons and Members based on recommendation by a Search-cum-Selection Committee materially differ from the scheme

contemplated under Rule 17 of the DPDP Rules, 2025 in terms of judicial oversight by mandating the inclusion of sitting or former judges in the Selection Committee, despite Rule 17 providing for a similar recommendation based appointment regime. For example:

A. The Chairperson and other Members of the CCI are appointed under Section 9(1) of the Competition Act, 2002, by the Central Government upon recommendation from a Selection Committee comprising (i) the Chief Justice of India or his nominee as the Chairperson of the Selection Committee, (ii) the Secretary in the Ministry of Corporate Affairs and the the Secretary in the Ministry of Law and Justice as Members, and (iii) two experts of repute who have special knowledge of, and professional experience in international trade, economics, business, commerce, law, finance, accountancy, management, industry, public affairs or competition matters including competition law and policy.

B. The Judicial Members and Expert Members of the NGT are appointed under Rule 3 of the National Green Tribunal (Manner of Appointment of Judicial and Expert Members, Salaries, Allowances and other Terms and Conditions of Service of Chairperson and other Members and Procedure for Inquiry)

Rules, 2010 on the recommendation of a Selection Committee comprising (i) a sitting Judge of the Supreme Court nominated by the Chief Justice of India, in consultation with the Minister of Law and Justice, as Chairperson, and (ii) the Chairperson of the Tribunal, the Secretary to the Government of India in the Ministry of Environment and Forests, the Director of the Indian Institute of Technology, Kanpur, the Director of the Indian Institute of Management, Ahmedabad, and the President of the Centre for Policy Research, New Delhi, as Members.

C. The Members of the NCLT and the Technical Members of the NCLAT are appointed as per Section 412 of the Companies Act, 2013 upon the recommendation of a Selection Committee consisting of (i) the Chief Justice of India or his nominee as the Chairperson of the Selection Committee, and (ii) a senior Judge of the Supreme Court or Chief Justice of High Court, the Secretary in the Ministry of Corporate Affairs, and the the Secretary in the Ministry of Law and Justice as Members.

HHH. BECAUSE multiple statutory tribunals and quasi-judicial bodies further ensure judicial oversight through statutory requirements that judicial members sit on the tribunal itself along with technical or expert members, like the CAT which has Judicial and Administrative Members under Section 5 of the

Administrative Tribunals Act, 1985; the NGT which has Judicial and Expert Members under Section 4 of the National Green Tribunal Act, 2010, or; the NCLT which has Judicial and Technical Members under Section 408 of the Companies Act, 2013.

III. BECAUSE the appointment procedure for the Chairperson and Members of the DPB differ materially from other statutory tribunals and quasi-judicial bodies in that it is effectuated through the delegated legislation Rule 17 of the DPDP Rules, 2025. For all the above-mentioned tribunals and quasi-judicial bodies except for Judicial and Expert Members of the NGT, the appointments of the Chairperson and Members were effectuated solely through the parent legislation.

JJJ. BECAUSE Section 19(3) of the DPDP Act, 2023, is vague and arbitrary as it do not prescribe any minimum for required years of experience, do not require the Chairperson and Members of the DPB to have judicial experience, and do not require that the Chairperson and Members be well versed in privacy and data protection law. This is in stark opposition to the comprehensive and specific qualifications required for the Chairpersons and Members of other statutory tribunals and quasi-judicial bodies. For example, Sections 6(1) and 6(2) of the Administrative Tribunals Act, 1985 state the following qualifications for appointment as Chairman, Vice-Chairman, and other Members of the CAT–

"6. Qualifications for appointment as Chairman, Vice-Chairman and other members.—

(1) A person shall not be qualified for appointment as the Chairman unless he is, or has been, a Judge of a High Court:

Provided that a person appointed as Vice-Chairman before the commencement of this Act shall be qualified for appointment as Chairman if such person has held the office of the Vice-Chairman at least for a period of two years.

(2) A person shall not be qualified for appointment,—

(a) as an Administrative Member, unless he has held for at least two years the post of Secretary to the Government of India or any other post under the Central or State Government and carrying the scale of pay which is not less than that of a Secretary to the Government of India for at least two years or held a post of Additional Secretary to the Government of India for at least five years or any other post under the Central or State Government carrying the scale of pay which is not less than that of Additional Secretary to the Government of India at least for a period of five years:

Provided that the officers belonging to All-India services who were or are on Central deputation to a lower post shall be deemed to have held the post of Secretary or Additional Secretary, as the case may be, from the date such officers were granted proforma promotion or actual promotion whichever is earlier to the level of Secretary or Additional Secretary, as the case may be, and the period spent on Central deputation after such date shall count for qualifying service for the purposes of this clause;

> *(b) as a Judicial Member, unless he is or qualified to be a Judge of a High Court or he has for at least two years held the post of a Secretary to the Government of India in the Department of Legal Affairs or the Legislative Department including Member-Secretary, Law Commission of India or held a post of Additional Secretary to the Government of India in the Department of Legal Affairs and Legislative Department at least for a period of five years"*

Similarly, Section 8(2) of the Competition Act, 2002, requires the following qualifications of the Chairperson and every other Member of the CCI–

> *"8.Composition of Commission*
>
> *(2) The Chairperson and every other Member shall be a person of ability, integrity and standing and who has special knowledge of, and such professional experience of not less than fifteen years in, international trade, economics, business, commerce, law, finance, accountancy, management, industry, public affairs or competition matters, including competition law and policy, which in the opinion of the Central Government, may be useful to the Commission"*

Further, Section 5 of the National Green Tribunal Act, 2010, lists the following qualifications for the appointment of Chairperson, Judicial Member and Expert Member of the NGT–

> *"5.Qualifications for appointment of Chairperson, Judicial Member and Expert Member.—*
>
> *(1) A person shall not be qualified for appointment as the Chairperson or Judicial Member of the Tribunal unless he is, or has*

been, a Judge of the Supreme Court of India or Chief Justice of a High Court:

Provided that a person who is or has been a Judge of the High Court shall also be qualified to be appointed as a Judicial Member.

(2) A person shall not be qualified for appointment as an Expert Member, unless he,—

(a) has a degree in Master of Science (in physical sciences or life sciences) with a Doctorate degree or Master of Engineering or Master of Technology and has an experience of fifteen years in the relevant field including five years practical experience in the field of environment and forests (including pollution control, hazardous substance management, environment impact assessment, climate change management, biological diversity management and forest conservation) in a reputed National level institution; or

(b) has administrative experience of fifteen years including experience of five years in dealing with environmental matters in the Central or a State Government or in a reputed National or State level institution."

Finally, Sections 409 and 411 of the Companies Act list the following qualifications for the President and Members of NCLT, and the chairperson and Members of the NCLAT respectively–

"409. Qualification of President and Members of Tribunal.—

(1) The President shall be a person who is or has been a Judge of a High Court for five years.

(2) A person shall not be qualified for appointment as a Judicial Member unless he—

(a) is, or has been, a judge of a High Court; or

(b) is, or has been, a District Judge for at least five years; or

(c) has, for at least ten years been an advocate of a court.

Explanation.—For the purposes of clause (c), in computing the period during which a person has been an advocate of a court, there shall be included any period during which the person has held judicial office or the office of a member of a tribunal or any post, under the Union or a State, requiring special knowledge of law after he become an advocate.

(3) A person shall not be qualified for appointment as a Technical Member unless he—

(a) has, for at least fifteen years been a member of the Indian Corporate Law Service or Indian Legal Service 1[and has been holding the rank of Secretary or Additional Secretary to the Government of India]; or

(b) is, or has been, in practice as a chartered accountant for at least fifteen years; or

(c) is, or has been, in practice as a cost accountant for at least fifteen years; or

(d) is, or has been, in practice as a company secretary for at least fifteen years; or

(e) is a person of proven ability, integrity and standing having special knowledge and professional experience of not less than fifteen years in industrial finance, industrial management, industrial reconstruction, investment and accountancy.

> *(f) is, or has been, for at least five years, a presiding officer of a Labour Court, Tribunal or National Tribunal constituted under the Industrial Disputes Act, 1947 (14 of 1947)*
>
> *...*
>
> *411. Qualifications of chairperson and Members of Appellate Tribunal.—*
>
> *(1) The chairperson shall be a person who is or has been a Judge of the Supreme Court or the Chief Justice of a High Court.*
>
> *(2) A Judicial Member shall be a person who is or has been a Judge of a High Court or is a Judicial Member of the Tribunal for five years.*
>
> *(3) A technical member shall be a person of proven ability, integrity and standing having special knowledge and professional experience of not less than twenty-five years in industrial finance, industrial management, industrial reconstruction, investment and accountancy."*

KKK. In contrast, Section 19(3) of the DPDP Act, 2023 merely requires that the Chairperson and other Members of the DPB to meet the following criteria–

> "*19. Composition and qualifications for appointment of Chairperson and Members.*
>
> ..
>
> *(3) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central*

Government may be useful to the Board, and at least one among them shall be an expert in the field of law."

Section 19(3) of the DPDP Act, 2023 does not prescribe any minimum for required years of experience, does not require the Chairperson and Members of the DPB to have judicial experience, and does not require the Chairperson and Members to be well versed in privacy and data protection rendering it arbitrary.

LLL. BECAUSE this material and manifest divergence from established constitution and appointment practices of other statutory tribunals and quasi-judicial bodies without any compelling justification, renders the impugned provisions and rules arbitrary.

(V) SURVEILLANCE

Violation of Standards set under the PUCL Judgment

MMM. BECAUSE Section 36 of the DPDP Act, read with Rule 23 of the DPDP Rules, and the Seventh Schedule, (**"impugned provisions"**) grant the Central Government the power to compel the DPB, any Data Fiduciary or intermediary to furnish information that may be called for, creating a parallel regime of *de facto* surveillance in India in a manner that is unconstitutional, as it infringes on the right to life and liberty under Article 21 of the Constitution:

"Section 36- Power to Call for Information:

The Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for.

Rule 23- Calling for information from Data Fiduciary or intermediary

(1) The Central Government may, for such purposes of the Act as are specified in Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, within the specified period as may be given in such.

(2) Where the disclosure of furnishing of information as referred to in sub-rule (1) is likely to prejudicially affect the sovereignty and integrity of India or security of the State, the Central Government may require the Data Fiduciary or intermediary to not disclose such furnishing to affected Data Principal or any other person except with the previous permission, in writing, of the authorised person.

(3) For the purposes of this rule, the expression "intermediary" shall have the same meaning as assigned to it in the Information Technology Act, 2000 (21 of 2000)."

NNN. BECAUSE Section 36 of the DPDP Act merely states that the Central Government may, "for the purposes of this Act", require the Board, any Data Fiduciary, or intermediary to furnish such information as it may call for. The said provision does not contemplate the creation of an elaborate

subordinate framework prescribing the categories of information, purposes, authorised persons, timelines, and secrecy obligations.

OOO. BECAUSE Rule 23 of the DPDP Rules and the Seventh Schedule thereto, purport to operationalise Section 36 by creating an independent statutory regime which identifies purposes, designated authorised persons, and imposes additional legal obligations upon Data Fiduciaries and intermediaries. In the absence of any specific statutory delegation under Section 36 enabling such detailed rule-making, Rule 23 travels beyond the scope of the parent statute and is liable to be struck down as ultra vires the DPDP Act.

PPP. BECAUSE it is settled law that delegated legislation cannot create substantive obligations, restrictions, or prohibitions unless the parent statute expressly authorises such delegation, and any subordinate legislation that expands the scope of a statutory power beyond legislative intent is liable to be invalidated.

QQQ. BECAUSE the impugned provisions of the DPDP Laws fall afoul of the standards and guidelines laid down in ***People's Union for Civil Liberties (PUCL)* v. *Union of India***, (1997) 1 SCC 301 (PUCL), and in any event the said safeguards, having been evolved in the context of telephone tapping, are required to be applied and strengthened in light of the fundamentally different nature of modern digital

surveillance, large-scale data processing, and contemporary proportionality jurisprudence as recognised by this Hon'ble Court in *Puttaswamy.*

RRR. BECAUSE the impugned provisions are in violation of the ruling under the ***PUCL*** judgment, where this Hon'ble Court held that the "occurrence of any public emergency" or "in the interest of public safety" are the *sine qua non* for the application of provisions of Section 5(2) of the erstwhile Indian Telegraph Act, 1885 which dealt with provisions for interception. This Hon'ble Court had held explicitly that unless either of the two conditions exists, authorities have no jurisdiction to exercise such powers, as out below:

> *"28. Section 5(2) of the Act permits the interception of messages in accordance with the provisions of the said section. "Occurrence of any public emergency" or "in the interest of public safety" are the sine qua non for the application of the provisions of Section 5(2) of the Act. Unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers under the said section. Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression "public safety" means the state or condition of freedom from danger or risk for the people at large. When either of these two conditions are not in existence, the Central Government or a State Government or the authorised officer cannot resort to telephone-tapping even though there is satisfaction that it is necessary or expedient so to do in the*

> *interests of sovereignty and integrity of India etc. In other words, even if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the State or friendly relations with sovereign States or public order or for preventing incitement to the commission of an offence, it cannot intercept the messages or resort to telephone-tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires. Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. Either of the situations would be apparent to a reasonable person."*

SSS. BECAUSE the impugned provisions fly explicitly in the face of the ruling, as they make no mention of either "public order" or "the interest of public safety", which are the only two conditions this Hon'ble Court upheld as valid reasons for conducting interceptions or issuing of an interception order. In contrast, Rule 23 and the Seventh Schedule of the DPDP Rules show that reliance has been placed on "the interest of sovereignty and integrity of India or security of the State", which this Hon'ble Court in the ***PUCL*** judgment held to be explicitly invalid conditions for interception, barring the presence of situations of violations of public order and public safety.

TTT. BECAUSE a statute that suffers from overbreadth or vagueness is ripe for both constitutional and unconstitutional use by the State and its

instrumentalities (***Shreya Singhal* v. *Union of India***, (2015) 5 SCC 1, [55-86]; ***Chintamanrao* v. *State of M.P.***, 1950 SCC 695, [13]; ***State of Madras* v. *V.G. Row***, (1952) 1 SCC 410, [22-24]; ***State of Bombay* v. *F.N. Balsara***, 1951 SCC 860 [71-72]). To prevent arbitrary and discriminatory enforcement of a provision like Section 36 of the DPDP Act that allows the Central Government to call for information, laws must provide explicit standards for those who apply them. This prevents impermissible delegation of basic policy matters to the State and its instrumentalities, which carries with it the dangers of arbitrary and discriminatory application. For this reason, Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules is vague, overbroad and arbitrary contrary to Article 14 of the Constitution of India.

UUU. BECAUSE the Hon'ble Court in its judgment in ***PUCL***, emphatically held that privacy is a part of the rights enshrined under Article 21 of the Constitution and any violation of privacy must be through procedure established by law, and that this "procedure established by law" must rule out anything "anything arbitrary, freakish or bizarre" and must be "just, fair, and reasonable", which is the touchstone on which infringement of Article 21 rights may be justified:

> *"17. We have, therefore, no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty"*

> *enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law."*
>
> *...*
>
> *30. The above analysis of Section 5(2) of the Act shows that so far the power to intercept messages/conversations is concerned, the section clearly lays down the situations/conditions under which it can be exercised. But the substantive law as laid down in Section 5(2) of the Act must have procedural backing so that the exercise of power is fair and reasonable. The said procedure itself must be just, fair and reasonable. It has been settled by this Court in Maneka Gandhi v. Union of India that "procedure which deals with the modalities of regulating, restricting or even rejecting a fundamental/right falling within Article 21 has to be fair, not foolish, carefully designed to effectuate, not to subvert, the substantive right itself". Thus understood, "procedure" must rule out anything arbitrary, freakish or bizarre. A valuable constitutional right can be canalised only by civilised processes."*

VVV. BECAUSE Section 36 of the DPDP Act enables the Central Government to compel disclosure of information from any Data Fiduciary or intermediary, thereby authorising access to personal data in respect of which individuals possess a reasonable expectation of privacy. However, the said provision contains no requirement of independent or prior authorisation by a judicial authority or any independent oversight mechanism.

WWW. BECAUSE this Hon'ble Court has repeatedly emphasised that where the State seeks to intrude into personal liberty and privacy, especially through search, seizure, or compelled disclosure mechanisms, such intrusion must be accompanied by meaningful checks and authorisation requirements to prevent abuse. The absence of any requirement of independent approval, recorded satisfaction, or review renders the impugned provision manifestly arbitrary and unconstitutional.

XXX. BECAUSE the lack of any statutory requirement to record reasons in writing, to specify the exact nature and scope of information sought, and to limit the request to necessity and proportionality, creates a regime of uncontrolled executive discretion, contrary to the constitutional limitations imposed upon State surveillance.

YYY. BECAUSE the impugned provisions violate the privacy of citizens and are therefore violative of Article 21 of the Constitution. The impugned provisions do not provide for any procedure to prevent arbitrariness in execution, including the presence of judicial, parliamentary, or independent oversight mechanism over electronic surveillance conducted under the DPDP Laws, either at the *ex-ante, ex-post*, or the review stage. Further, the Central Government is granted sweeping, broad-based powers to compel Data Fiduciaries and intermediaries to hand over any information,

including information about users, completely bypassing the procedural safeguards on interception. These impugned provisions therefore create a procedure of surveillance parallel to that of Section 69 of the IT Act, and the Interception Rules, 2009, while omitting the safeguards under which such laws ought to operate as per judicial pronouncements.

ZZZ. BECAUSE in the absence of such legislative safeguards, mandated by the ***PUCL*** judgment, and codified under statutes, the DPDP Laws are rendered unconstitutional, violative of precedent, and dangerously overbroad, violating the right to privacy, as well as the rights to life and personal liberty of citizens.

AAAA. BECAUSE the impugned provisions lack any due process, and are thus unconstitutional. This Hon'ble Court in ***Puttaswamy*** and in ***Mohd. Arif* v. *Supreme Court,*** (2014) 9 SCC 737 has held that a law would be amenable to challenge under Article 21 not only on the ground that the procedure which it prescribes is not "fair, just and reasonable", but also on the grounds that the substantive provisions of the law violate the Constitution, and lack substantive due process.

BBBB. BECAUSE the operation of the surveillance framework in India causes a chilling effect on the exercise of rights by citizens, and is best explained by the B. N.Justice Srikrishna Committee Report, as resulting in a "wide remit to intelligence and law

enforcement agencies" while lacking "sufficient legal and procedural safeguards to protect individual liberties" owing to the lack of meaningful oversight outside of the executive and the lack of checks and balances to obstruct the development of a surveillance society.

CCCC. BECAUSE the impugned provisions are therefore constitutionally void as per Article 13(2), which prohibits the State from making any law which takes away or abridges the rights conferred by Part III of the Constitution of India and declares that any law made in contravention of that clause shall, to the extent of such contravention, be void. The impugned provisions infringe upon the Fundamental Rights of citizens granted under Article 21 of the Constitution.

DDDD. BECAUSE the Seventh Schedule of the DPDP Rules, 2025 expands the purposes for which the Central Government may demand personal data to include vague and open-ended grounds such as "performance of any function under any law" and "disclosure of any information for fulfilling any obligation under any law"

EEEE. BECAUSE the aforesaid formulation effectively permits compelled disclosure of personal data for any governmental purpose whatsoever, thereby nullifying the requirement that privacy-intrusive State action must be limited to narrowly defined, legitimate aims.

FFFF. BECAUSE such an unstructured and unlimited power amounts to a blanket authorisation for executive access to personal data, making Section 36 read with Rule 23 a provision capable of both constitutional and unconstitutional application, and is therefore liable to be struck down as void for overbreadth and vagueness.

GGGG. BECAUSE Rule 23(2) of the DPDP Rules empowers the Central Government to direct that a Data Fiduciary or intermediary shall not disclose the fact of furnishing information to the affected Data Principal, where such disclosure is considered likely to prejudicially affect "sovereignty and integrity of India" or "security of the State"

HHHH. BECAUSE the said provision introduces a secrecy regime by which an individual may never learn that their personal data has been accessed, demanded, or disclosed to the Government, thereby eliminating any meaningful opportunity to challenge such disclosure, seek legal remedy, or even exercise informational self-determination.

IIII. BECAUSE the imposition of such a secrecy obligation is disproportionate and unconstitutional since it operates without any requirement of judicial oversight, without any prescribed timeline, without a requirement of periodic review, and without affording the affected individual any procedural protection.

JJJJ. BECAUSE the impugned secrecy regime also has a chilling effect on the exercise of fundamental rights, including freedom of speech and freedom of the press, as it enables covert and unaccountable acquisition of information by the State.

KKKK. BECAUSE the DPDP Rules do not prescribe any procedure through which a Data Principal may seek disclosure of whether their personal data has been furnished to the Government under Section 36 read with Rule 23. The absence of any disclosure mechanism ensures that the power remains practically immune from accountability.

LLLL. BECAUSE the right to privacy necessarily includes the right to know when one's personal data has been accessed or disclosed, and the absence of any such procedural mechanism violates the minimum requirement of fairness, transparency, and accountability expected of a constitutionally compliant data protection framework.

MMMM. BECAUSE Section 36 of the DPDP Act read with Rule 23 and the Seventh Schedule does not provide any statutory limitation on the period for which personal data, once demanded and furnished to the Central Government, may be retained.

NNNN. BECAUSE the absence of any retention limitation, deletion requirement, or destruction mandate results in the creation of an indefinite and perpetual storage regime in the hands of the State, which is

fundamentally inconsistent with the constitutional principle of storage limitation and data minimisation, and fails the proportionality requirement laid down by this Hon'ble Court.

OOOO. BECAUSE in the absence of a statutory requirement for periodic review, destruction upon cessation of necessity, and maintenance of detailed records of access, Section 36 read with Rule 23 enables dragnet-style collection and indefinite retention of personal data, thereby facilitating mass surveillance and violating Articles 14 and 21 of the Constitution.

Failure to satisfy the Puttaswamy Test

PPPP. BECAUSE the impugned provisions are violative of the right to privacy and fail the standards as laid down in the case of ***Puttaswamy,*** where this Hon'ble Court held that where the State intends to infringe upon the right to privacy or aims to interfere with the exercise of the right, the interference must pass the the three-fold test of legality, necessity, and proportionality. The Hon'ble Apex Court held thus:

> *"310. State must nevertheless put into place a robust regime that ensures the fulfilment of a three-fold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). They emanate from the procedural and content-based mandate of Article 21. The first requirement that there must be a law in existence to justify an encroachment on privacy is an express requirement of Article 21. For, no person can be deprived of his life or personal liberty except in accordance with*

> *the procedure established by law. The existence of law is an essential requirement. Second, the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness. Legitimacy, as a postulate, involves a value judgment. Judicial review does not re-appreciate or second guess the value judgment of the legislature but is for deciding whether the aim which is sought to be pursued suffers from palpable or manifest arbitrariness. The third requirement ensures that the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law. Hence, the three-fold requirement for a valid law arises out of the mutual interdependence between the fundamental guarantees against arbitrariness on the one hand and the protection of life and personal liberty, on the other. The right to privacy, which is an intrinsic part of the right to life and liberty, and the freedoms embodied in Part III are subject to the same restraints which apply to those freedoms."*

QQQQ. BECAUSE the impugned provisions here fail to satisfy all three prongs of ***Puttaswamy*** test and are hence violative of the right to privacy under Article 21.

Legality

RRRR. BECAUSE the impugned provisions fail to meet the first ***Puttaswamy*** principle of legality or legal backing of the State action, as they are in contravention of the ***PUCL*** judgment which requires the mandatory existence of a public emergency or public safety conditions for passing any order for interception. The same is not made out in the impugned provisions, and the overly broad category of "the interest of sovereignty and integrity of India or security of the State" is used instead.

Necessity

SSSS. BECAUSE the impugned provisions fail to satisfy the second principle of the ***Puttaswamy*** test, which requires that any action which attempts to impinge upon a right to privacy must also be legitimate and necessary in a democratic society.

TTTT. BECAUSE the impugned provisions are not necessary as there exist less intrusive and more proportionate provisions for similar measures to be carried out under Section 69 of the IT Act, read with the Interception Rules, 2009. Sub-section (2) of Section 69 states that the procedure and safeguards for interception, monitoring or decryption would be prescribed through Rules to ensure that such interception and surveillance does not carry on unchecked.

Firstly, the directions for interception or monitoring or decryptions shall be issued by the competent

authority as per Rule 3 of the Interception Rules, 2009. The competent authority as defined under Rule 2(d) means the Secretary in the Ministry of Home Affairs in the case of the Central Government and the Secretary in-charge in the Home Department in the case of the State Government or Union Territory. No person other than the competent authority can issue such orders. However, in unavoidable circumstances, such orders may be issued by an officer not below the rank of Joint Secretary to the Government of India who has been duly authorised by the competent authority.

Further, Rule 8 of the Interception Rules, 2009 provides that the competent authority shall consider alternative means of acquiring the information before issuing such directions. Rule 10 of the Interception Rules, 2009 prescribes that the directions issued under Rule 3 of the Interception Rules, 2009 shall specify the name and the designation of the officer of the authorised agency and the use of the information disclosed.

Additionally, Rule 11 of the Interception Rules, 2009 provides that the directions issued shall remain in force for a period not exceeding sixty days, but they can be renewed from time to time for a period not exceeding the total of one hundred and eighty days.

UUUU. Finally, Rule 22 of the Interception Rules, 2009 provides for the Review Committee and mentions

that the Review Committee shall meet once in two months to review the directions issued under Rule 3 and record its findings whether they are in accordance with Rule 3 read with Section 69(2) of IT Act or not. Where the Committee is of the opinion that the directions are not in accordance with the provisions, it shall set aside the directions and may order the destruction of the copies including the corresponding electronic records of the intercepted or monitored or decrypted information.

Proportionality

VVVV. BECAUSE the impugned provisions lack the above mentioned safeguards, and are more intrusive in nature, thereby failing the third principle of proportionality under the ***Puttaswamy*** test.

WWWW. BECAUSE the impugned provisions grant the Central Government overbroad and unchecked powers to compel any Data Fiduciary or intermediary to hand over information on the grounds of "the interest of sovereignty and integrity of India or security of the State". This power is neither proportionate nor legitimate in the absence of situations demanding emergent actions or having the element of public safety concerns. Therefore, the provisions do not meet the second limb of the ***Puttaswamy*** test.

XXXX. BECAUSE in the absence of legality, necessity, proportionality, or procedural safeguards such as the

ones highlighted, the impugned provisions fail all prongs of the ***Puttaswamy*** test and are therefore liable to be struck down on the grounds that they are violative of Article 21 and the Right to Privacy guaranteed thereunder.

YYYY. BECAUSE as stated by the B.N. Srikrishna Committee Report, surveillance must be carried out with "a degree of transparency that can pass the muster of the ***Puttaswamy*** test of necessity, proportionality and due process" so as to "ensure scrutiny over the working of such agencies and infuse public accountability." In the present instance, the impugned provisions lack transparency, any sort of oversight, and therefore lack public accountability.

ZZZZ. BECAUSE the existence of Section 69 of the IT Act read with the Interception Rules, 2009 make Section 36 of the DPDP Act obsolete and the only foreseeable scenario where its existence can be tolerated is if it is put to the same safeguards as that of the IT Act and its subsequent rules. Even so, Section 36 of the DPDP Act, still remains a parallel provision, subject to be used arbitrarily and is liable to be struck down.

Infringement of Fundamental Right to Freedom of Speech and Expression

AAAAA. BECAUSE the impugned provisions of the DPDP Laws are violative of Article 19(1)(a) of the

Constitution of India as they give unbridled and arbitrary power to the Central Government to impose unchecked government surveillance and interception by bypassing statutes with safeguards and, depending on function creep under the DPDP Act, to intercept and gather information, directly affecting the fundamental right to freedom of speech and expression. .

BBBBB. BECAUSE the impugned provisions vest the Central Government with wide powers, including no provision to delete information after a certain period, no review committee, the ability to delete the orders for interception, decryption and monitoring along with the information thereby making legal challenges to the orders of unreasoned surveillance impossible.

CCCCC. BECAUSE Rule 23(2), which states that where the disclosure of furnishing of information as referred to in sub-rule (1) is likely to prejudicially affect the sovereignty and integrity of India or security of the State, the Central Government may require the Data Fiduciary or intermediary to not disclose such furnishing to the affected Data Principal or any other person except with the previous permission, in writing, of the authorised person, violates the consent-based architecture of the DPDP Act, as well as Article 19(1)(a) of the Constitution. The non-disclosure of such information is the denial of the freedom of speech

and expression, the position this Hon'ble Court approved in the judgment of ***Thalappalam Service Coop. Bank Ltd.*** **v.** ***State of Kerala*****,** (2013) 16 SCC 82. It was held that:

> *"55. The right to information also emanates from the fundamental right guaranteed to citizens under Article 19(1)(a) of the Constitution of India. The Constitution of India does not explicitly grant a right to information. In Bennett Coleman & Co. v. Union of India [(1972) 2 SCC 788] this Court observed that it is indisputable that by "freedom of press" meant the right of all citizens to speak, publish and express their views and freedom of speech and expression includes within its compass the right of all citizens to read and be informed. In Union of India v. Assn. for Democratic Reforms [(2002) 5 SCC 294] this Court held that the right to know about the antecedents including criminal past of the candidates contesting the election for Parliament and State Assembly is a very important and basic facet for survival of democracy and for this purpose, information about the candidates to be selected must be disclosed. In State of U.P. v. Raj Narain [(1975) 4 SCC 428], this Court recognised that the right to know is the right that flows from the right of freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution. In People's Union for Civil Liberties v. Union of India [(2003) 4 SCC 399], this Court observed that the "right to information is a facet of freedom of 'speech and expression' contained in Article 19(1)(a) of the Constitution of India. Right to information, thus, indisputably is a fundamental right". (SCC p. 494, para 45) so held in several judgments of this Court, which calls for no further elucidation."*

DDDDD. BECAUSE the Hon'ble Supreme Court in a catena of decisions has laid down that in interpreting a constitutional provision, the court should keep in mind the social setting of the country so as to show a complete consciousness and deep awareness of the growing requirements of the society, the increasing needs of the nation. The DPDP Act, ostensibly passed to protect the Right to Privacy as envisaged under ***Puttaswamy***, is now being used instead to violate that very right.

5. For the aforesaid reasons, the Petitioners submit that the aforementioned provisions of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 are unconstitutional, *ultra vires* the Constitution, violative of binding precedent, and contrary to India's constitutional and international obligations. The implementation of this intrusive and stifling framework directly affects the fundamental rights of citizens at large in this country, including the rights guaranteed under Articles 14, 19 and 21 of the Constitution. In particular, the impugned provisions have a chilling effect on the freedom of speech and expression under Article 19(1)(a), undermine the freedom to practise any profession, including the profession of journalism, under Article 19(1)(g), and violate the right to privacy and informational self-determination under Article 21. The Petitioners submit that the impugned framework further enables excessive executive discretion and weakens institutional safeguards, thereby undermining the doctrine of separation of powers and the rule of law.

6. The Petitioners are, therefore, constrained to approach this Hon'ble Court under Article 32 of the Constitution, seeking appropriate writs, orders and directions for quashing and setting aside Sections 7, 17(2)(a), 24, 36, 44(2)(a) and 44(3) of the Digital Personal Data Protection Act, 2023 and Rules 5, 6, 17, 18, 21 and 23 and the Second Schedule, Fifth Schedule, Sixth Schedule and Seventh Schedule of the Digital Personal Data Protection Rules, 2025, to the extent challenged herein, as being unconstitutional and violative of the fundamental rights guaranteed under Part III of the Constitution of India.

PRAYERS

In the above premises, it is prayed that this Hon'ble Court may be pleased:

a) Issue an appropriate writ, order or direction or declaration quashing and setting aside Sections 7, 17(2)(a), 19(3) 24, 36, 44(2)(a), and 44(3) of the Digital Personal Data Protection Act, 2023, to the extent challenged herein, as being unconstitutional, void and inoperative, and violative of Articles 14, 19(1)(a), 19(1)(g), 21 and 21A of the Constitution of India.

b) Issue an appropriate writ, order or direction, or declaration quashing and setting aside Rules 5, 6, 17, 18, 21 and 23, and the Second Schedule, Fifth Schedule, Sixth Schedule and Seventh Schedule of the Digital Personal Data Protection Rules, 2025, to the extent challenged herein, as being unconstitutional, void and inoperative, and violative of Articles 14, 19(1)(a), 19(1)(g), 21 and 21A of the Constitution of India.

c) Issue an appropriate writ, order or direction, or declaration quashing and setting aside Section 17(2) of the Digital Personal Data Protection Act, 2023, insofar as it empowers the Central Government to exempt any of its instrumentalities from the application of the provisions of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025.

d) Issue an appropriate writ, order or direction, or declaration quashing and setting aside the Second Schedule of the Digital Personal Data Protection Rules, 2025.

e) Issue an appropriate writ, order or direction, or declaration quashing and setting aside Section 44(2)(a) of the Digital Personal Data Protection Act, 2023, insofar as it extinguishes the right of affected persons to seek compensation or civil remedy for unlawful processing of personal data and/or data breach.

f) Issue an appropriate writ, order or direction, or declaration quashing and setting aside Section 44(3) of the Digital Personal Data Protection Act, 2023 insofar as it dilutes the right to information of the citizens of India.

g) Issue an appropriate writ, order or direction, or declaration quashing and setting aside Section 19(3) and Section 24 of the Digital Personal Data Protection Act, 2023 read with Rules 17, 18 and 21 and the Fifth and Sixth Schedules of the Digital Personal Data Protection Rules, 2025, insofar as they relate to the constitution, appointment, service conditions and functioning of the Data Protection Board of India.

h) Issue an appropriate writ, order or direction, or declaration directing the Respondent No. 1 to frame a constitutionally

compliant mechanism for appointment, tenure and service conditions of the Data Protection Board of India, ensuring its independence from executive control.

i) Issue an appropriate writ, order or direction, or declaration quashing and setting aside Section 36 of the Digital Personal Data Protection Act, 2023 read with Rule 23 and the Serial No. 1 of the Seventh Schedule of the Digital Personal Data Protection Rules, 2025.

j) Issue an appropriate writ, order or direction, or declaration directing the Respondent No. 1 to incorporate and notify a specific and proportionate exemption under the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 for processing of personal data for journalistic, editorial, investigative and public interest reporting purposes, including protection of journalistic sources. Alternatively, issue an appropriate writ, order or direction, or declaration quashing and setting aside Section 7 of the Digital Personal Data Protection Act, 2023, insofar as it fails to provide an exemption for processing of personal data for journalistic purposes.

FOR WHICH ACT OF KINDNESS, THE PETITIONER SHALL AS IN DUTY BOUND, EVER PRAY.

Drawn on: 04.02.2026

Drawn by:

Settled by:

Filed on:19.02.2026
Place: New Delhi

I.A. 66957/2026 517

IN THE HON'BLE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (C) NO. 275 of 2026

(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

[PUBLIC INTEREST LITIGATION]

IN THE MATTER OF:

GEETA SESHU & ANR …PETITIONERS

VERSUS

UNION OF INDIA & ORS. …RESPONDENTS

APPLICATION SEEKING EX-PARTE INTERIM RELIEF

TO
THE HON'BLE CHIEF JUSTICE OF INDIA AND
HIS COMPANION JUDGES OF
THE HON'BLE SUPREME COURT OF INDIA

THE HUMBLE PETITION OF
THE PETITIONER ABOVE NAMED

MOST RESPECTFULLY SHEWETH:

1. The Petitioners have filed the accompanying writ petition under Article 32 of the Constitution of India seeking an appropriate writ, order, direction or declaration

a) Strike down Sections 7, 17(2)(a), 24, 36, 44(2)(a) and 44(3) of the Digital Personal Data Protection Act, 2023, to the extent challenged herein;

b) Strike down Rules 5, 6, 17, 18, 21 and 23 and the Second Schedule, Fifth Schedule, Sixth Schedule and Seventh Schedule of the Digital Personal Data Protection Rules, 2025, to the extent challenged herein;

c) Strike down Section 17(2)(a) of the Digital Personal Data Protection Act, 2023, insofar as it empowers the Central Government to exempt any of its instrumentalities from the application of the provisions of the DPDP Act and the DPDP Rules;

d) Strike down Section 44(2)(a) of the Digital Personal Data Protection Act, 2023, insofar as it extinguishes the right of affected persons to seek compensation or civil remedy for unlawful processing of personal data and/or data breach;

e) Issue an appropriate writ, order or direction, quashing and setting aside Section 44(3) of the Digital Personal Data Protection Act, 2023 insofar as it dilutes the right to information of the citizens of India.

f) Strike down Section 24 of the Digital Personal Data Protection Act, 2023 read with Rules 17, 18 and 21 and the Fifth and Sixth Schedules of the DPDP Rules, 2025, insofar as they relate to the constitution, appointment, service conditions and functioning of the Data Protection Board of India;

g) Issue a writ in the nature of mandamus directing the Respondents to frame and notify a constitutionally compliant mechanism for appointment, tenure and

service conditions of the Data Protection Board of India, ensuring its independence from executive control;

h) Strike down Section 36 of the Digital Personal Data Protection Act, 2023 read with Rule 23 and the Seventh Schedule of the DPDP Rules, 2025;

i) Issue a writ in the nature of mandamus directing the Respondents to incorporate and notify a specific and proportionate exemption under the DPDP Act and DPDP Rules for processing of personal data for journalistic, editorial, investigative and public interest reporting purposes, including protection of journalistic sources.

2. The contents of the said petition are not repeated herein for the sake of brevity and thus the Applicants submit that the contents of the accompanying writ petition may be read as part and parcel of the instant application and crave leave of this Hon'ble court to refer and rely on the same.

3. It is submitted that the Petitioners have a *prima facie* case in their favour and balance of convicnec lies in their favour too.

4. It is submitted that grave *prejudice* will be caused to the Applicants if appropriate interim reliefs are not granted in the present facts and circumstances of the case.

5. That liberty is sought to refer and rely upon all the grounds urged in the accompanying writ petition as part of contentions to be raised during the time of hearing of the present application.

6. The present application is made *bonafide* and is just and necessary.

PRAYERS

It is, therefore, prayed that the Hon'ble Court may be pleased to:

a) Stay the operation of Section 24 of the Digital Personal Data Protection Act, 2023 read with Rules 17, 18 and 21 and the Fifth and Sixth Schedules of the Digital Personal Data Protection Rules, 2025, insofar as they relate to the constitution, appointment, service conditions and functioning of the Data Protection Board of India;

b) Stay the initiation and continuation of any process, procedure, notification, appointment, recruitment, administrative action, or any other steps undertaken by the Respondents for the purpose of constituting and operationalising the Data Protection Board of India, including but not limited to appointments of Chairperson and Members, framing of terms of service, staffing, and establishment of infrastructure, pursuant to the DPDP Act and the DPDP Rules;

c) Stay the operation of Section 17(2)(a) of the Digital Personal Data Protection Act, 2023, insofar as it empowers the Central Government to exempt any of its instrumentalities from the application of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 and consequently stay any notifications, orders or exemptions issued or sought to be issued thereunder;

d) Stay the operation and implementation of Rule 6 of the Digital Personal Data Protection Rules, 2025, insofar as it mandates retention of personal data and/or logs beyond what is strictly necessary for the purpose for which such data was collected, and pending final adjudication of the present writ petition;

e) Stay the operation and implementation of Section 36 of the Digital Personal Data Protection Act, 2023 read with Rule 23 and the Seventh Schedule of the Digital Personal Data Protection Rules, 2025, including any action initiated thereunder, insofar as the said provisions enable the Central Government to require Data Fiduciaries and intermediaries to furnish information, data, or records

without adequate safeguards and oversight;

f) Direct the Respondents to ensure that no coercive steps are taken against journalists, editors, media organisations, or persons engaged in journalistic activity for processing of personal data for journalistic, investigative, editorial or public interest reporting purposes, pending the final disposal of the present writ petition;

g) Direct the Respondents to maintain *status quo* and restrain them from bringing into force, enforcing, or operationalising the impugned provisions challenged in the present writ petition, including by issuance of any further notifications, rules, guidelines, exemptions, or executive directions, to the extent such provisions are scheduled to come into effect pursuant to the notified commencement dates and phased implementation under the DPDP Laws;

h) Pass any other order(s) as this Hon'ble Court may deem fit in the facts and circumstances of the case.

AND FOR THIS ACT OF KINDNESS THE PETITIONER SHALL EVER PRAY AS IS DUTY BOUND.

FILED BY

Filed On: 19.02.2026
Place: New Delhi

ADVOCATE FOR THE APPLICANTS