IN THE HON'BLE SUPREME COURT OF INDIA
ORIGINAL JURISDICTION

I.A. No. _____ of 2026

IN

WRIT PETITION(S) (CIVIL) NO. 177 OF 2026

IN THE MATTER OF:

VENKATESH NAYAK PETITIONER

VERSUS

UNION OF INDIA RESPONDENT

AND IN THE MATTER OF:

FOUNDATION OF DATA PRIVACY PROFESSIONALS IN INDIA

...APPLICANT/INTERVENER

AN APPLICATION FOR INTERVENTION

PAPER-BOOK
(FOR INDEX, KINDLY SEE INSIDE)

ADVOCATE FOR APPLICANT: RAGHVENDRA KUMAR

INDEX

IN THE HON'BLE SUPREME COURT OF INDIA
ORIGINAL JURISDICTION

I.A. No. _____ of 2026
IN
WRIT PETITION(S) (CIVIL) NO. 177 OF 2026

IN THE MATTER OF:

VENKATESH NAYAK — PETITIONER

VERSUS

UNION OF INDIA — RESPONDENT

AND

IN THE MATTER OF:

FOUNDATION OF DATA PRIVACY PROFESSIONALS IN INDIA
(Through its Chairman & AR,
Mr. Vijayashankar Nagaraja Rao)
Address: 37, 20th Main Road, BSK First Stage,
Bengaluru, Karnataka-560050

INTERVENER/ APPLICANT

APPLICATION FOR INTERVENTION ON BEHALF OF THE ABOVE-MENTIONED APPLICANT

TO,

THE HON'BLE CHIEF JUSTICE OF INDIA

AND COMPANION JUDGES OF THE HON'BLE

SUPREME COURT OF INDIA.

THE HUMBLE PETITION OF THE

APPLICANTS ABOVE-NAMED

MOST RESPECTFULLY SHOWETH:

1. The above-captioned writ petition broadly challenges the constitutional validity of certain provisions of the Digital Personal Data Protection Act, 2023 ***("DPDPA")***, which is being heard by this Hon'ble Court along with two other connected matters, namely W.P.(C) No.211/2026 titled *"The Reporters Collective Trust & Anr. Vs. Union of India & Ors."* and W.P.(C) No.212/2026 titled *"National Campaign for Peoples Rights to Information Vs. Union of India"* raising similar issues.

2. The Applicant, the Foundation of Data Protection Professionals in India **(FDPPI)**, is a not-for-profit organization incorporated as a Section 8 Company limited by Guarantees registered in 2018 under the Companies Act, 2013. The Applicant organization is engaged in promoting awareness, professional development, research and policy discourse relating to data protection, privacy governance and digital regulatory frameworks in India. The Applicant represents a large community of professionals, researchers, compliance practitioners and industry stakeholders engaged in implementing data protection frameworks across India.

   A copy of Certificate of Incorporation of the Applicant is annexed herewith as **ANNEXURE A-1 (Page No. 12)**.

3. The Chairman of the Applicant organization is a cyber law researcher and public policy analyst who has been associated with the development of cyber law and data protection discourse in India for over two decades and is the author of many books on Cyber Law and Data Protection with the latest

being “Wisdom Companion for Champions of DPDPA Compliance”, which covers the DPDPA Rules of November 13,2025 in great detail. He is also the architect of Digital Governance and Protection Standard of India **(DGPSI)**, a framework of compliance of DPDPA. The framework provides a structured guideline for compliance of DPDPA.

A copy of Compendium of Earlier Articles in www.naavi.org is annexed herewith as **ANNEXURE A-2 (Pages 13 to 45).**

PURPOSE OF INTERVENTION

4. That one of petition tagged along with the captioned writ petition has prayed for the complete invalidation of both the Act passed by the Parliament in August 2023 and the Rules notified on November 13, 2025.

5. That one of the issues raised by the petitioners is concerns relating to amendments made to Section 8(1)(j) of the Right to Information Act, 2005 through the DPDPA, not declaring “Journalists” as a category to whom provisions of DPDPA should be exempted and exemptions provided for law enforcement and the power of the Government to call for information from the regulated entities.

6. That the petitions, in their own understandings, have raised issues of substantial public importance concerning the balance between informational privacy, transparency and digital governance.

7. That the Applicant seeks the leave of this Hon’ble Court to intervene in the present proceedings in order to place before this Hon’ble Court the perspective of professionals and

practitioners involved in the field of data protection, compliance and governance.

8. That the Applicant submits that the outcome of the present proceedings will have a significant impact on the development of India's data protection ecosystem and on the practical implementation of the statutory framework established under the DPDPA.

9. That in 2006, a Bill namely "Personal Data Protection Bill, 2006" was introduced in the then Parliament along with the "Information Technology Amendment Bill 2006". While the Information Technology Amendment Bill went onto be enacted later in 2008, the Personal Data Protection Bill, 2006 was allowed to lapse. However, the Information Technology Amendment Act 2008 introduced certain provisions in Information Technology Act 2000, for personal data protection purpose in the form of Sections 43A and others. The current Digital Personal Data Protection Act, 2023, which is the subject matter of the current discussions replaces Section 43A with a more elaborate Personal Data Protection Eco system.

10. That in due course, this Hon'ble Court in ***Justice K.S. Puttaswamy (Retd.) & Anr. vs Union of India (2017)*** recognized the right to privacy as a fundamental right under the Constitution of India. Following the said judgment and several years of legislative deliberation, Parliament enacted the Digital Personal Data Protection Act, 2023 (DPDPA 2023).

11. That the DPDPA seeks to protect individuals' personal data while enabling lawful processing necessary for governance, economic activity and digital innovation.

12. That The DPDPA 2023 in its Preamble has declared its intention to protect the Right of the individuals to protect their personal data through measures to regulate the Personal Data processing industry adopting the globally unique “Fiduciary” approach to Personal Data protection.

13. That the Applicant submits that the DPDPA is a comprehensive regulatory framework, which establishes *inter alia*:

(a) rights of individuals (Data Principals),

(b) obligations of entities processing personal data (Data Fiduciaries),

(c) consent management mechanisms,

(d) breach notification requirements, and

(e) regulatory oversight through the Data Protection Board of India.

14. That the entire framework created by the Act is designed to address risks arising from large-scale digital data processing in modern information systems.

15. That Applicant endorses that Balancing Constitutional Rights in any legal framework is tough ask and the same situation was faced while drafting this Personal Data Protection act.

16. That the Applicant respectfully submits that both privacy and transparency are important constitutional values recognized under Articles 19 and 21 of the Constitution. The Legislative policy necessarily involves balancing these values in light of evolving technological realities. The DPDPA represents Parliament’s attempt to harmonize the right to privacy with the public interest in transparency and governance. DPDPA is a legislation to provide a regulatory Framework re-defining the

"Sensitive Personal Data Protection guidelines currently available under Section 43A of the Information Technology Act, 2000. DPDPA has widened the compliance requirements under Section 43A of Information Technology Act, 2000 by extending it to Government organizations from "Body Corporates", introducing accountability for the Data Fiduciaries and providing for a regulatory board in the form of Data Protection Board with a deterrent penalty system.

17. That it needs to be understood that the regulations under the Act are generally structured on the basis of "Purpose of Processing" and since it has to ensure preservation of the duty of the Government to protect National Security, Sovereignty and Integrity of the State etc. as provided in the Constitution, certain exemptions have been provided under the Act with necessary in-built security safeguards.

18. **Regarding R.T.I. Concerns:** The Applicant submits that concerns regarding the alleged dilution of the RTI regime require careful constitutional analysis avoiding a speculative exaggeration of the possible misuse of the proposed changes. The amendment relating to Section 8(1)(j) of the RTI Act seeks to prevent injudicious disclosure of personal data held by public authorities where such disclosure may infringe privacy rights and bring upon liabilities under Section 33 of the DPDPA on the Government department. It is respectfully submitted that "Exemptions" under the Act for the Government are purpose based and does not extend to exemption on penalties. If therefore during an RTI reply, the department knowingly or inadvertently infringes on the privacy of a citizen, it is open for a complaint under DPDPA

resulting in the penalties under Section 33. In such an event where a liability is fixed under DPDPA on the entity revealing the information to the RTI applicant, such applicant may not take any responsibility for indemnifying the department for having been instrumental in creating such a liability. The Applicant respectfully submits that the RTI framework must be interpreted in a manner consistent with the constitutional recognition of privacy as a fundamental right. It is submitted that when RTI-2005 was enacted, Right to Privacy was not considered as a "Fundamental Right" and it was only with the ***Puttaswamy*** Judgement that "Right to privacy" became a "Fundamental Right" to be protected along with the Right to Information warranting a change in the RTI-2005 provisions to the extent necessary to balance the two rights and which is evident from these amendments.

19. That India today hosts one of the largest digital ecosystems in the world, involving extensive processing of personal data across public and private sectors. The DPDPA provides a much-needed regulatory architecture for safeguarding personal data and establishing accountability for entities processing such data. Striking down or suspending the operation of the Act would create a regulatory vacuum in relation to digital personal data protection. It is important for the global commercial world to recognize that the Indian judicial system also supports the new law.

20. That it is a settled principle of constitutional jurisprudence that courts ordinarily prefer interpretative approaches such as harmonious construction and reading down in order to preserve legislative intent.

21. That if this Hon'ble Court finds any ambiguity or concern in the impugned provisions, such issues may be addressed through appropriate interpretative guidance without invalidating the entire statutory framework.

22. That the Applicant has already prepared a set of recommendations which are provided in an annexure to meet the concerns before the Hon'ble Court in the current petition.

23. That thus this Hon'ble Court has issued notices to i) Union of India; ii) Ministry of Law and Justice; iii) Ministry of Personnel/ Public Grievance and Pensions.

24. That the present Applicant organization has been actively engaged in developing compliance frameworks, professional training programs and policy discussions relating to data protection in India and hence the Applicant is well placed to assist this Hon'ble Court in interpreting the practical implications of the statutory framework created under the DPDPA.

25. That the rights and interests of the present Applicant are mostly similar as that of the Union of India and Applicant/ Intervener wants to assist the Union of India.

26. That the present application is being filed *bona fide* and in the interest of justice with a view to protect right to privacy of all Data Principals in India and to assist this Hon'ble Court by throwing more light with Applicant organisation's experience and expertise.

27. The Applicant states that no other application seeking similar relief(s) has been filed by the Applicant in any other Court.

PRAYER

It is therefore, most respectfully prayed that this Hon'ble Court may be pleased to:

a) Permit the Applicant to intervene in the Writ Petition (Civil) No. 177/2026;

b) Permit the Applicant to make written and oral submissions in the Writ Petition (Civil) No. 177/2026;

c) Pass such other order or orders that this Hon'ble Court may deem fit and proper in the facts and circumstances of the case.

AND FOR THIS ACT OF KINDNESS THE APPLICANT AS IN DUTY BOUND SHALL EVER PRAY.

FILED BY:

DATE: 13.03.2026

(RAGHVENDRA KUMAR)
ADVOCATE FOR THE APPLICANT

IN THE SUPREME COURT OF INDIA
ORIGINAL JURISDICTION

I.A. NO. OF 2026
IN
WRIT PETITION (CIVIL) NO. 177 OF 2026

IN THE MATTER OF:

Venkatesh Nayak ...Petitioner(s)

Versus

Union of India ...Respondent(s)

AND IN THE MATTER OF:

FDPPI ...Interveners/Applicants
(Foundation of Data Protection Professionals in India)

AFFIDAVIT

I, Vijayashankar Nagaraja Rao, S/o Shri S.Nagaraja Rao, aged about 72 years, resident of 37, 20th main, BSK First Stage, Bangalore 56050, do hereby solemnly affirm and declare as under:

1. That I am the Applicant/Intervenerin the captioned matter and as such, I am fully conversant with the facts and circumstances of the case and hence competent to swear this affidavit.

2. That I have gone through and understood the contents of the instant application, which are true to my knowledge and belief.Nothing material has been concealed by me nor any material is false.

3. That the Annexure(s)to the Interlocutory Application are the true copies of their respective originals.

NOTARY S.N. MADHU ... OF INDIA

For Foundation of Data Protection Professionals in India

Chairman/Director

Deponent

DEPONENT

VERIFICATION:

I, the deponent above-named, do hereby verify that averments made in this affidavit from paras 1 to 3 are true to my knowledge and belief. No part of it is false and nothing material has been concealed therefrom.

Verified at Bengaluru on this 13th day of March, 2026.

For Foundation of Data Protection Professionals in India

Chairman/Director

DEPONENT

SWORN TO BEFORE ME
S.N. MADHU
Advocate & Notary Public
Government of India
934-A, 2nd 'A' Cross, 3rd Phase,
6th Block, BCK 3rd Stage, Kathriguppe
Near Ayyappa Temple, Bangalore-560 085.

W.D.L: 2026

सत्यमेव जयते

GOVERNMENT OF INDIA
MINISTRY OF CORPORATE AFFAIRS

Central Registration Centre

Certificate of Incorporation

[Pursuant to sub-section (2) of section 7 of the Companies Act, 2013 (18 of 2013) and rule 18 of the Companies (Incorporation) Rules, 2014]

I hereby certify that FOUNDATION OF DATA PROTECTION PROFESSIONALS IN INDIA is incorporated on this Seventeenth day of September Two thousand eighteen under the Companies Act, 2013 (18 of 2013) and that the company is limited by guarantee.

The Corporate Identity Number of the company is U72501KA2018NPL116325.

The Permanent Account Number (PAN) of the company is **AADCF4963H**

The Tax Deduction and Collection Account Number (TAN) of the company is **BLRF04845B***

Given under my hand at Manesar this Seventeenth day of September Two thousand eighteen .

DS MINISTRY OF CORPORATE AFFAIRS 27

Digital Signature Certificate
Mr. Wagh Tushar Mohan

For and on behalf of the Jurisdictional Registrar of Companies
Registrar of Companies
Central Registration Centre

Disclaimer: This certificate only evidences incorporation of the company on the basis of documents and declarations of the applicant(s). This certificate is neither a license nor permission to conduct business or solicit deposits or funds from public. Permission of sector regulator is necessary wherever required. Registration status and other details of the company can be verified on www.mca.gov.in

---

Mailing Address as per record available in Registrar of Companies office:

FOUNDATION OF DATA PROTECTION PROFESSIONALS IN INDIA
No. 37/5, Ujvala, 20th Main,, Banashankari 1st Stage, II Block,
BANGALORE, Bangalore, Karnataka, India, 560050

* as issued by the Income Tax Department

Naavi.org

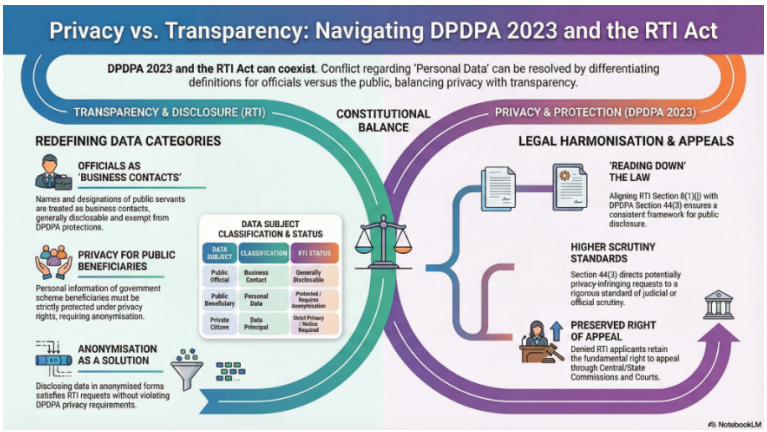
Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Compendium of Earlier Articles in www.naavi.org

1. Whose Privacy are the Petitioners of DPDPA Challenge Brigade are protecting?



The petitions filed in Supreme Court against DPDPA 2023 mainly revolves around Section 44(3) and thee conflict with RTI Act. Petition of Mr Venkatesh Nayak restricts its prayer to the declaration that Section 44(3) is Ultra-vires the Articles 14,19 and 21 of the Constitution. Additionally, it argues that Sections 17(1)(c),17(2) , 33(1) and 36 as well as Rule 23(2) as ultra-vires the constitution.

In this context let us see whose Personal data is at stake in an RTI application. Is it the personal data of the official who was involved in any of the decisions or Is it the personal data of the public whose personal data is sought to be disclosed in the reply.

We also should verify if there are already grounds in RTI act itself where the provision of information can be rejected even before invoking Section 44(3) of DPDPA 2023.

Let us look at the personal information involved of the official. The official is a public servant and once he is appointed for a public post, the information becomes a matter “Made public” and hence is not covered under Section 44(3) of the Act. This is a matter of interpretation of “Personal Data” which should exclude data that is made public as a “Business Contact”. The official’s name and designation is similar to “Business Contact” and hence is outside the scope of DPDPA.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

However, the personal information of the beneficiaries of a Government project which is part of the information sought need to be considered as subject to Privacy Rights.

This can be anonymized before release in which case there is no violation of DPDPA.

Hence if the Government considers that no personal information is disclosed under Section 8(1)(j) other than in Anonymized form, the dispute would vanish.

This can be done through a reading down on both 8(1)(j) of RTI act and Sec 44(3) of DPDPA stating that disclosure of information of public during a RTI disclosure shall be consistent with the DPDPA under Section 7(d) and 17(2) (b) .

Under Section 17(2)(b) there is an additional restriction that says that the processing does not include making a decision that affects the data principal. Hence if the objective of the RTI activist is to stop any benefits under any scheme then the affected Data Principals have to be made parties to a legal request of their information and the department has to send notices to all the beneficiaries that a request has been made about their personal data. Since this would in most cases involve a disproportionate effort, the denial of information is justified under Section 8/9 of the RTI act itself.

In protecting the RTI of the activist, Judiciary cannot deny the Right to privacy of persons who are pawns in the dispute between the RTI activist and the Government. If the petitioners are comfortable with Section 9 of RTI act which enables disclosure of information which could result in infringement of Copyright, there is no logic why they should be excessively concerned about the amendment to 8(1)(j) which protects the information property rights of a data principal who is a beneficiary of a Government scheme.

What Section 44(3) has done is to remove the burden on the PIO to decide under Section 8(2) of RTI act that "public interest in disclosure outweighs the harm to the protected interests.". This could however be a part of a judicial review and the RTI applicant who is denied information can proceed to challenge the denial in a Court of law.

If necessary, he can appeal on the decision to the CPIO and the State/Central Commission. Hence denial of any information under Section 44(3) amendment does not infringe any right fundamental or otherwise, linked to Article 14,19,21 or otherwise. It only diverts one stream of information which the PIO considers prima-facie to infringe on the privacy of a citizen to a higher standard of scrutiny.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

As indicated earlier, the above view does not apply to the identity of the officials who are discharging their duties in an official capacity.

If there is any information of the official beyond the identity which can be used for alleging corruption etc., then his own privacy rights should naturally be applicable along with the intention of the RTI being treated as "litigation".

Hence the petition of Mr Venkatesh Nayak and others on Section 44(3) can be resolved with a clarification and reading down of the section that it does not apply to the disclosure of the names of the decision makers but only applies to the information of the public.

We shall discuss 17(1)(c), 17(2), 33(1) and 36 as well as Rule 23(2) separately in our subsequent articles.

We need to debate if we don't have our right to get DPDPA and DPDPA Rules retained in public interest as much as the few petitioners want it to be scrapped. The Supreme Court has to settle once for all how it can decide on the applications of a few advocates claiming to be representing public interest and not involve the larger public to express their objections. Who is representing the "Real Public Interest" should be considered before entertaining the applications of the select few who always oppose the Government. If the background of the petitioners are checked, it would be clear that they only oppose the Government and it is not clear if their intentions are positive to the Country. The real public interest is therefore not represented by them as much as what Naavi or FDPPI represents.

I recall that in one of the old (around the year 2000) cases in Mumbai High Court on Cyber Cafe regulations, the Mumbai High Court had published an article of Naavi.org (at that time naavi.com) along with some other information and had invited the public to send their views. Without any intervention the Court had involved the "Real Public" to participate in the decision. Supreme Court should follow similar principles and should not allow the few petitioners to hijack the "Right to Represent the public".

I am a member of the public and I do not consider the petitioners to be representing my View.

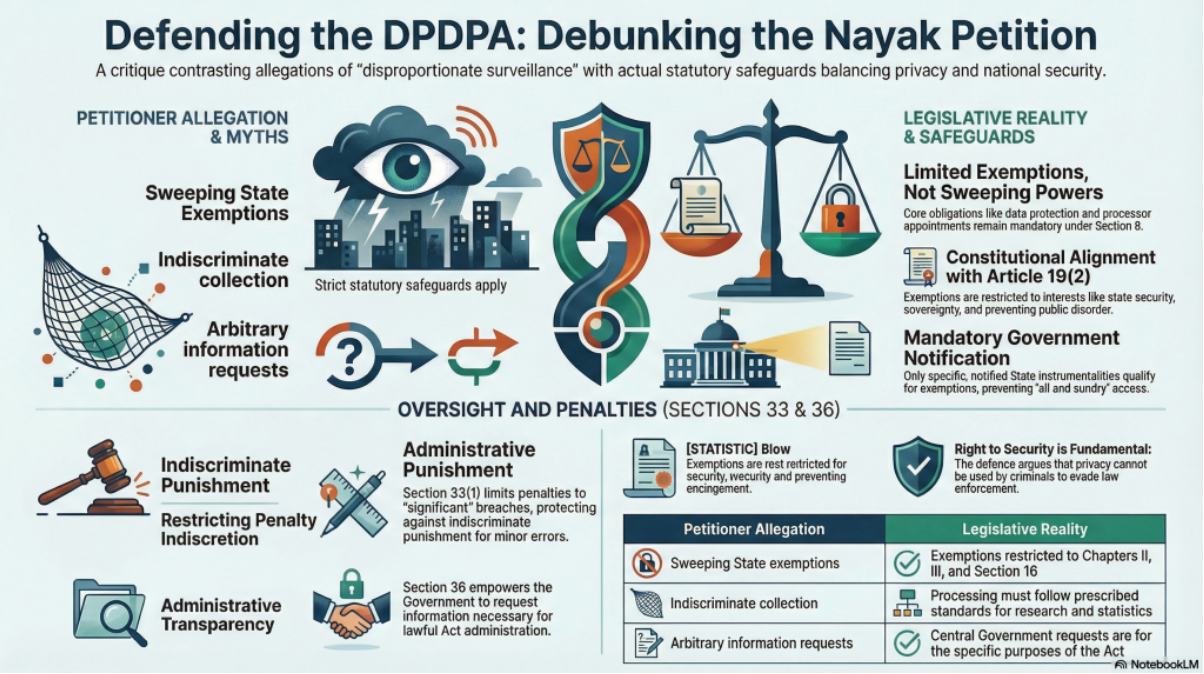
Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

2 .Nothing is wrong with Section 17(1)(c) and 17(2)



Let us now continue on our discussion on the petition of Mr Venkatesh Nayak on Sections 17(1) (c) and 17(2) as well as 33(1) and 36 which are sought to be scrapped.

The petition says that Sections 17(1)(c) and 17(2)(a) and 17(2)(b) empowers "Disproportionate surveillance" by granting sweeping exemptions both to State and Non-State instrumentalities" without any objective scrutiny or statutory responsibility, under garb of crime prevention. It also alleges that the collection can be indiscriminate and can be used for policing using predictive algorithms. The lack of safeguards is allegedly failing the proportionality test. The petitioner states that there is no legitimate reason to exempt state actors from being bound by statutory obligations under the DPDPA. even for research and statistical purposes.

Let us recall what the two sections state.

Section 17(1)(c): The provisions of **Chapter II, except sub-sections (1) and (5) of section 8**, and those of **Chapter III and section 16 shall not apply** where—personal data is processed

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

in the interest of **prevention, detection, investigation or prosecution of any offence or contravention of any law** for the time being in force in India;

Section 17(2)

The **provisions of this Act shall not apply** in respect of the processing of personal data—

(a) by such **instrumentality of the State as the Central Government may notify, 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 relating to any of these,** and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and

(b) necessary for **research, archiving or statistical purposes** if the personal data is **not to be used to take any decision** specific to a Data Principal and such processing is carried on **in accordance with such standards** as may be prescribed.

It appears that the learned counsels have either not read the sections diligently or trying to mislead the Court with wrong statements.

Section 17(1)

Firstly, Section 17 (1) does not provide "Sweeping powers". The powers are restricted to exemptions under Chapter II which relate to consent and other obligations, Chapter III which relates to Right and Section which relates to Cross border transfer. Even under Chapter II Sections provisions of 8(1) and Sectio 8(5) are not exempted.

Section 8(1) relates to the appointment of a data processor and Section 8(5) relates to protection of personal data.

The petitioner's concern that the data collected for law enforcement would be algorithmically analysed to create biases etc is a pure figment of imagination particularly without the processing being done by private sector data processors or joint data fiduciaries.

Further the purpose related to **prevention, detection, investigation or prosecution of any offence or contravention of any law** for the time being in force in India is directly pointing to constitutional exceptions under Article 19(2) which even Justice Puttaswamy Judgement has recognized. Limited exemptions related to exceptions under Constitutions cannot be called "Sweeping exemptions". If the petitioner is serious, we can also state that they are making sweeping statements to mislead the Court and implying speculative fears which does not exist.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

We should also note that the same exemptions of Chapter II except Section 8(1) and 8(5), Chapter III and Section 16 is also available to many other instances by the private sector including notified startups, during mergers and acquisitions and during recovery of bad debts by financial institutions. Does the petitioner also allege that these private sector agencies also enjoy sweeping powers of surveillance?

It appears that the petitioners have failed to understand the exemptions properly.

Section 17(2)

Now let us turn our attention to Section 17(2) which states

The **provisions of this Act shall not apply** in respect of the processing of personal data—

(a) by such **instrumentality of the State as the Central Government may notify, 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 relating to any of these,** and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and

(b) necessary for **research, archiving or statistical purposes** if the personal data is **not to be used to take any decision** specific to a Data Principal and such processing is carried on **in accordance with such standards** as may be prescribed.

Have the petitioners observed that for this exemption, the instrumentalities of the State also have to be "Notified". It does not include all and sundry instruments of state. Further, such instrumentalities of state should be processing data in the interest of sovereignty and integrity of India etc.. Which are exceptions under Article 19(2).

Where is the exemption to "Non State Instrumentalities" as mentioned in Ground Y of the petition (page 30) and where is any definition of a "Non State Instrumentality"?

The objection under Ground Y deserves a summary rejection.

For the purpose of research, archiving or statistical purpose, the exemption is limited to instances where the data is not used to take any decisions specific to a data principal. Further such data has to be processed subject to standards that have been prescribed under Rule 5 - second schedule.

Hence under both Sections 17(1) and 17(2) there are enough safeguards to prevent misuse of data collected under these exemptions.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Why Law Enforcement Agencies need a free hand

I would like to further reiterate, that the statement in page 31 of Venkatesh Nayak petition para AA that "There is no legitimate reason to exempt the state actors " for security purposes is a complete nonsense. It is the duty of a Government to secure the citizens and Right to Security is a fundamental right of citizens that the Government must protect. There is no right to criminals to use Privacy as an excuse to hide their activities and for the petitioners to support such criminals by raising objections to laws that help mitigate crime risk to the society.

Hence the grounds for considering Sections 17(1) and 17(2) as unconstitutional is not tenable.

Section 33(1)

Section 33(1) states

"If the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may, after giving the person an opportunity of being heard, impose such monetary penalty specified in the Schedule."

We don't know what the petitioners want if there is non compliance. Is it wrong for the law to specify a penalty?

Petitioners harp on the use of the word "Significant Data Breach". This actually restricts the powers of the Board that for insignificant data breaches, Board should not use the penalty provisions indiscriminately.

Naavi.org has suggested methods including the "Valuation of Data" as a measure of the harm caused and the decision if any is appealable.

Hence the objection deserves summary rejection .

Section 36

Section 36 states

" 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"

Again the petitioners simply speculate that the section is arbitrary. The Central Government is the administrator of the law and would require many types of information both from the Board as well as the Data Fiduciaries. Claiming that this is "Arbitrary", "Excessive", "amenable for abuse" etc is a play of words that has no relevance to the real concerns of the public."

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

In summary the petition lacks genuine grounds for challenging either Section 44(3) or Section 17(1) or 1792) or 33 or 36.

Let us watch further developments in this regard.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

3 Reporter's Collective Trust prayer that DPDPA should be scrapped is manifestly arbitrary.

The petition of Mr Venkatesh Nayak against DPDPA was restrained in praying only for Section 44(3) removal and a few other sections, which we have discussed in detail in the previous series of articles.

In comparison, the petition of the Reporter's Collective Trust and Mr Nitin Sethi is conspicuous with its summary demand for declaring the whole of DPDPA 2023 and the whole of the Rules as void.

The demand is ridiculously excessive and indicates no intention of real concern on public interest but reflects only the anti Government agenda to stop whatever good can happen. It is difficult to understand how petitioners call themselves as supporters of Privacy when they are trying to dismantle the very law meant to protect privacy.

We all know that no law is perfect. Some times laws need to be explained through the rules and even amended in a short time. In a complicated law like DPDPA which seeks to balance multiple rights under the constitution, differences are inevitable and we should learn to manage them rather than try to scuttle the law itself.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Wisemen warn "Don't Cutoff your nose if you have Cold". Unfortunately the petitioners who want the act to be scrapped because of some disagreements have not heard of this proverb.

This petition has highlighted the following concerns/view points that can be contested..

1. Right to Information is a fundamental right under Article 19(1)(a) as per earlier Supreme Court judgements.
2. Right to information is essential for carrying out the function of a Journalist and the Act does not provide exemption for journalists.
3. Amendment in Section 44(3) has no legitimate aim under Article 19(2)
4. Proposed amendment interferes with the social audits that a journalist wants to conduct
5. DPDPA applies only to digital information where as RTI applies to all kinds of records and hence DPDPA provision is unreasonable.
6. Disclosure under Section 8(2) of RTI act is discretionary and 8(1)(j) offers a better standard.
7. K S Puttaswamy judgement should not apply to public purpose activities including journalism.
8. Exemption for research under Section 17(2)(b) is not applicable to journalistic reports
9. Section 12 mandates immediate deletion on withdrawal of consent, evidence of a journalistic report may be not available for post facto validation.
10. Whole of the Act and the Rules are void for "Vagueness".
11. Though Section 17(5) provides for a provision for exemption, Central Government does not have powers to exempt for journalistic purpose.
12. Government calling for information from a data fiduciary is violative of the constitution and gives raise to "Potential for Abuse".
13. Even when a disclosure of personal information is prejudicial to the sovereignty and integrity of India, it cannot be prevented from being released under RTI.
14. Section 36 enables "Unreasonable data searches" and hence against the Puttaswamy judgement

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

15. Because the Central Government has a range of less intrusive alternatives including obtaining independent authorization from a Court, there is no need for Section 36.
16. Data Protection Board lacks independence
17. DPB functioning as a digital office is exclusionary.
18. Penalties from Rs 50 crores to Rs 250 crores are exaggeratory.

We appreciate the ingenuity of the petitioners in picking out very many points out of the act and the rules to be objected to, there are umpteen contradictions within the petition. In some cases they swear by the Puttaswamy judgement and in some cases they want it to be violated.

The net impression is that this petitioner does not tolerate the existence of the Government itself and does not want the Government to have any powers of Governance. They respect Puttaswamy judgment but want the Act to be scrapped. The argument are highly speculative and does not merit even basic consideration.

The only point they make is “Journalism should have some exemptions”. They admit that the act has the power of exemption but still claim that Government does not have the power. The petitioners are confused about what they want and express it with clarity.

This petition deserves to be rejected with a directive to correct and resubmit making it more specific, avoiding self contradictions.

We will continue our discussions on some of the individual points and highlight the contradictions.

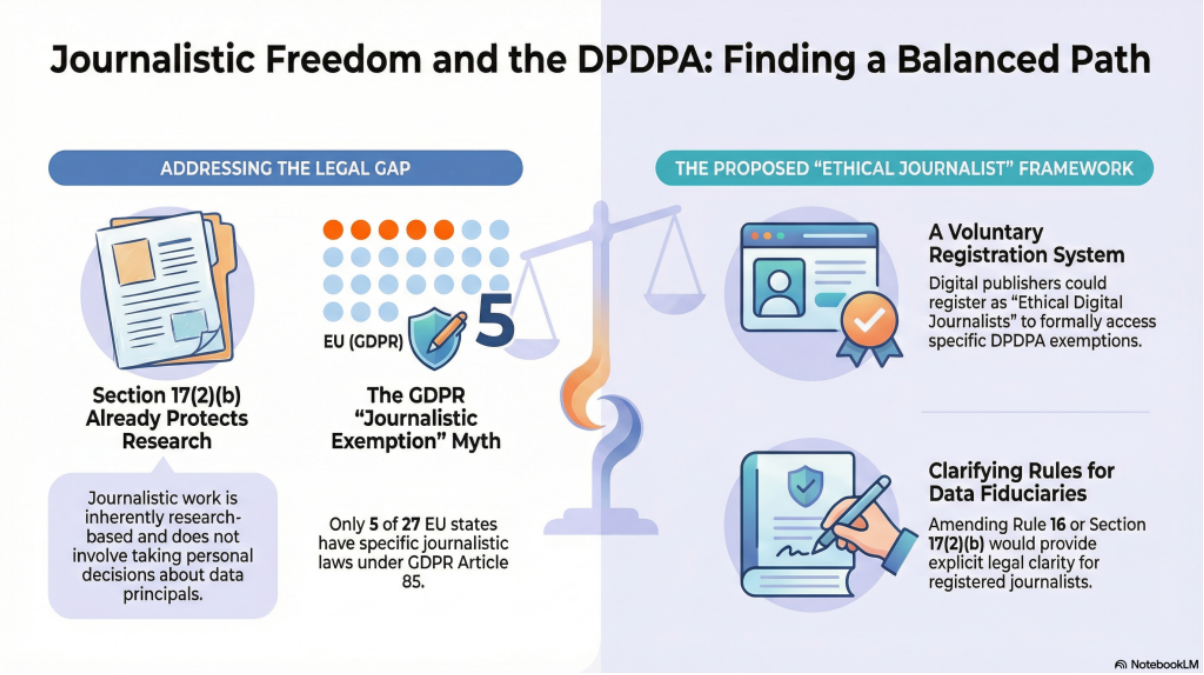
Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

4 .Are the "Scrap DPDPA Brigade" suggesting introduction of Registration of journalists by Government of India?



The petitioners who are challenging DPDPA in Supreme Court have one specific demand that they should be provided exemption from the provisions of DPDPA.

If we go through the petition of the Reporter's Collective, it provides an elaborate argument why the Act should be scrapped because it does not provide exemption to journalists.

The petition however acknowledges that there is exemption for "Research" but it concludes that this does not apply to Journalistic research. the petition also acknowledges that the Government has powers to exempt any class of data fiduciaries or data from any of the provisions of the Act under Section 17(5) but contends that this cannot be applied to journalists. Hence the only remedy they suggest is to declare the Act and the Rules as Void. The petitioner has not provided any suggestions on how their concern can be remedied without scrapping the law itself.

The demand is arbitrary and indicates a malicious intention to stop the progressive legislation.

The petitioners try to project GDPR as a reference to state that exemptions for Journalists are adopted in EU. This is an incomplete statement which is meant to mislead the Court.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Article 85 of GDPR, states as follows

Article 85: 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.

We should note that GDPR only empowers the member states to follow their own laws related to journalists. As of date, it appears that only the following States have specific laws made in this regard.

- **Austria**
- **Belgium**
- **Bulgaria**
- **Cyprus**
- **Czech Republic**

This means that there are other 22 States of the EU which have not followed Article 85 of GDPR.

In most countries exemptions are provided on a case to case basis and with certain eligibility criteria such as “Registered Journalists”.

Are the petitioners ready for the Government or DPB to introduce a “Registration System”? for Journalists to be exempted from DPDPA?

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

It would not be a bad idea to introduce a registration system for all "Digital Journalists" who want to be provided a recognition with an exemption from DPDPA.

We remember that Mr Kapil Sibal himself when he was the Minister in the Government of India had suggested that all bloggers should be registered with the Government.

Some time back the MeitY had introduced self regulation of digital media and had proposed online registration of digital publishers.

This system can now be pursued and registered Digital Publishers including YouTube bloggers can be given an option to register as "Ethical Digital Journalists" who will abide by certain rules and can also avail the exemptions from certain provisions of DPDPA for their journalistic research and publication.

What is required is to add an explanation to the Section Rule 16 of DPDPA Rules-Nov 13, (Second schedule) or add an additional rule for Section 17(2)(b) and make it applicable only to registered journalists.

Section 17(2)(b) which states:

The provisions of this Act shall not apply in respect of the processing of personal data— necessary for research, archiving or statistical purposes if the personal data ***is not to be used to take any decision specific to a Data Principal*** *and such processing is carried on in accordance with such standards as may be prescribed.*

Since a journalist does not take any decision about the data principal, his research confined to journalism is already exempted under this section. Whether the research is a fact finding research or an investigative research or a RTI research, as long as the intention is limited to "Research" this section is a sufficient protection to journalism.

Hence there is no reason to tamper with the law any further.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

5. DPDPA and Conformance to Puttaswamy Judgement

Above picture is representative and has been created using Nano banana AI tool

The petitions from the Scrap DPDPA Brigade in Supreme Court refers to DPDPA 2023 and the Rules as not being in conformity with the famous K S Puttaswamy Judgement of the Supreme Court of 24th August 2017. (KSP judgement)

The essence of the decision in the case of KSP was that

"Privacy is a fundamental Right under the constitution and is part of Article 21 of the Constitution subject to the reasonable restrictions under Article 19(2). "

The bench however did not define Privacy nor gave any restrictive boundaries to the Right to privacy whether it is restricted to Information Privacy. It however extensively noted the risks related in information privacy. In its directions, it stopped at stating that the Right is part of the fundamental Rights and parts of M P Sharma judgment and Kharak Singh judgement are over ruled.

The KSP judgement did not further gave any order to the Government to pass any statutory law to protect the Privacy Rights of Indian population. Hence the statement of the petitioners

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

in the Reporter's Collective Trust that "DPDPA Act and Rules are in complete contravention of the law laid down in the KSP judgement" is incorrect.

Before this judgement was out, the Government had already formed the Justice Srikrishna Committee which went on to give its report in 2018 which after several iterations became DPDPA 2023.

DPDPA 2023 was under no obligation to define "What is Privacy" and "How the Government Protects Privacy". Hence the Government chose to restrict the law as "Law for protecting the personal data" and went on to define personal data.

Privacy in India is therefore protected by the Constitution directly and DPDPA 2023 facilitates the Data Principal to protect his privacy by protecting his personal data with the deterrence mentioned in DPDPA 2023.

The Government also adopted a strategy different from GDPR and laws of other countries by designating the entity determining the purpose and means of processing of personal data as a "Data Fiduciary" placing on them the onus of understanding what the data principal wants and carry out his permissions. Hence Consent was the backbone of the law.

Since Article 19(2) prescribed the reasonable exceptions, Government also recognized "Legitimate Uses" under Section 7 and Exemptions under Section 17. Both Sections 7 and 17 are applicable to both the Government and the Private Sector. Some of the exemptions are partial exemptions. Legitimate use is conditional.

The only blanket exemption is related to some of the aspects of the Article 19(2). Even here, all exemptions available under Article 19(2) have been invoked. Government has been very conservative. Also 17(2) is applicable to only such instrumentalities of State which are notified. Unless an entity is notified, the exemptions are not applicable even for the approved purposes such as the interests of sovereignty and integrity of India etc

To call this provision as "Attempt for Mass Surveillance",, "Excessive", "Disproportionate" etc… is false.

The Call for scrapping of DPDPA is atrocious. DPDPA tries to make Data Fiduciaries responsible and not indulge in indiscriminate harvesting of personal data, use it for spamming, profiling etc. The industry is interested in monetizing the personal data of individuals without a fair compensation to the data principals.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

DPDPA is expected to put an end to the obnoxious practice of Corporates stealing personal data without proper consent and enriching by their use. While DPDPA may not fully prevent the woes of the public from being targeted with Spams, Use of dark patterns to manipulate purchase decisions, use of techniques to change the freedom of mental decision making through mind bending communication strategies, it has given a hope to public that things may move in that direction.

The penalties at levels of Rs 250 crores are one of the highest in India but are no where near the international norms at 4% of global turnover to 10% of national turnover etc. The penalty structure under DPDPA does not mandate either Rs 50 crores or Rs 250 crores. It leaves the discretion to DPB to determine the penalty taking into account the capacity of the data fiduciary to pay. There is also a voluntary undertaking provision where penalty can be waived.

Without properly reading the law the petitioners make unsubstantiated statements including that journalists cannot pay the fine of Rs 250 crores and hence the law is unconstitutional.

This is an attempt to misrepresent the law.

The petitioners seem to place “Journalists” as if they are above law. Journalism has a public purpose and today most of the journalists are not the committed journalists of the yesteryear. They are under influence of money bags and politicians. Hence giving an unfettered freedom to them is a danger to the society.

Remember, Even Hindenburg can claim to be a “Research organization” as much as any other journalist.

Journalists who are also lawyers are persons who normally use RTI information for purposes other than public good. Even the NGOs they represent are often funded by international organisations and protect the interests of their foreign bosses more than Indian public.

We therefore seriously question the credibility of the petitioners who ought to declare their sources of revenue.

Bar Association also has to ensure that members of the Bar do not claim to be “Registered Journalists” and claim the benefits of the so called “Freedom of Speech” etc. This is a disguised attack on the society.

The NGOs headed by lawyers who say they are representing public interest should not be allowed by the Supreme Court to file PIL without proper scrutiny.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

I wish the Supreme Court prevents the gross abuse of the PIL privilege used as a weapon against progress.

Lawyers are considered as officers of the Court but we wonder if they are more officers of vested interests often guided by commercial or political considerations using the Court as a play ground for meeting their objectives outside the Court.

Otherwise it does not make sense for any of the petitioners to ask for scrapping of DPDPA just to ask for some exemptions for the profession of their clients.

The petitions filed should therefore not be considered as PILs. They are petitions filed on behalf of the clients like an association of journalists or an association of RTI activists.

The real public advocacy champions are not capable of matching the expenditure required to fight their passions in the Supreme Court and have to often remain in the background. The Court should recognize this and bring such organizations forward and listen to their advice.

The concerns related to Section 44(3) or 17(2)(b) are easily addressable in the rules and have already been addressed. The petitioners do not want to see through the provisions with an open mind and are ascribing motives to every word in the Act and the Rules without justification.

It is our desire that the honourable Supreme Court does not allow such pseudo public interest champions misleading the Court through their oratory and professional standing.

Naavi.org

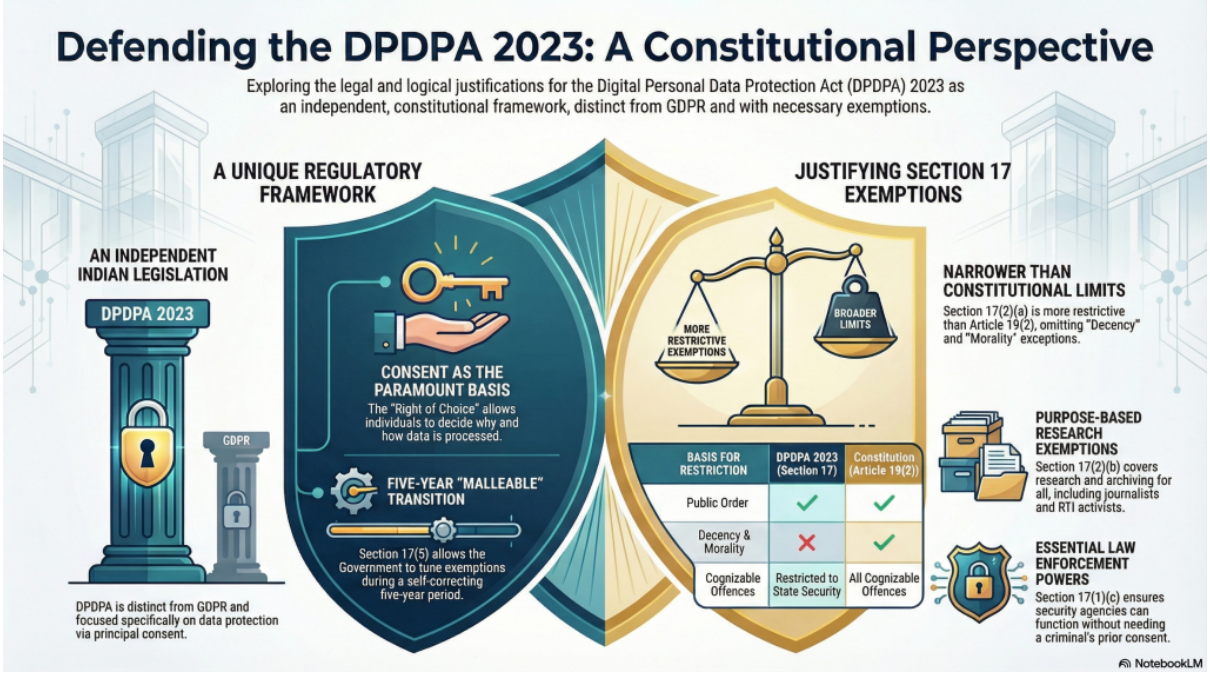
Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

6.DPDPA Exemptions : Don't Judge by what DPDPA does not do

Posted on March 3, 2026



We have tried to point out inconsistencies in the petitions of the "Scrap-DPDPA Brigade" through many of our previous articles.

The net point we are making is

Objection Section 44(3) is not relevant since

a) Every PIO is should not forced to take a judicial view under DPDPA whether Privacy interests are involved or not in releasing an information

b) PIO is encouraged to take the safety first option of rejecting release if prima facie personal information is involved so that the disgruntled applicant can invoke either the Grievance redressal mechanism under ITA 2000/DPDPA or RTI Act.

We have addressed some part of the objections related to exemptions under Section 17 which we shall explore further now.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

DPDPA has to be considered as a law which is different from GDPR. Its approach to Personal Data Protection is different from that of GDPR. Similarly, DPDPA 2023 cannot be directly linked to the Puttaswamy Judgement on "Privacy is a Fundamental Right". DPDPA 2023 is about personal data protection by organizations at the instance of the data principal. Protection of Privacy or being compliant to Privacy Principles under GDPR are incidental.

The petitioners have failed to look at DPDPA 2023 as an independent legislation and are trying to interpret it under different lens of either a Privacy Activist or a GDPR follower. These are giving raise to some disagreements. The Supreme Court has to understand this difference before giving any value to the arguments of the petitioners.

We shall try to address some of these issues here.

First of all, we need to take note of the following character of DPDPA 2023

1. DPDPA 2023 has not segregated Personal Data into Sensitive Personal Data and Non Sensitive personal Data
2. DPDPA 2023 has designated Data Controllers under GDPR as Data Fiduciaries providing them additional fiduciary responsibilities to take decisions in the interest of the Data Principals beyond the Consent.
3. DPDPA 2023 has chosen "Consent" as the only legal basis for processing of personal data since "Right of Choice" of the data principal is paramount to protect his "Personal Data Protection Rights".
4. It is the Data Principal who decides why he wants his personal data to be processed in a particular manner. It could be to protect his privacy or it could be to protect his Security or it could be to protect any other Right of his choice.
5. The cross border restrictions are based on "Types of Data" and "Types of Data Fiduciaries" and not "Adequacy or SCC"
6. The exemptions are also defined on the basis of "The purpose of processing more than the class of Data Fiduciaries".

These are fundamental differences in the approach of DPDPA to Personal Data protection and should be borne in mind when discussing whether DPDPA 2023 is constitutional or not.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

We cannot judge DPDPA 2023 as unconstitutional by what it fails to do. We have to rather look at what it proposes to do and determine whether it violates any constitutional principles.

Arguing that DPDPA is not constitutional because it does not protect "Privacy" the way the petitioners think it should is fallacious.

Petitioners have raised objections specifically on Sections 17(1)(c), 17(2).

When we look at Section 17,we can observe that it is divided into five sub sections namely 17(1), 17(2), 17(3), 17(4) and 17(5).

Section 17(5)

Section 17(5) is a section empowering the Government to provide any exemption within the next 5 years. By the end of 5 years, Section 17 will crystallize. Till then Section 17 is malleable and can be tuned as required. Hence even if some of the provisions of the current Section 17 is not acceptable, there is a self correcting ability within the Act and there is no need to scrap DPDPA.

Section 17(3)

Section 17(3) is a section that empowers the Government to declare any data fiduciary (including start ups and perhaps even digital publications) to be exempted from the provisions of Section 5 (Notice before collection), Section 8(3) (Completeness, Accuracy and consistency), Section 8(7) (Erasure on withdrawal of consent, Completion of purpose), Sections 10(Obligations of a Significant Data Fiduciary) and Section 11 (Right to Access).

Exemption under Section 17(3) is by specific notification and should be justified with the criteria of Volume and Nature of personal data processed. This would be documented and be available for judicial scrutiny.

Section 17(4)

Exemption under Section 17(4) applies to State or instrumentalities of the State. It is applicable to Section 8(7) (Erasure on withdrawal of consent, Completion of purpose), 12(3) (Erasure of personal data as a Right). It is subject to a further condition that the processing does not involve making of a decision that affects the data principal and is not related to updating or correction of data.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Thus 17(3) and 17(4) and 17(5) does not result in any major harm to the data principal and is subject to judicial scrutiny when invoked.

This leaves Section 17(1) and 17(2) to discuss.

Section 17(1)

Section 17(1) is restricted to exemption of Chapter II (Obligations of a Data Fiduciary) other than 8(1) (Responsibility for a Data Processor) and 8(5) (Protection of Personal data). It is not restricted to Government bodies only but extends to Private sector also based on specific purposes such as

a) For enforcement of legal rights

b) Processing by Courts or other judicial entities

c) Prevention, detection, investigation or prosecution of any offence or contravention of any law

d) Data of foreigners processed in India

e)For processing during mergers and acquisitions after approval of Court

f) For processing by Financial Institutions after default

In these 6 subsections, the objections are being raised only on 17(1)(c) which is related to law enforcement duties. If the petitioners think Police should take prior consent for processing the personal data of a criminal or a suspected criminal, they are living in a world of fantasy. Their speculation that it can be used for wide spread surveillance of citizens is not based on any facts. It is a pure speculation and imaginary. If such a situation arises checks and Balances need to be set up by the Law enforcement agency itself.

While DPDPA does not exempt "Security" of data, other laws including Section 72 of ITA 2000, and Section 316 of Bharatiya Nyaya Samhita, include responsibilities that the law enforcement person should secure the data collected for prevention or detection of crime.

Hence there is a reasonable check and balance associated with the power and there is no reason to endanger the community by preventing the law enforcement from discharging their duty to secure the nation. The Right to Security of a Citizen is also a fundamental right and a sacred duty of the Government.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

If the objections raised on Section 17(1)(c) is upheld it becomes a Right of a Criminal to hide under privacy excuses.

The same petitioners what Privacy not be a constraint for release of information under RTI but have objections for collection of such information by the law enforcement for prevention of crimes. This is the typical Urban Naxalite mentality that tries to protect dishonest criminals at the expense of honest citizens.

Acceptance of the objection of the Rights of Law enforcement will weaken the security framework of the country and preserving it is well within the Article 19(2) of the Constitution.

Section 17(2)

Lastly we shall explore Section 17(2). This contains two subsections 17(2)(a) and 17(2)(b) both need to be discussed in depth.

Section 17(2)(a)

Section 17(2)(a) applies only to "Notified" instrumentalities of the State and can only be used

"*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 relating to any of these,*"

This sub section reflect the reasonable exceptions under Article 19(2) for Article 21 (from which right to privacy is derived).

It is interesting however to see that Article 19(2) states

Nothing … shall …prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred ….. in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with Foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Let us compare the two underlined portions.

What DPDPA States	What Article 19(2) Permits
maintenance of public order or preventing incitement to any cognizable offence relating to any of these	*public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence*

It is observed that DPDPA has curtailed the exemptions that were feasible under Article 19(2) substantially. For example, DPDPA has removed exception such as "Decency", "Morality" and "Contempt of Court". Even in respect of "Cognizable offences", DPDPA restricts the exemptions only to such cognizable offences that relate to "i*nterests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order" and not to all cognizable offences.*

Hence we cannot find any fault with the Government of having misused the provisions of Article 19(2) and has shown extreme restraint in structuring Section 17(2)(a).

I don't see how the petitioners find this as giving "Sweeping powers of surveillance" etc except in their imagination.

Section 17(2)(b)

This sub section addresses the necessity for "Research", "Archiving" and "Statistical Purposes" and has to be seen with the conditions attached to the exemption and the standards of security prescribed under the Rules 16(with Second schedule).

This also has relevance to the arguments of the Reporter's Collective Trust that exemption has not been provided to the "Journalists" as a category of data fiduciaries.

Firstly we shall see the "Purpose" for which this exemption can be used. This subsection can be used for three aspects namely "Research", "Archival" and "Statistical Analysis". But it can be used only where there is no "Decision making" about the data principal involved. When a research is conducted, the output in the form of a report is generated. It can be used for general understanding of the market and not specifically to take a decision about the individual whose data is being processed.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

As an example, when a hospital takes the diagnostic data about a patient, and uses it for diagnosis and delivery of its health services, the research done for the purpose is for taking a decision about the data principal. It is not exempt from DPDPA provisions.

The same data may be used to generate a research report about a decease and used for industry analysis not specifically for being used for the data principal. That research can even be done on de-identified or pseudonymised or anonymised data of patients.

Statistical analysis can also be done on anonymised information.

Such processing is exempted from the provisions of the Act.

The Rule 16 reiterates the purpose of archiving and also the need for security etc.

There does not seem to be any objection for such Health related research or Financial research where there is no decision making and data is used subject to the security standards prescribed.

Role of a Journalist and his Research

The petition of the Reporter's Collective Trust strongly objects to the category of "Journalists" not being specifically mentioned in the Act. It ignores the fact that even Research for Medical or Financial evaluation is also not specifically mentioned. Use for research by any type of organization whether it is public or private is covered under Section 17(2)(b). It even covers research by Reporter's Collective Trust itself. I hope they have no objection for it.

The case of RTI activist also comes under comparable objectives. An RTI activist may conduct a research involving personal data provided it is not required to be used for any decision making against the individual, including filing an objection for a benefit granted by the Government under a scheme or for alleging corruption against the official. If the RTI activist needs to do a research on how a Government scheme is functioning, he can request and work with pseudonymised information or even anonymised information. In such an instance the objections raised under Section 44(3) also become meaning less since the PIO can release data without the personal identity. I am sure that the Government can make arrangements to remove the identity in a set of data to be released subject to cost and time involved.

If a Journalist wants to use any information for a journalistic research, the Act does not bar him from claiming the exemption as long as he can justify that the requirement is for a "Research". The special case of an "Investigative report" which later becomes a "Disputed defamation" exercise is to be handled as a "Risk for the Investigative journalist". If he collects data on his

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

own through research without specific consent or legal basis and uses it for developing a report which does not contain any identity of a person, then the report would be considered as not infringing privacy of any person and as long as the personally identified information collected for the research is held confidential and secure by the journalist, there should be no issue of non compliance of DPDPA and the fines.

It is true that GDPR may make a specific mention of "Journalist" for exemption purpose. At the same time GDPR also speaks of Churches for exemption. India has chosen not to specifically exempt either Journalists not doctors nor advocates nor chartered accountants nor temples, nor churches nor mosques, nor educational institutions nor madrassas, as an exempted category as of now. The law has specified if the purpose is research, archival, statistical analysis, provision of benefits to the population etc then some exemptions may be available either under Section 17 or under legitimate use under Section 7.

Indian law is fair and does not discriminate different kinds of data fiduciaries for this purpose. It only tries to classify some data fiduciaries as "Significant Data Fiduciaries" and imposes additional obligations.

Just as journalists tomorrow objections can be raised by SMEs or Micro enterprises or One man Business entities why they are not provided exemptions etc. The demand by Reporter's Collective is to introduce a "Discrimination" in the name of "Journalism" which is not warranted.

Further in the modern world of digital journalism, every individual who writes a blog or posts a YouTube video or a TikTok reel, is a journalist. Why should a journalist registered with the Reporters' Collective alone be provided a special status? The Intermediary guidelines under ITA 2000 does not spare an individual blogger from punishment if he violates a law. Hence the concept of "Who is a Journalist" in the digital media era has changed and there is no need to provide a special status to the journalists.

The days when Journalists were considered as the "Fourth Pillar of Democracy" is long lost. Today every journalist is either an employee of a journal or a contractual employee of some publication or George Sorros or a Political party. Hence there is absolutely no reason why "Journalists" should be considered as a special category of Data Fiduciaries and given some exemptions.

For example Naavi is himself a prolific writer and a journalist and Naavi.org itself is a publication. We have even submitted request for registration under the MeitY scheme of self

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

regulation of digital media. However naavi.org may not have a registration with the Press Council or the Reporter's collective and may not get invitations for Government events or IPL matches.

I therefore consider that the petition of Reporter's collective claiming extra privileges under DPDPA is not relevant and must be dismissed.

Let us see if what we have expressed here reaches the ears of the Supreme Court or at least the Meity or the Attorney General. Let us not allow the petitioners to use their selective presentations to mislead the Court.

In summary, I request the Supreme Court to judge DPDPA by what it does and not what it does not do but what petitioners wish it would do. Let DPDPA stand by its own Karma and not what any RTI activist or a journalist claiming to represent the public wishes.

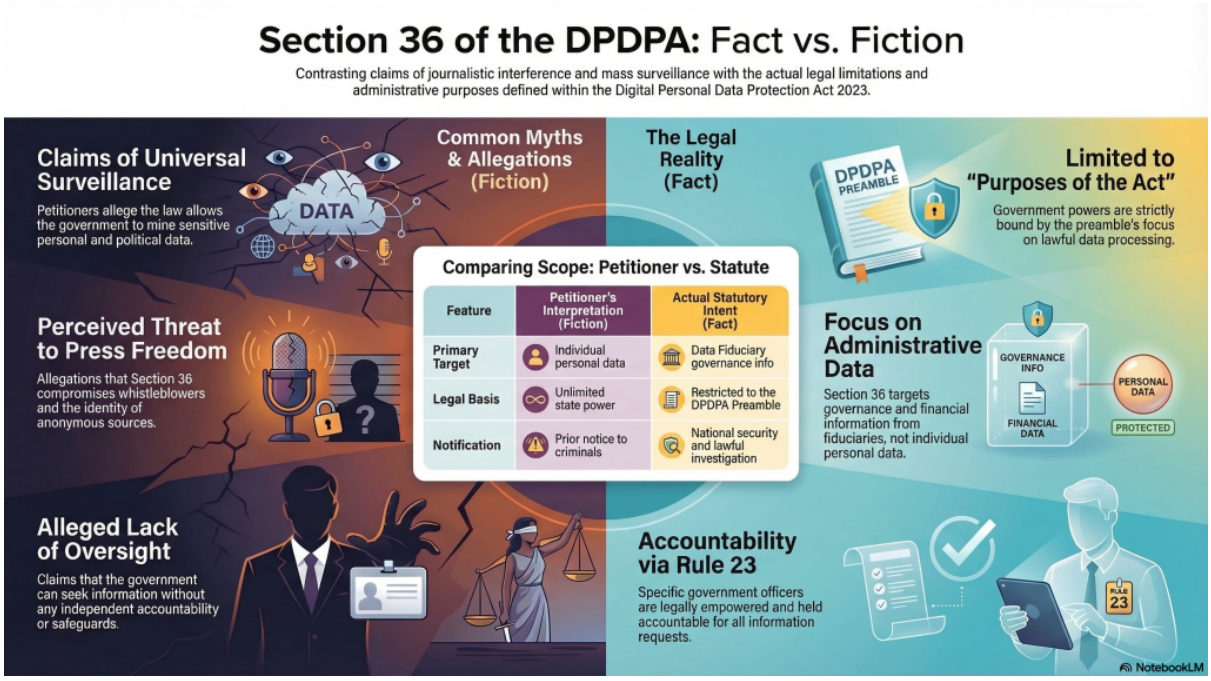
Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

7.How the Reporter's Collective is trying to fool the Supreme Court



The Reporter's Collective petition goes much beyond the "Dilution of RTI", "No exemption for Journalistic work", "Exemption to Government for enabling mass surveillance" and attacks Section 36 as an instrument of violation of the "Right to Freedom of Press". This is an interesting but malicious argument meant to fool the Supreme Court which the Court should identify and penalize.

Section 36 of DPDPA is an innocuous single line section which states

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.

The Reporter's collective has demonized this section through several pages of argument as an important ground to declare the Act as violative of the constitutional right of the *"Freedom of speech and expression of the journalist's Private sources, whistle blowers and informants to the potential for compromise of their personal identity and personal data."*

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Let us deeply analyse this contention that "Government being empowered to seek information from Data Fiduciaries" is curbing the sources of information of an investigative journalist and therefore violative of the "Freedom of Press".

The contention must be appreciated for its ingenuity and linking the unlink able. This is the creative mind of the PIL advocate at its best.

The arguments draw a parallel between "Extracting information by planting a Pegasus software without the knowledge of a potential informant of a journalist" in the Manohar Lal Sharma vs Union of India case, to the Government seeking information from a regulated entity. Again the Section 36 can be used only "For the purposes of the Act". The purpose of the act as described in the Preamble and through the sections do not include digging of information of an investigative journalist.

Let us recall the preamble once again….DPDPA 2023 is an act to provide for the processing of digital personal data in a manner that recognises both

a) the right of individuals to protect their personal data and

b) the need to process such personal data for lawful purposes and

c) for matters connected therewith or incidental thereto.

Hence Section 36 does not give any powers to the Government as claimed in the petition ..

i) which can reveal significant information about any person.

ii) which can be used to identify otherwise anonymous metadata obtained by various means,

iii) which can also be used to identify anonymous online content obtained by various means.

iv) Can identify and reveal intimate details about an individual's life religious affiliations, political beliefs, sexual orientations, health concerns, or personal relationships.

v) lacks any oversight or accountability mechanism that independently authorizes the request for information from the Central Government. (petitioners forget that under Rule 23, different officers of the Government are specifically empowered and are accountable for seeking such information)

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

vi) empowers the Central Government to call for a broad category of information pertaining to information which is likely to "prejudicially affect the sovereignty and integrity of India or security of the State", without sufficient procedural safeguards.

These contentions of the petitioner are not substantiated by any part of the law as proposed and are only an imagination of the petitioners. Thet are plain falsehood meant to mislead and cheat the Supreme Court.

The petitioners seem to think that for every administrative decision to be taken by the DPB or the Authorized official of the Government on the Data Fiduciary, an independent Court order is required. This is a suggestion to reduce the Supreme Court to the level of the Secretary of the MeitY.

The petitioner thinks that Under section 36, Government will be seeking information about an individual without consent. This is a known false statement since Section 36 is about seeking information about Governance, Financial, Administrative and other information from the Data Fiduciary and not seeking information from an individual or about an individual. If incidentally the Data Fiduciary needs to reveal any personal information of a data principal, then the data fiduciary is responsible for the use of legitimate basis for the disclosure or resist it in a Court of law.

The petitioner is childish and contends that the individual whose information may be revealed for national security reasons should be informed before hand that their information is being collected by the Government. It is utter foolishness to expect this and it appears that the petitioners are already preparing to represent the criminals whose information may be potentially revealed during a criminal investigation.

The petioners of the Reporter's Collective petition have proven beyond doubt that they have intentions of preventing whatever benefits this law may give to the society and exhibit a mindset to assist criminals through their "Own concept of Privacy as a tool to hide crimes". In this perspective, they may consider DPDPA as a hindrance.

But we the real public of India do not agree with their views and do not consider them as representing the public of India.

Supreme Court should not only recognize these ulterior designs and reject the petition but penalize the petitioners with a substantial fine.

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

8. Reporter's Collective petition. Creative but sinister

One more objection raised by Reporter's Collective which is bizarre and sinister is the interpretation that while the Search Committee may recommend some candidates either for the Chairman's position or the members of Data Protection Board, The Government may appoint some body other than the recommended persons.

It is not clear where from they got this creative idea which is unsubstantiated and completely ridiculous.

The petition goes further and states that since the DPB may act through a "Digital office" it is "exclusionary" forgetting that the law is meant only for "Digital Personal Data" and the related disputes and further that the disputes with Data Principals if any for personal remedy may be handled not by DPB but by the Adjudicating officer of ITA 2000. When the subject matter of the dispute itself is "Digital", it is difficult to understand how the dispute can be settled without touching a "Digital Office". The petitioner has just invented a reason to raise the dispute.

To support its view it has referred to several judicial decisions which have no relation to the formation of DPB through a process involving selection by a search committee consisting of three secretaries and two external persons.

Finally, the petitioner thinks that the penalty of Rs 50 crores to Rs 250 crores are exaggerated forgetting that the recommendation is "Upto" Rs 50 crores or "Upto" Rs 250 crores. The law does not mandate specifically that the minimum penalty should be Rs 50 crores. The law also provides an option for Voluntary undertaking which could mean that in some instances, no financial penalty may be imposed at all and only certain remedial directions may be issued.

Petitioners also need to reflect that under GDPR penalties are at levels of 1 billion US dollars in some cases and comparatively the maximum penalties under the DPDPA are much lower.

The petitioners assume that though the Act provides that Government may exempt specific classes of fiduciaries or specific classes of data from parts of the act, and such selective exemptions may be for SMEs, or even for Religious institutions such as Temples or even for the Journalists, the Government is not empowered to grant such powers. This sort of statements are malicious and meant only to make the Court believe what is not true.

The petitioners need to be asked to justify some of these assertions or admit that they are committing "perjury".

Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050

www.naavi.org: naavi@naavi.org: +919343554943

Thus, on several grounds the petition from Reporter's collective is considered as based on false premises meant to mislead the Court. It should ideally be rejected with a penalty.

We would have appreciated if the Reporter's Collective had restricted itself to express its concerns and seem specific remedies rather than asking for scrapping of the entire Act. This demand betrays that the petitioners have come with a pre-conceived conspiracy to get the act scrapped and prevent the Indian public from getting whatever benefits they would have expected from the "Right to Protect Personal Data" which the Act tries to provide.

We have our prescriptions on how the act and the rules may be interpreted to the effect that none of the concerns expressed can be considered as not addressable with a suitable interpretation.

Naavi

V A K A L A T N A M A
IN THE SUPREME COURT OF INDIA
ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. 177OF 2026

IN THE MATTER OF:
VENKATESH NAYAK ...PETITIONER(S)

VERSUS

UNION OF INDIA ...RESPONDENT(S)

AND IN THE MATTER OF:
Foundation of Data Protection Professionals in India ...Interveners/Applicants

I, Vijayashankar Nagaraja Rao, Chairman, Foundation of Data Protection Professionals in India,thePetitioner in the above Petition, do hereby appoint & retain Mr. Raghavendra Kumar ,**Advocate-on-Record** of the Supreme Court to act and appear for me/us in the above Suit Appeal/Petition/Reference and on my/our behalf to conduct and prosecute (or defend) or withdraw the same and all proceedings that may be taken in respect of any application connected with the same or any decree order or passed therein, including proceedings in taxation and application for Review, to file and obtain return of documents, and to deposit and receive money on my/our behalf in the said Suit Appeal/Petition/Reference and in applications of Review, and to represent me/us and to take all necessary steps on my/our behalf in the above matter. I/We agree to ratify all acts done by the aforesaid Advocate pursuance of this authority.

Dated this 7th March,2026

ACCEPTED, IDENTIFIED & SATISFIED,VERIFIED

For Foundation of Data Protection Professionals in India

(Petitioner)
Chairman/Director

AOR,
CODE:

MEMO OF APPEARANCE

To,

The Registrar,
The Supreme Court of India,
New Delhi

Sir,

Please enter my appearance on behalf of the Petitionerin the matter mentioned above.

New Delhi, Dated this the____ March, 2026.

Yours faithfully

For Foundation of Data Protection Professionals in India

Chairman/Director

SIGNED BEFORE ME

S.N. MADHU B.Com., LL.B
Advocate & Notary Public
Government of India
#94 1-A, 2nd 'A' Cross, 3rd Phase,
6th Block, BSK 3rd STage, Kathriguppa,
Near Ayyappa Templ Bangalore 560 085

NOTARY
S.N. MADHU
KATHRIGUPPE
BANGALORE URBAN
Regn No: 10103
Expiry Date
19-03-2028
GOVERNMENT OF