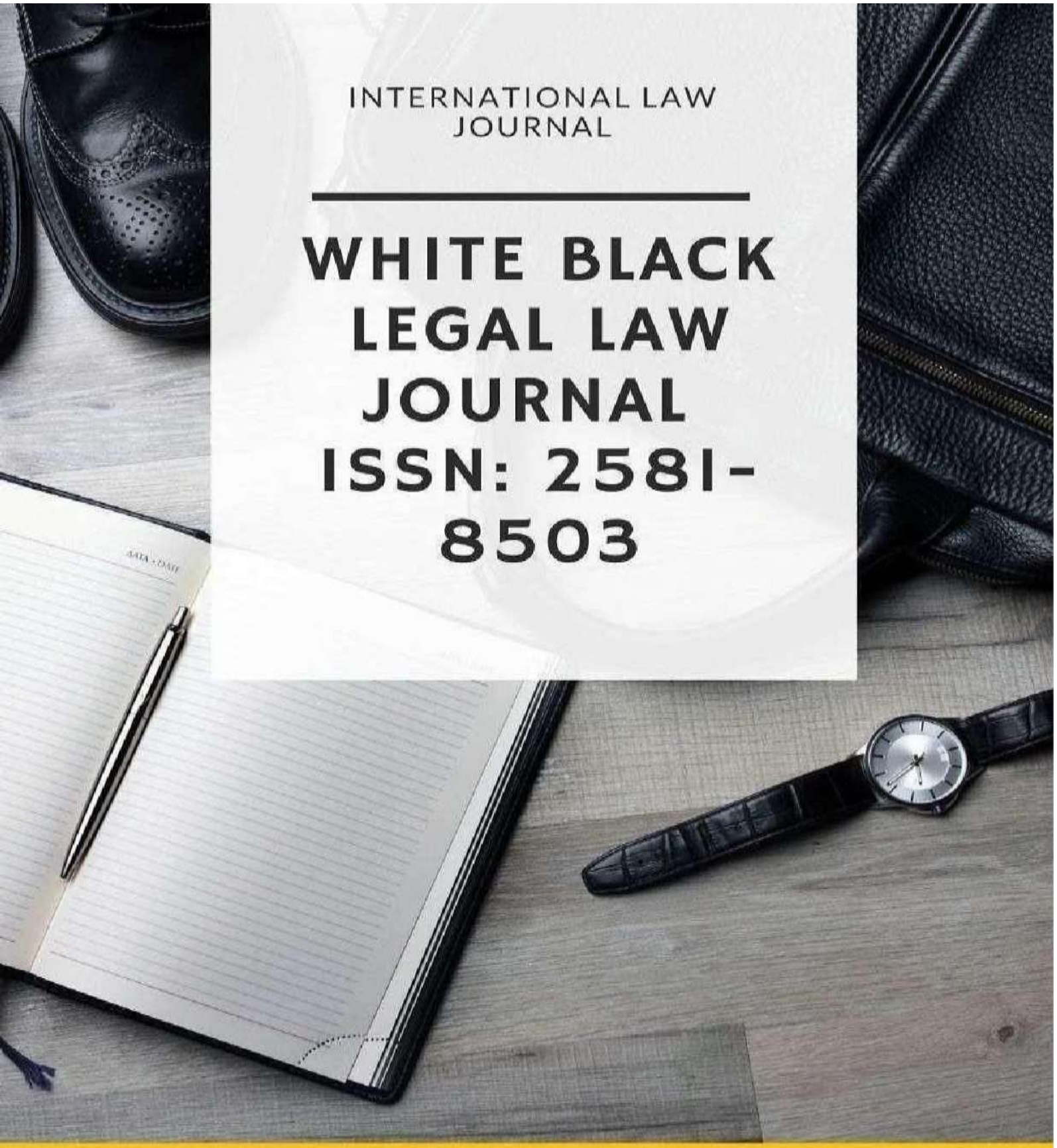

INTERNATIONAL LAW JOURNAL

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.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

"CONSENT IN THE DIGITAL AGE: A COMPARATIVE STUDY OF THE GDPR AND THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023"

AUTHORED BY - MONISHA K
VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES, SCHOOL OF LAW, PALLAVARAM, CHENNAI

CO-AUTHOR - SRIVINITHRA
Assistant Professor, School of Law
VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES, SCHOOL

ABSTRACT

Consent forms the cornerstone of modern data protection law, yet its operationalisation under the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDP Act) reveals a profound legal fiction—formally valid but substantively hollow. This article critically examines whether consent-based frameworks genuinely protect data subject rights or merely legitimise data exploitation within asymmetric platform economies. Through comparative doctrinal analysis of the GDPR and the DPDP Act 2023, evaluated against the constitutional standard of *Justice K.S. Puttaswamy v. Union of India* (2017), the study exposes structural deficiencies in consent architecture, deemed-consent provisions, government exemptions, and supervisory mechanisms. The article argues that the four cumulative conditions of consent—free, specific, informed, and unambiguous—cannot be satisfied in conditions of extreme power asymmetry between data subjects and dominant technology firms. It concludes by proposing normative reforms beyond the consent paradigm toward enforceable data minimisation, algorithmic accountability, and an institutionally independent data protection authority in India.

Keywords: Consent, Legal Fiction, Data Protection, Informational Privacy, GDPR, DPDP Act 2023, Surveillance Capitalism, Puttaswamy, Data Subject Rights, Power Asymmetry.

1. INTRODUCTION

The twenty-first century has fundamentally transformed the relationship between individuals and information. Personal data—once confined to filing cabinets and bureaucratic registers—now flows continuously across digital infrastructures at a scale and velocity no legal system fully anticipated. Every search query, financial transaction, social media interaction, and location ping generates data points that are harvested, aggregated, profiled, and monetised by technology corporations operating seamlessly across national boundaries.[1]

Within this transformed landscape, consent has emerged as the principal legal device for legitimising the processing of personal data. Both the GDPR and the DPDP Act position consent as the foundational lawful basis for data processing, formally requiring it to be free, specific, informed, and unambiguous. Yet a critical examination reveals that consent, as operationalised within these frameworks, functions as a legal fiction—formally valid but substantively hollow. Every day, millions of users click 'I Agree' to thirty-page privacy policies they neither read nor comprehend, and the law treats that click as the foundation upon which entire data economies are built.[2]

This article argues that such an assumption is fundamentally flawed. In reality, consent under both regimes is coerced, because refusal means denial of essential services; uninformed, because privacy notices are deliberately complex and inaccessible; manipulated, because dark patterns in interface design trick users into broader data sharing than they intend; and ultimately meaningless, because withdrawal of consent carries no practical consequence in platform ecosystems built on perpetual data extraction. The DPDP Act further deepens this problem through sweeping legitimate-use provisions, broad governmental exemption clauses, and a structurally compromised Data Protection Board—raising serious constitutional concerns against the proportionality standard established in *Puttaswamy*. The article unfolds in six parts: it traces the philosophical foundations of consent (Part 2); develops the legal fiction theory (Part 3); analyses consent under the GDPR (Part 4) and the DPDP Act (Part 5); undertakes comparative critique (Part 6); and concludes with normative recommendations (Part 7).

2. THE PHILOSOPHICAL FOUNDATIONS OF CONSENT

Consent as a normative concept possesses a distinguished philosophical pedigree. Enlightenment thinkers such as John Locke grounded legitimate political authority in the consent of the governed, arguing that no person could be bound by an obligation to which they had not, at least tacitly, agreed.[3] This contractarian tradition placed voluntary agreement at the centre of the relationship between the individual and the State, and later between private parties

in contract law. The deeper moral foundation lies in Kantian autonomy: the capacity to govern oneself according to reasons one has reflectively endorsed is, on Kant's account, a defining attribute of the rational agent and the source of human dignity.[4] To process a person's data without genuine agreement is, on this view, to treat them merely as a means and to bypass their capacity for self-determination.

In bioethics, consent acquired a more procedural character through the doctrine of informed consent, which emerged in the twentieth century in response to abuses in medical experimentation. The Nuremberg Code of 1947 and the Declaration of Helsinki codified the requirement that research subjects give voluntary, informed, and competent agreement before participating in any experiment.[5] That tradition introduced three criteria—information, voluntariness, and capacity—that would later migrate into data protection law, although in adapted and often diluted form. Translating consent from these contexts into the regulation of data processing, however, raises distinctive difficulties. Unlike a discrete medical procedure or a bilateral commercial transaction, the processing of personal data is continuous, diffuse, and technically opaque. The classical ideal of a discrete, informed, and voluntary act of agreement ill fits this reality.

3. CONSENT AS LEGAL FICTION: A THEORETICAL FRAMEWORK

The disjunction between the philosophical ideal of consent and its operational reality in the digital environment has led a growing body of scholarship to characterise consent in data protection law as a legal fiction. Lon Fuller's classical analysis describes legal fictions as statements known to be inaccurate but employed because they serve a useful procedural or doctrinal purpose.[6] When a user clicks 'I accept' at the foot of a thirty-page privacy notice, the law treats this act as expressing free, informed, and specific agreement, even though every party involved understands that the user has neither read nor comprehended the document. The law thus constructs the appearance of voluntary choice in order to legitimise a transaction whose underlying reality bears little resemblance to genuine consent.

Empirical research consistently confirms this gap. McDonald and Cranor estimated that reading the privacy policies an average user encounters in a year would consume hundreds of hours, rendering genuine informed engagement practically impossible.[7] Daniel Solove has called this phenomenon the 'consent dilemma' of privacy self-management: the more rights individuals are given to make decisions about their data, the more decisions they must make, and the less capable they become of making any of them well. Elettra Bietti has gone further, arguing that consent has become a 'free pass' that allows powerful platforms to immunise

themselves from regulatory scrutiny by extracting agreement to terms that no rational user would accept under conditions of meaningful choice.[8]

The fictive character of consent is most acute in the relationship between individual users and the small number of dominant technology companies that operate the platforms through which most online activity is conducted. Users typically lack the technical knowledge to understand how their data will be processed, the bargaining power to negotiate alternative terms, and any practical alternative to the dominant service. Network effects, switching costs, and the absence of interoperability mean that declining consent often entails exclusion from the basic infrastructure of contemporary social, economic, and political life. The fiction theory does not necessarily entail abandoning consent as a legal device. It does, however, demand intellectual honesty about what consent in this context actually achieves, and it suggests the need for supplementary mechanisms—purpose limitation, data minimisation, and substantive prohibitions—that do not rely on the unrealistic assumption of a fully informed, autonomous data subject.

4. CONSENT UNDER THE GDPR: A RIGOROUS STANDARD WITH OPERATIONAL LIMITS

4.1 Defining Informational Privacy and Constitutional Anchoring

To understand the GDPR's treatment of consent, one must first appreciate the normative concept consent is asked to protect: informational privacy. The classical conception was articulated by Warren and Brandeis as 'the right to be let alone'.[10] Computerised processing rendered that formulation insufficient, as personal information once disclosed can be aggregated and analysed at virtually no cost. Alan Westin reformulated privacy as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others.[11] Helen Nissenbaum has refined this through contextual integrity: information appropriate to share with a doctor may be wholly inappropriate to share with an employer or advertiser.[12] The Indian Supreme Court's recognition in *Puttaswamy* that informational privacy is a facet of the fundamental right under Article 21 echoes this control-based conception.[9]

4.2 The Four Cumulative Conditions: Article 4(11)

Article 4(11) of the GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement.'[13] Four cumulative conditions must therefore be

satisfied. The *freely given* requirement demands genuine choice and the absence of coercion. The *specific* requirement insists on clearly identified purposes, rendering bundled consents incompatible with the Regulation. The *informed* requirement obliges controllers to disclose, in clear and plain language, the identity of the controller, the purposes of processing, and the categories of data. The *unambiguous* requirement, reinforced by the demand for a clear affirmative action, definitively excludes silence, inactivity, and pre-ticked boxes.

4.3 Operational Conditions: Article 7

Article 7 supplements these definitional provisions. Article 7(1) imposes a burden of proof on the controller to demonstrate that consent was given. Article 7(2) requires consent requests embedded in broader documents to be presented in a manner clearly distinguishable, intelligible, and easily accessible. Article 7(3) guarantees the right to withdraw consent at any time, with the requirement that withdrawal be as easy as the giving of consent. Article 7(4) addresses conditionality, providing that utmost account must be taken of whether the performance of a contract is made conditional on consent to processing not necessary for that contract.[14]

4.4 The Jurisprudence of the Court of Justice

The Court of Justice has reinforced this strict reading. In *Planet49*, the Court held that pre-ticked checkboxes do not constitute valid consent, since silence or inactivity cannot satisfy the requirement of an unambiguous indication.[15] The *Schrems* line of authority addresses the systemic adequacy of legal frameworks within which consent operates: the Court invalidated both the Safe Harbour and the Privacy Shield decisions for failing to ensure essentially equivalent protection in third countries.[19] Most recently, in *Meta v. Bundeskartellamt*, the Court held that the dominant position of a controller is a relevant factor in assessing whether consent is freely given—a recognition that consent's voluntariness is structural, not merely subjective.[29]

4.5 The Lawfulness Framework: Article 6 and Special Categories

Consent is one of six lawful bases for processing under Article 6(1).[16] Where processing concerns special categories—data revealing racial or ethnic origin, political opinions, religious beliefs, health data, or sexual orientation—Article 9 imposes a stricter regime requiring explicit consent.[17] Recital 43 provides that consent should not be regarded as freely given where there is a clear imbalance between the data subject and the controller—an explicit recognition of the structural power asymmetries that the legal fiction critique foregrounds.[18]

5. CONSENT UNDER THE DPDP ACT 2023: A CONSTITUTIONAL EXAMINATION

5.1 Constitutional and Policy Foundations

The constitutional foundation of the DPDP Act lies in *Puttaswamy*, which held the right to privacy to be a fundamental right protected as an intrinsic part of Article 21. Justice Chandrachud, writing the plurality opinion, identified informational privacy as encompassing the individual's interest in controlling the dissemination of personal information. Crucially, the judgment articulated the doctrinal test that any infringement of privacy must satisfy: legality, legitimate State aim, proportionality, and procedural safeguards.[31] The Srikrishna Committee Report (2018) translated these constitutional commitments into a policy framework, observing that consent had become a 'fairy tale' in many digital contexts because of asymmetries of information and bargaining power, and recommending a hybrid architecture combining consent with non-consent grounds, an independent regulator, and heightened safeguards for sensitive data.[27]

5.2 Section 6: The Consent Standard

Section 6(1) of the DPDP Act provides that consent must be free, specific, informed, unconditional, and unambiguous, with a clear affirmative action.[21] The textual resemblance to Article 4(11) of the GDPR is striking, with the notable substitution of 'unconditional' for the GDPR's implicit conditionality test. Section 6(3) requires the notice to be available in English or any of the twenty-two languages set out in the Eighth Schedule to the Constitution at the option of the data principal—a provision of considerable practical significance in a multilingual jurisdiction.[22] Sections 6(4) and 6(5) introduce the consent manager, an intermediary registered with the Data Protection Board through whom data principals may give, manage, review, and withdraw consent across multiple data fiduciaries.[23] The provision is novel and reflects an architectural choice peculiar to the Indian framework, intended to ease the burden of consent management.

5.3 Section 7: The Question of Deemed Consent

The 2022 draft of the Bill had introduced the controversial concept of 'deemed consent', by which the data principal would be presumed to have consented in a wide range of circumstances. Following extensive criticism, the 2023 Act replaced 'deemed consent' with section 7, titled 'Certain Legitimate Uses'.[24] The terminological change is significant: the Act no longer presents these grounds as forms of consent at all, but as alternative, non-consent-based legal bases for processing—including processing by the State for subsidies and benefits,

compliance with statutory orders, medical emergencies, employment-related purposes, and disasters. The list is exhaustive: the Act contains no residual 'legitimate interests' basis equivalent to GDPR Article 6(1)(f), with the consequence that consent in India must do more regulatory work than in Europe.

5.4 Section 17: The Government Exemption Regime

One of the most contested features of the Act is the breadth of the exemptions available to instrumentalities of the State. Section 17(2) empowers the Central Government, by notification, to exempt any instrumentality of the State from the application of the provisions of the Act in the interests of sovereignty, security, friendly relations with foreign States, public order, or the prevention of incitement to a cognisable offence.[25] The grounds substantially track those that *Puttaswamy* identified as legitimate aims for the limitation of fundamental rights, but the absence of express conditions of necessity, proportionality, or independent oversight in the operative text raises a serious question of constitutional compatibility. The proportionality test articulated in *Puttaswamy* requires that any restriction be the least intrusive means available to achieve the legitimate aim and that the law include adequate procedural safeguards. Whether section 17 will withstand scrutiny against this benchmark is likely to be the subject of future litigation.[32]

5.5 The Data Protection Board

Sections 18 and 19 establish the Data Protection Board of India as the supervisory authority. The Board is appointed by the Central Government on terms and conditions to be prescribed by rules, and its functions are essentially adjudicatory and remedial.[26] The Board does not possess the plenary rule-making and policy-shaping competence of a typical European supervisory authority; the rule-making power vests primarily in the Central Government, which is itself a major potential data fiduciary and a beneficiary of the section 17 exemption regime. The Srikrishna Committee had recommended a substantially more autonomous regulator, with security of tenure, plenary powers to issue regulations, and the capacity to investigate proactively. The narrowing of these competences in the 2023 Act represents a deliberate legislative choice and one of the principal points at which the Indian regime falls short of the international benchmark set by the GDPR.

6. THE LEGAL FICTION IN PRACTICE: COMPARATIVE CRITIQUE

6.1 Convergence in Form, Divergence in Substance

The textual proximity of Article 4(11) of the GDPR and section 6(1) of the DPDP Act is not accidental: it reflects the GDPR's status as a global benchmark. Yet the operational reality in both jurisdictions reveals the legal fiction at work. Under the GDPR, empirical and regulatory studies have documented widespread non-compliance with the requirements of granularity, withdrawal, and informed presentation, particularly in cookie consent interfaces and platform terms of service.[28] Enforcement has been concentrated in a small number of high-profile decisions and hampered by jurisdictional disputes under the one-stop-shop mechanism. Under the DPDP Act, the structural deficiencies are even more pronounced: the absence of categories of sensitive data, the omission of rights to data portability and against automated decision-making, the breadth of section 17, the institutional subordination of the Data Protection Board, and an absolute-cap penalty methodology weaker than the GDPR's turnover-based regime.[30]

6.2 Dark Patterns, Bundled Consent, and the Manufactured Choice

The fictive character of consent is most acute in the systematic deployment of deceptive design patterns, or 'dark patterns', through which platforms manipulate user choice via visual hierarchies, default settings, and confirmshaming. The European Data Protection Board has acknowledged that such designs vitiate the freely given character of consent. The Indian framework currently lacks comparable guidance, and the freely given character of consent under section 6(1) cannot survive the systematic deployment of interface design choices that nudge users towards acceptance. Bundled consent—conditioning access to services on agreement to processing for unrelated purposes—remains pervasive in both jurisdictions, despite its formal prohibition. The German Federal Cartel Office's *Facebook* decision and the subsequent CJEU judgment in *Meta v. Bundeskartellamt* recognise that the dominant position of a controller is a relevant factor in assessing whether consent is freely given.[29]

6.3 The Constitutional Stakes

In the Indian context, the legal fiction of consent has constitutional consequences. *Puttaswamy* requires that any infringement of informational privacy satisfy the proportionality framework of legality, legitimate aim, proportionality, and procedural safeguards. A consent regime that operates as a fiction—legitimating processing through agreements that are coerced, uninformed, manipulated, or meaningless—cannot satisfy this standard. The textual rigour of section 6 is, if anything, more demanding than Article 4(11): the inclusion of 'unconditional' as

an express criterion, the multilingual notice obligation, and the consent manager mechanism each represent advances over the European text. Yet a textually rigorous standard cannot deliver substantive autonomy if it is undermined by exemptions inadequately tested for proportionality, by an institution lacking the independence to enforce it, by penalties insufficient to deter the largest controllers, or by transfer rules that permit data to flow to jurisdictions in which the safeguards established by the Act are unavailable.

7. CONCLUSION AND RECOMMENDATIONS: BEYOND THE CONSENT PARADIGM

This article has argued that consent under both the GDPR and the DPDP Act 2023 functions more as a procedural legal formality than a substantive protection of individual autonomy. The hypothesis is substantiated: although the Indian Act establishes a textually rigorous standard of consent that closely follows international best practice, its operational effectiveness in securing the substantive informational autonomy promised by *Puttaswamy* is materially compromised by structural deficiencies in the Act and its institutional architecture. Comparative engagement with the GDPR identifies specific reforms necessary to remedy these deficiencies. The fundamental insight is that no consent regime, however textually rigorous, can by itself deliver the substantive autonomy that data protection law promises.

Several normative recommendations follow. *First*, the elimination of the sensitive personal data category should be revisited; categories such as health, biometric, religious, caste, sexual orientation, and political affiliation data deserve heightened protection on the model of GDPR Article 9(2)(a). *Second*, the rights catalogue should be strengthened to include rights to data portability and protection against decisions taken solely on the basis of automated processing—essential safeguards in an era of algorithmic decision-making in lending, insurance, and welfare administration. *Third*, the section 17 exemption power should be amended to incorporate express requirements of necessity, proportionality, and minimum impairment, with mandatory publication of reasons and periodic independent review.

Fourth, the institutional architecture of the Data Protection Board should be brought into closer alignment with the Srikrishna Committee's recommendations, with security of tenure, plenary regulatory powers, and budget independent of executive discretion. *Fifth*, the absolute-cap penalty regime should be supplemented by a turnover-based alternative on the model of GDPR Article 83. *Sixth*, the Board should issue guidance on dark patterns and consent interfaces, drawing upon the work of the European Data Protection Board. *Seventh*, consent assessment under section 6 should be informed by the principle of contextual integrity, recognising that

information appropriate to share in one context may be wholly inappropriate to share in another.

Most fundamentally, India must move decisively beyond consent formalism toward enforceable data minimisation, algorithmic accountability, purpose limitation, and an institutionally independent Data Protection Board—so that data subject rights are transformed from paper guarantees into lived constitutional realities. Consent must be embedded in a wider architecture of independent supervision, deterrent enforcement, structural prohibitions on the most harmful practices, and recognition of the asymmetries of power that distort the conditions of choice. The challenge for the Indian regime, as it moves from enactment to implementation, is to construct that wider architecture in a manner consistent with both the universal principles of informational privacy and the distinctive constitutional and social context of India.

ENDNOTES / REFERENCES

1. Shoshana Zuboff, *The Age of Surveillance Capitalism* 63–97 (2019).
2. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1880–1883 (2013).
3. John Locke, *Two Treatises of Government* bk. II, ch. VIII (Peter Laslett ed., 1988).
4. Immanuel Kant, *Groundwork of the Metaphysics of Morals* 4:429 (Mary Gregor trans., 1998).
5. Nuremberg Code (1947); World Medical Association, Declaration of Helsinki (1964, as amended).
6. Lon L. Fuller, *Legal Fictions* 9–12 (1967).
7. Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 562–565 (2008).
8. Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 Pace L. Rev. 307, 320–326 (2020).
9. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
10. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
11. Alan F. Westin, *Privacy and Freedom* 7 (1967).
12. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 127–157 (2010).
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 4(11) [hereinafter GDPR].

14. GDPR art. 7.

15. Case C-673/17, Bundesverband der Verbraucherzentralen v. Planet49 GmbH, ECLI:EU:C:2019:801.

16. GDPR art. 6(1).

17. GDPR art. 9.

18. GDPR recital 43; European Data Protection Board, Guidelines 05/2020 on Consent ¶¶ 13–24 (May 4, 2020).

19. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650; Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Schrems, ECLI:EU:C:2020:559.

20. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023) [hereinafter DPDP Act].

21. DPDP Act § 6(1).

22. DPDP Act § 6(3).

23. DPDP Act § 6(4)–(5).

24. DPDP Act § 7.

25. DPDP Act § 17(2).

26. DPDP Act §§ 18–19.

27. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (MeitY, July 2018).

28. Bart W. Schermer, Bart Custers & Simone van der Hof, *The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection*, 16 Ethics & Info. Tech. 171, 174–178 (2014).

29. Bundeskartellamt, Facebook, Decision B6-22/16 (Feb. 6, 2019); Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537.

30. GDPR art. 83(5); DPDP Act § 33 and Schedule.

31. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶ 310 (India).

32. Smriti Parsheera, *India's Digital Personal Data Protection Act 2023: Analysis and Open Questions*, 9(2) Indian J.L. & Tech. 1 (2023).