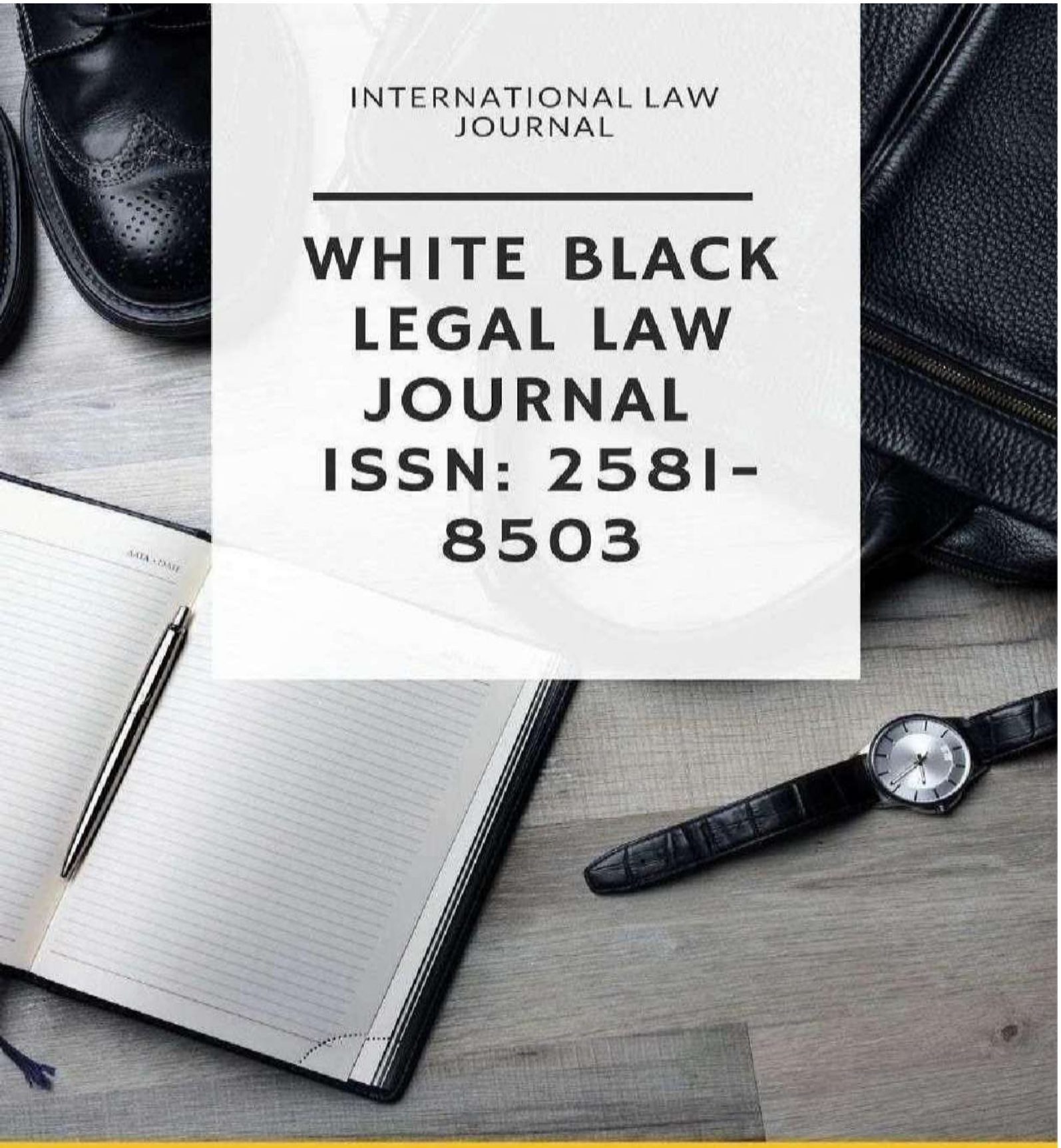

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

REGULATORY AMBIGUITIES OF DPDP ACT 2023 IN INDIA

AUTHORED BY - VISHNU VARDHAN .G

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first attempt to create a complete body of law protecting data in the era of digital technology. Even though there are many opportunities through this new act, it has also been designed with many gaps which limit its ability to achieve its original goal of creating a balance between the legitimate needs of the state and individuals' constitutional rights to privacy. This article takes a critical look at three major gaps in the DPDP Act and they are: the broad exemptions allowed for the government to deny individuals' privacy rights in favour of state's security, without establishing a reasonable slot machine between each interest; (2) the inadequacy of the Data Protection Board of India (DPBI) to independently oversee and enforce the DPDP Act; and (3) the ambiguity for micro, small, and medium enterprises (MSMEs) created by the vague definitions of "legitimate uses" and "Significant Data Fiduciaries" that make compliance uncertain. By comparing DPDP Act and General Data Protection Regulation (GDPR), and looking at Indian case laws including the Puttaswamy v. Union of India case, this paper emphasizes the need for legislative and regulatory changes that are required to turn the constitutional right of privacy into a practical right of the individual which meets the state's requirements as well. The research suggests that introducing amendments which includes incorporating explicit proportionality tests, refining the definition of Significant Data Fiduciaries, and strengthen independent oversight mechanisms over the DPBI can substantially enhance the protection of personal data in India.

Keywords: Data Protection, Privacy Rights, Government Exemptions, Regulatory Independence, DPDP Act, Proportionality, Significant Data Fiduciaries.

INTRODUCTION

Background and Legislative Context

The establishment of the Digital Personal Data Protection Act, 2023, represents the beginning of a new era for digital governance in India, following the historic ruling in the case of **K.S. Puttaswamy (Retd.) v. Union of India (2017)**[1], which declared the right to privacy as a fundamental human right protected by Articles 14, 19, and 21 of the Indian Constitution. This landmark judgment served as a foundational force for the formulation of a comprehensive statutory framework on data protection, affirming that safeguarding informational privacy is integral to the constitutional guarantee of life and personal liberty under Article 21, and inherently linked to the wider spectrum of fundamental rights enshrined in Part III of the Constitution of India.

The Government of India has passed the DPDP Act, 2023, to fulfil the constitutional requirement by providing the legislative infrastructure required to support privacy and data protection rights. Under the DPDP Act, individuals must consent to allow data processing by a third party; an obligation is placed on the third party to notify individuals about any breach of their data; material breaches can be subject to penalties of up to ₹250 crores; and the Data Protection Board of India has been created to oversee enforcement of these data protection provisions. Overall, the legislative journey of the DPDP Act is reflective of the recommendations made in the report of the Justice Srikrishna Committee in 2017, which recognized the need for a balancing act between state and individual rights and interests in promoting technological innovation.

While the DPDP Act has established a legislative framework for the realization of individuals' privacy and data protection rights, there exist significant discrepancies between the intent of the DPDP Act and the enforceability of the Act in practice.

This research paper identifies and examines three interconnected shortcomings that compromise the efficacy of the Act:

1. **Wide-ranging Governmental Exemptions (Section 17):** This provision in the new law contains broad-ranging exemptions generally in respect of national security but in

[1] AIR 2017 SUPREME COURT 4161

the absence of judicial frameworks to assess necessity and proportionality.

2. **DPBI Independence Concerns:** The institutional design of the regulatory authority reflects the dominance of the executive branch in the mechanism of appointment and casts doubt upon the impartial adjudication of disputes in which government entities are involved.
3. **Denotational Vagueness:** There is a lack of sufficient clarity in the key operational terminology compliance uncertainty and disproportionately impacting small business concerns.

Research Significance and Scope

This study's relevance today is confirmed by the concurrent establishment of the DPBI as part of the ongoing dialogue across the world regarding how best to both protect personal data and maintain flexibility in how we regulate personal data. Based upon initial experiences with implementing the DPDP Act, it appears that there is currently an inherent conflict between the stated goal of protecting personal data in the DPDP Act and the practical means of providing a wide range of exemptions to such protections.

The study is of significance to many audiences:

1. **Policymakers and Regulatory Authorities:** They may wish to identify areas within which clarity is needed through subsidiary regulations or amending legislation.
2. **Compliance Officers and Organizations:** They will gain insight into interpretative difficulties and the effect of those difficulties on compliance-related costs, especially with regard to micro, small, and medium enterprises (MSMEs).
3. **Privacy Advocates and Civil Society:** They have a reason to advocate for a constitutional interpretation of data protection legislation that includes safeguards against unconstitutionality.
4. **Comparative Legal Scholars:** They will benefit through the balance between the protection of individual privacy and legitimate governmental interest in the governance of data.

Methodological Framework

This paper discusses several central research inquiries, which are:

1. Do government exemptions in Section 17(2) comply with the Proportionality Framework of Puttaswamy, and what measures ensure compliance with constitutional

principles?

2. Does the institutional design of the DPBI support an independent perspective for dispute resolution that involves government entities?
3. What compliance issues that arises from the terms that are ambiguous in DPDP Act, and what regulatory clarifications would reduce the compliance costs for MSMEs while preserving protectionary measures?

The methodology will be established through a combination of performing a doctrinal legal analysis of the DPDP Act 2023 and pertinent statutory provisions,

- comparative institutional analysis to evaluate the DPBI against established benchmarks of international DPAs under GDPR,

- conduct case law analysis of Indian constitutional jurisprudence in relation to established international case law,

- conduct regulatory gap analysis identifying clear regulatory statutory provisions that require clarifications or amendments.

The paper is structured in a manner that build a progressive argument, beginning with establishing constitutional foundations for argumentation with each identified gap subsequently analyzed, with proposed solutions that make comparisons, culminating with recommendations for specific reforms.

PRIVACY AS A CONSTITUTIONAL GUARANTEE

The Puttaswamy Judgment and its Signifcance

The decision of the Supreme Court in K.S. Puttaswamy (Retd.) v. Union of India, is a landmark decision that laid down that privacy is part of the fundamental steady structure of the Indian constitutional regime. A unanimous nine-member Constitution Bench headed by Chief Justice J.S. Khehar, held that the Constitution guarantees a right to privacy to every human being and such right is part of an individual's human dignity. Justice D.Y. Chandrachud in his judgment explained in detail a broad, multidimensional view of privacy - that included personal autonomy, bodily integrity, control over one's information, freedom of choice to preserve human dignity. The court observed that privacy is an embodiment of the spirit which the Constitution has tried to ingrain and is a necessary condition for the exercise of an individual's choice which forms the basic fabric on which the public order rests, and therefore it will be protected not only against State action but also against an incursion from private actors as well as a skewed distribution of power in society.

The Proportionality Framework

Crucially, the Court in the case of K.S. Puttaswamy (Retd.) v. Union of India established that privacy, like other fundamental rights, can be restricted only under specific conditions:

"Any restriction on the exercise of the right to privacy must be prescribed by law. The law must define the circumstances and the procedure pursuant to which the right can be restricted. The restriction must be needed in a democratic society for a legitimate aim. The nexus between the restriction and its aim must be rational, and there must be a direct and substantial relation between the restriction imposed and the aim sought to be achieved. The restriction must be necessary in a democratic society, in the sense that it addresses a pressing public need. The restriction must also be reasonable in its operation."[2]

The above four components form the basis of this framework:

1. **Legal Requirements** - Restrictions shall only be imposed by law, clearly defined.
2. **Legitimate Purpose** - All objections shall serve a legitimate public purpose and must be based on a recognized societal need (i.e. national security; preservation of public order; prevention of crime; protection of public health).
3. **Necessary and Proportionate** - Restrictions should not exceed what is necessary and proportionate to achieving their objectives. Therefore, there should not be any equally effective alternative means that are less restrictive.
4. **Protective Mechanisms** - The framework will also provide mechanisms for independent oversight, accountability and remedy.

Informational Privacy as Fundamental Right

Justice Chandrachud's judgment particularly emphasized informational privacy in the digital context, he emphasized on informational self-determination, the ability to control one's personal data, directly informed the DPDP Act's foundational principle of consent-based processing. However, as this paper argues, the Act's exemptive provisions inadequately implement this constitutional principle.

The Puttaswamy Legacy: From Constitutional Right to Statutory Right

The Digital Personal Data Protection Act (DPDP), 2023, is the first legislative enactment to

2. AIR 2017 SUPREME COURT 4161

bring out the the right mentioned in the case of Puttaswamy through a statutory framework. The DPDP includes provisions for data processing obligations in Section 3, consent requirements in Section 4 and obligation for breach notification in Section 7 which states all of which are grounded in the Puttaswamy constitutional framework.

The key area of complication is Section 17 of the DPDP which provides governmental agencies with broad exemptions from statutory compliance without a robust application of the proportionality framework found in the Puttaswamy decision. This lack of a coherent overlay between the established constitutional principle embodied in Puttaswamy and the broad exemptions allowed by Section 17 of the DPDP will be the basis for the initial significant gap assessed in the current research.

STATE EXEMPTIONS AND PROPOTIONALITY

Textual Scope of Government Exemptions

Section 17(2)(a) of the DPDP Act grants an exemption to authority—the Central Government may exempt "any instrumentality of the State" from "the provisions of this Act" (emphasis added). The scope is extraordinarily broad: it permits complete exemption from all protections—consent requirements, breach notification, data minimization, purpose limitation, security obligations, and transparency requirements.

Additionally, Section 17(2)(b) provides a cascading exemption: if an exempted government agency shares personal data with another government entity, that second entity is also exempted from compliance obligations when processing such data. As one observer noted, "any exempted agency of the government can collect and process the personal data of citizens without following any of the safeguards prescribed in the DPDP Act, such as getting consent, securing data from breaches, maintaining accurate and complete data."

Comparative Evaluation of The 2018 Bill Approach

The changes in exemption provisions across successive versions of the legislation indicate a worrying trend. The 2018 Personal Data Protection Bill (which preceded the 2023 DPDP Act) contained more circumscribed exemption mechanisms:

Government exemptions were limited to security of the State and only "if authorized pursuant to a law...made by Parliament"

The exemption required an explicit legal authorization—not merely executive discretion. The exemption applied only to "a victim, witness, or any person with information about the relevant offense or contravention.

A compliance waiver was permitted only if compliance would be "prejudicial to the prevention, detection, investigation or prosecution of any offense."

The Justice Srikrishna Committee, in justifying these limitations, noted that they were "concerned about the possible misuse of the provisions when a situation arises whereby the privacy rights of the individual, as provided under this Act, have to be subsumed for the protection of the larger interests of the State."

By contrast, the 2023 DPDP Act eliminated these safeguards. The exemption no longer requires explicit parliamentary authorization, applies to any government activity (not merely security investigations), and includes no temporal limitation or necessity assessment. This represents a significant weakening of constitutional principles.

International Comparative Framework of the protection standards

GDPR provides EU Member States with an example of how similar legislation should function. Article 4(11) states: "An individual should give freely, and after having been provided with the necessary information to understand how their data will be processed." Further, processing of individuals' data will be lawful only if it meets one of similar bases in Article 6. These include: Consent, Necessity, Fulfillment of a Legal Obligation, Protection of the Vital Interests of the Data Subject, Performance of a Public Task, or Legitimate Interest.

It is important to note that Article 23 of the GDPR also permits Member States to impose limitations on individuals' rights as data subjects when such limitations meet the criteria of being necessary and proportionate, and respect the essence of fundamental rights and freedoms, for the benefits of a democratic society. The same criteria and limitations to individuals' rights as a data subject are contained in the Constitution of the United States. However, the Constitution does not grant individuals' rights as data subject higher priority than having unrestricted access to individuals' personal data.

The GDPR includes numerous fundamental safeguards that define its method of applying exceptions. Examples include that restrictions are limited to the particular rights of access,

rectification, and deletion; they are not simply an overall exemption from every obligation; limits on the ability of member states to impose restrictions through their respective national laws, rather than simply issuing executive notices; restrictions must be carefully assessed for their necessity and proportionality to prevent excessive uses of the restriction; and there must be continuous monitoring by independent data protection authorities with authority to investigate and enforce even in the context of security-related data issues. In particular, the 2020 Schrems II ruling from the European Court of Justice has confirmed that if the government accesses personal data without the existence of proportionality safeguards, it violates the principles of GDPR, regardless of whether it is for reasons of national security.

Risk of Abuse and Chilling Effects on Privacy

The absence of proportionality constraints in Section 17(2)(a) creates several concrete risks:

A. Expansive State Surveillance:

India has launched numerous surveillance programs that would qualify for exemption under that authority. Examples of these programs include the Crime and Criminal Tracking Network and Systems (CCTNS), which includes a national facial recognition and surveillance database, as well as the Aadhaar biometric database (which consists of enrollment information and biometric information for over 1.4 billion people) and the communication surveillance program through the Unified Access and Oversight Framework, which oversees telecommunication services. The provisions in Section 17(2)(a) regarding exemptions, thus allowing these programs to operate without consent, breach notification or independent oversight, directly contradicts the tenets laid down in the Puttaswamy framework**.**

B. Precedent in Recent Case Law:

In **Prahlad Rathour v. State of Chhattisgarh** [3], the High Court of Chhattisgarh ruled that the existence of consent when an individual wishes to access his/her social network is an infringement on the fundamental right to privacy. The Court ruled that "if access was granted to examine a Facebook or Instagram account of the prosecutrix and audiotapes were played, then the privacy of the prosecutrix would be violated".

Although the ruling provides protection, it also demonstrates how government agencies that fall under the exemption allowed by Section 17(2)(a) can, in reality, avoid those protections

[3] 2025 SCC OnLine Chh 5068

and have unrestricted access to social network and email accounts without restriction on protection.

C. Chilling Effect on Expression and Association:

The existence of government agencies having unlimited and unauthorized access to one's private information creates a negative impact on an individual's freedom of expression and association; thus, creating a "chilling effect" on their ability to communicate freely with others and associate with a group or organization, for example, through the "panopticon" effect. The previously noted effect is that people tend to alter their behavior (speaking, interacting) when they are informed they may be under surveillance.

Proposed Reform: Integrating Proportionality Framework

To align Section 17(2)(a) with Puttaswamy constitutional requirements, the following amendments are recommended:

The government must create explicit exemptions that conform to proportionality standards set out Constitutionally; An example would be to issue a list of specific exemptions rather than issuing framework exemptions to demonstrate why there are no less restrictive ways to achieve a similar result. The government must also demonstrate that advantages make exceeding privacy intrusions reasonable and implement time limits with protocols in place for the periodic evaluation of the exemptions. Following the example of the 2018 Bill, any exemption must require explicit permission from Parliament rather than just notification from the Executive Branch to enhance democratic accountability and to mitigate the opportunity for government overreach.

Additionally, the DPBI should also be expressly granted the authority to evaluate notifications related to exemptions for proportionality, investigate complaints regarding misuse, conduct ongoing audits on entities exempt from the collection of data, and establish interpretive guidelines regarding acceptable and non-acceptable activities associated with exemptions. As such, all exemptions should carry a set time frame (for example, all security exemptions should be defined by a standard two years from the time of approval and subject to regular reviews) to ensure evaluation of proportionality is continuously assessed.

INSTITUTIONALINDEENDENCE AND ENFORCEMENT POWERS OF THE DATA PROTECTION BOARD

Institutional Design and Appointment Mechanisms

The DPBI (Data Protection Board of India), created by Section 18 of the Data Protection and Digital Privacy bill (DPDP), is intended to serve as the chief enforcer of data protection regulation. Its institutional makeup raises severe doubts about the ability to perform independently.

Structure: The Data Protection Authority is made up of a chairperson appointed through "appropriate procedures [as defined in existing laws]." The power to appoint these members under the Data Protection Authority rules is given to the Union Government according to the rules made under the Data Protection and Digital Privacy law in 2025.

Specifically, the chairperson is appointed by the Central Government from among persons recommended by a Committee comprising senior government officials.

The **Justice Srikrishna Committee Report (2017)**[4] explicitly recommended that to ensure independence comparable to international standards, the appointment committee should include "the Chief Justice of India or her nominee." However, the final DPDP Act omitted this safeguard.

Comparative Analysis with GDPR Supervisory Authorities:

Independently appointed mechanisms for Data Protection Authorities have been put in place under the GDPR across EU member nations. The position of the Federal Commissioner for Data Protection and Freedom of Information (BfDI) in Germany is given to the parliament via a two-thirds majority vote and has protections against removal in place. The CNIL (the French data protection authority) has its members on the Board appointed jointly by the President of France, the President of the National Assembly and the President of the Senate. The Information Commissioner's Office (ICO) in the UK has a separate independent commission that recommends candidates for Commissioner to the Monarch for appointment by Royal Appointment. All of the above-mentioned examples include a combination of judicial oversight, legislative involvement, and representation from multiple branches, which GPBI

[4] https://legalaffairs.gov.in/sites/default/files/Report-HLC.pdf

lacks.

Powers and Functions: Scope and Limitations

The powers granted to the Data Protection Board of India (DPBI) under section 8(6) of the Act do include those related to investigating breaches, adjudicating on complaints made by data principals, issuing orders, and imposing penalties. However, there are significant limitations on the DPBI that greatly restrict the ability to conduct effective investigations. The most significant limitation is the DPBI's lack of any proactive ability to investigate data breaches that were not reported to it. The DPBI does not have authority to perform independent audits of data processors, conduct systemic investigations of data processing practices unless the investigation is initiated by a data principal's complaint, or conduct systematic investigations of patterns of behaviour across multiple data processors. The investigative powers of GDPR supervisory authorities are much greater than those of the DPBI.

Additionally, enforcement against government entities is significantly limited because exemptions in section 17(2)(a) relieve governmental agencies of many of the substantive obligations created by the Act. This means that government entities may collect and process data without obtaining consent from data principals; may fail to notify data principals of breaches; may retain data indefinitely; and may process data without regard to limitations imposed by the Act, yet, at the same time, the DPBI is unable to provide oversight, impose penalties, or provide any mechanism for remedy to data principals with respect to governmental entities. This has created a significant imbalance in the power of the DPBI against private actors and the DPBI against government entities. The disparity of power is significant, as the surveillance powers of government entities present the greatest potential threat to the privacy rights of individuals.

Resource Constraints and Institutional Maturity

The DPBI, which officially started operations in November of 2025 as a new agency is operating under significant constraints, limiting its ability to operate effectively. Staffing for the DPBI is, as of now, at levels far below those necessary to process the volume of complaints as outlined in the DPBI's statutorily created complaints volume. International benchmarks provide examples of other similar agencies that require hundreds of personnel on a full-time basis for each complaint processed, while the DPBI presently lacks any of the current capacity to hire the level of staffing as per the international benchmark. In addition to hiring sufficient

staff, the DPBI requires hiring experienced staff with advanced technical skill levels in the areas of data systems, encryption protocols, and forensic investigation of data breaches, and the agency has yet to complete development of its infrastructure as well, including regional offices to provide nationwide access to the DPBI.

Empirical Lessons from GDPR Implementation

Since 2018, the implementation of GDPR has created a wealth of empirical knowledge regarding the prerequisites of institutional maturity necessary to enforce laws with applicability to all institutions equally. By levying in excess of €90 million worth of fines for individual infractions, CNIL (France) has created an effective deterrent; BfDI (Germany) has undertaken systemic investigations of social media companies' handling of users' data; and the European Data Protection Board (EDPB) is facilitating the coordinated application of all 27 EU member states' GDPR-compliant enforcement actions against businesses in order to prevent regulatory arbitrage. However, the GDPR has also exposed continuing challenges to enforcement, e.g., smaller data protection authorities (DPAs) are experiencing backlogs of complaints that effectively shield businesses from enforcement action; enforcement thereof by DPAs is applying different levels of scrutiny, resulting in varying breaches of businesses in different jurisdictions; and DPAs lack resources to proactively enforce the GDPR against all businesses but rather only those businesses deemed to be "high-profile." The foregoing experiences of enforcement apply to the DPBI (Data Protection Board of Ireland) and highlight the urgent need for the DPBI to enhance its operational capabilities while maintaining the necessary independence required by the GDPR.

Proposed Reforms: Enhancing DPBI Independence and Capacity

There are a number of reforms that need to be made in order to improve the DPBI's independence and effectiveness. Firstly, amend the DPDP Rules to create a multi-branch selection committee, that includes the Chief Justice of India from the Judiciary, the Chairperson of the Parliamentary Standing Committee from the Legislature, the Secretary of the Ministry of Electronics and Information Technology from the Executive, and two independent experts nominated by professional organizations - this would help to reduce Executive dominance and create an authentic institution. Secondly, the Chairperson and members of DPBI should each be appointed for a fixed six-year term, with removal permitted only on proven misconduct or incapacity and followed by approval of Parliament, using the model of the Supervisor’s Authority under GDPR. Thirdly, extend Section 18 to give DPBI the power to conduct suo -

motu investigations of systemic breaches, to audit the major data fiduciaries, issue preventive guidance and standards, and allow a stakeholder standing to lodge complaints directly with DPBI, including civil society and consumer organizations, as well as individuals. Fourthly, a commitment should be made by the Government to increase its workforce by 200-250 qualified employees within 18 months, create regional offices throughout major metropolitan areas, establish budgets specifically for technology and forensic infrastructure, and partner with global counterparts to provide training opportunities for personnel. Lastly, create a statutory requirement for the DPBI to conduct annual audits of the data practices of Government Agencies that have been given exemptions, and investigate any related complaints, and publish recommendations.

COMPARTIVE ANALYSIS OF INTERNATIONAL FRAMEWORK AND BEST PRACTICES

The GDPR through Article 52 provides strong independence safeguards for supervisory authorities, ensuring that each agency will operate independently without receiving instructions from the government. Examples include Germany's BfDI, France's CNIL, and Spain's AEPD, which play a role in ensuring that these independent bodies retain wide-ranging enforcement authority, including the ability to conduct investigations on their own initiative, impose penalties of up to €20 million or 4% of global revenues, engage in cross-border cooperation through the EDPB, and set regulatory standards. In contrast to Section 17(2)(a) of the DPDP Act, which allows a general exemption from the DPDP Act, the GDPR limits governmental processing of personal data to defined legal grounds (Article 6), limits data subject rights to the level of proportionality (Article 23), and there is full regulatory oversight and judicial review of all governmental processing activities.

The GDPR's definitions are more precise than those of the DPDP Act. Under the GDPR, "legitimate interests" (Article 6(1)(f)) requires a necessity standard, balancing tests, and EDPB guidance that excludes unsolicited marketing; "high-risk" areas where a DPIA is required (Article 35) include large-scale processing of sensitive data; and clear distinctions exist between the data controller and processor (Articles 4(7)-(8)), while the DPDP Act's definitions are vague. There are similar trends in other jurisdictions: in Singapore, the PDPA provides an exemption for public interest to the extent that it is necessary, Brazil's LGPD mandates proportionality of all data processing for the purpose of security, and South Korea's Act

necessitates that judicial scrutiny be applied to national security exemptions. This shows that effective data protection should support the state while balancing the rights of individuals.

Proposed Comprehensive Reforms

This paper proposes a detailed reform plan based on earlier published suggestions. The reform proposes a phased approach starting with clearing up the rules in 0–6 months for DPBI to provide guidance on the classification thresholds for SDF (i.e. >5 million individuals whose information is being processed by an SDF), sensitivity criteria, clarity in consent requirements around bundled consents and ease of withdrawal, examples where treatment for valid purposes has been given through proportionality, and initial notifications to individuals of being processed by an SDF and what kind of contests there will be to contest the processing of that information; amending rules in 6–18 months, creating the means for each DPBI to appoint multi-branch DPBIs, clearly defining SDF thresholds, forming new consent requirements that prohibit the use of 'dark' patterns to obtain consent, creating improved channels for expanding civil society input into SDFs and their operations, and developing the processes for documenting on our own motion investigations; and making amendments to the statute in 18–36 months to amend the statute Section 17(2)(a) by providing proportionality based exemptions subject only to DPBI review, strengthening the independence of DPBI through fixed tenures, requiring transparency on SDFs, providing clarity on statutory consent criteria, and providing a new Section 20 to require annual audits of exempted agencies.

To implement this, ₹500 crores will be needed to develop capacity for over 250 staff, regional offices, and international training partnerships as well as providing quarterly consultations with stakeholders, establishing write-in periods for public comment, developing independent evaluations, creating reports to Parliamentary on agencies receiving exemptions annually, conducting biannual compliance assessments, conducting surveys of citizens and providing funding for academics to support their work. In summary, while the DPDP Act, 2023 marks a first-time comprehensive legal framework for data protection in India, a number of critical implementation issues could diminish the effectiveness of the Act.

CONCLUSION

India has recently passed the Digital Personal Data Protection Act, 2023 (DPDP), that establishes a comprehensive legal framework for protecting individuals' personal data in India. However, the Act has significant implementation gaps that threaten to undermine its

effectiveness. Those significant gaps include: broad exemptions to governments under Section 17(2)(a) of the DPDP that do not contain the proportionality protections mandated by the Supreme Court in Puttaswamy; appointment of the Digital Personal Data Protection Bureau (DPBI) as primarily an executive body with limited investigative authority; lack of capacity to investigate (e.g., staffing of the DPBI is modest compared to the hundreds required to effectively enforce compliance), thereby rendering the DPBI powerless to investigate state entities and evaluate the potential for heightened risk to the privacy of individuals arising from state surveillance programmes; and vagueness in defining "Significant Data Fiduciaries," "legitimate uses," and "consent," all of which create the potential for regulatory capture, over compliance by the MSME sector, and stifling competition among companies. All of the above gaps collectively undermine the constitutional right to privacy in India. The proposed three-phased agenda would clarify the role of the DPBI within 0-6 months; make amendments to allow for independence through the implementation of rules regarding investigation authority from 6-18 months; and embed the proportionality principles mandated by the Supreme Court in Puttaswamy into legislation, thus allowing for both enforcement of the Act and a path forward to create digital trust.