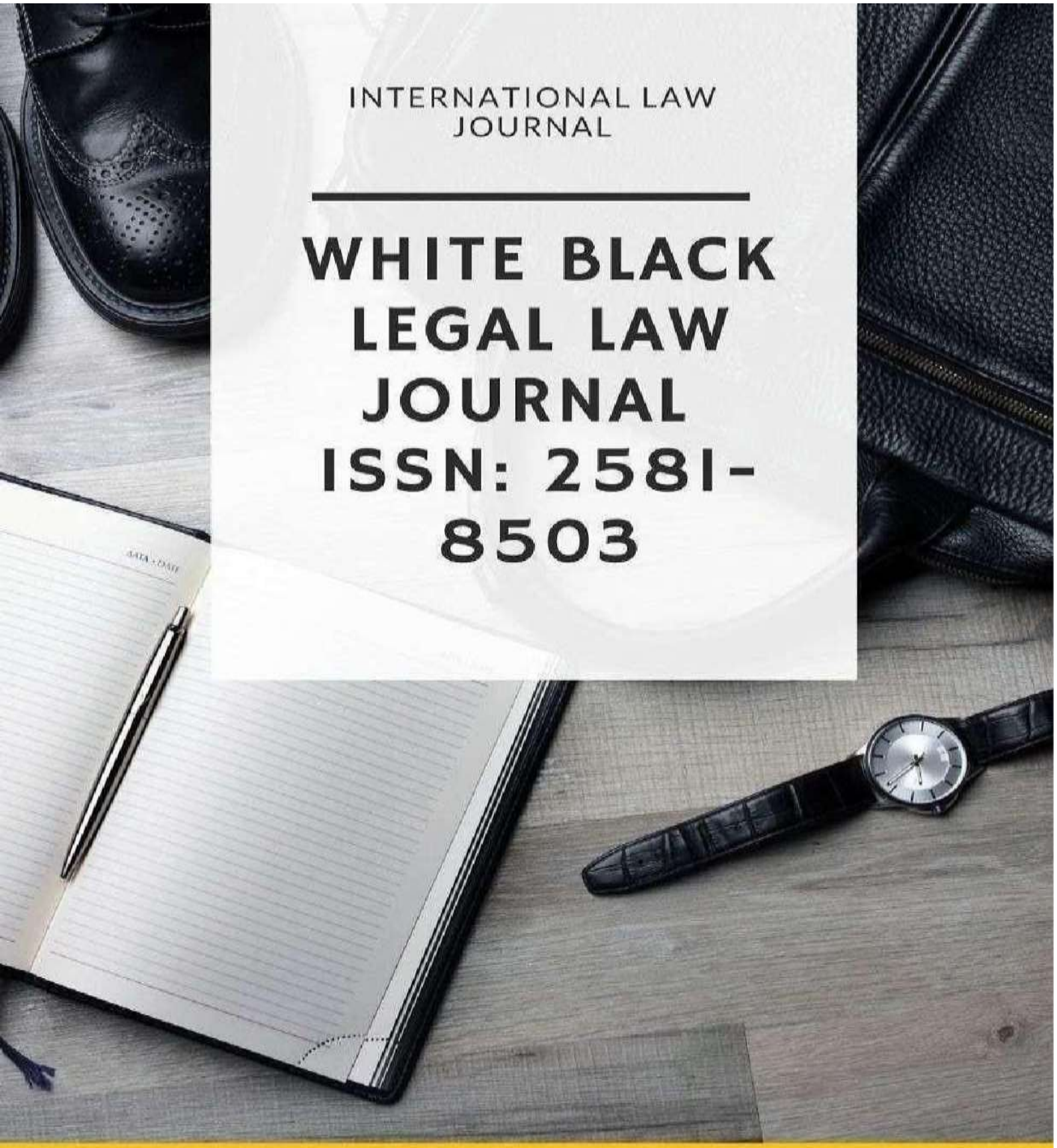

INTERNATIONAL LAW JOURNAL

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.

FREE SPEECH, PRIVACY, AND THE PRESS: RETHINKING CONSTITUTIONAL BALANCING UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - DEEPANSHI GARG

The idea of free speech has never been neat. When it works well, it is the lifeblood of democracy, enabling people to question authority, confront difficult realities, and engage in public life on a level playing field. However, this same freedom creates some of the most complex legal and moral dilemmas of our day when it clashes with individual privacy and a media ecosystem that is becoming more and more powerful. This essay questions whether the constitutional frameworks designed to handle those collisions are still effective.

State censorship was a fairly straightforward enemy when the First Amendment was adopted. The world we live in today, where a private platform can spread a false story to millions of people in a matter of seconds, where a journalist and an anonymous social media account make nearly identical legal claims to press protection, and where it is genuinely hard to distinguish between newsgathering and surveillance, is what it was not intended for. The old doctrinal tools are being pushed to perform tasks for which they were never designed, such as defamation standards developed in the 1960s, newsworthiness assessments created for a print era, and privacy torts that were already uncomfortable prior to the internet.

In American constitutional law, privacy is structurally weak. In the United States, privacy is mostly viewed as a tort, a remedy sought after the harm has been done and one that the First Amendment frequently thwarts, in contrast to European systems where it is recognized as a basic right capable of directly restricting what the press may disclose. More complex frameworks have been proposed by academics like Helen Nissenbaum, who contends that privacy is more about whether information moves in a fashion that respects the norms of the culture in which it was originally exchanged than it is about secrecy per se. Compared to what current theology offers, this framing—contextual integrity—points toward a deeper and more convincing understanding.

The issues are more than just theoretical. It is now feasible to create voice and video of actual individuals with remarkable realism thanks to deepfake technology, causing harm that defamation law is ill-equipped to address. Intimate personal profiles are compiled by data brokers, who assert First Amendment protection for this practice. Platforms deny editorial accountability while simultaneously invoking editorial discretion. A disconnect between the constitutional framework and the reality it is meant to control is revealed in each of these circumstances.

The current situation calls for a more honest recognition of the fact that speech can also be a weapon, that privacy and expression are both essential components of a free society, and that deciding between them necessitates more than just reflexively protecting whoever speaks loudest. This is not to say that free speech should be abandoned as a value because it is still indispensable. Legislators, courts, and finally the public must determine what kind of information environment they truly desire. The Constitution provides a place to start rather than a solution.

Keywords: *First Amendment, free speech, privacy rights, press freedom, defamation, data protection, contextual integrity, digital media, constitutional law, platform liability*

INTRODUCTION

Living in a time when there are more ways to express oneself than ever before while also feeling more concerned about the expense of doing so is almost paradoxical. We publish more, speak more, and reach a wider audience than any preceding generation. At the same time, there is mounting evidence that unrestricted speech, as a constitutional principle, can seriously expose actual persons. This essay does not address the topic of whether free speech is important. It really does. The question is whether the legal framework that surrounds it, which was mostly created in a pre-digital period and was influenced by presumptions about print newspapers and government censors, can still handle the tensions that arise from contemporary media and privacy concerns.

The conflict between personal privacy and freedom of expression is not new. Through defamation lawsuits, intrusion torts, and discussions about what the press is allowed to disclose about private individuals, courts have been navigating this issue for more than a century.

However, rather than just changing its magnitude, the digital revolution in public communication has fundamentally altered the essence of that conflict. A private truth that is published today does not disappear from a newspaper's archive; instead, it endures, spreads, and can be retrieved indefinitely. The distinction between investigative reporting and surveillance blurs in ways that previous jurisprudence is unable to clearly address when a journalist gains access to someone's location information or private communications. The law is finding it difficult to keep up with the various types of harms.

The First Amendment has traditionally served as somewhat of a trump card in speech and privacy conflicts in the United States. From New York Times Co. v. Sullivan (1964), which protected press freedom through the actual malice standard, to Snyder v. Phelps (2011), which protected even extremely offensive public protest, the Supreme Court's seminal decisions demonstrate a constitutional culture that favors expression and firmly places the burden of proof on those who would restrict it. Genuine products of that culture include a free press, strong political opposition, and a custom of holding those in positions of authority accountable. However, it has also created a legal environment in which private interests frequently lose when a speaker invokes the First Amendment, even in cases when the public interest is only marginally served and the harm is severe.

There has been a significant shift in the European constitutional tradition. The General Data Protection Regulation (GDPR) views privacy as a basic right in and of itself, capable of directly restricting what media companies and individuals may gather, keep, and publish about others, rather than as a residual interest to be weighed against speech. A philosophical commitment to informational self-determination that has no true equivalent in American constitutional doctrine is reflected in the right to be forgotten, the principle of data minimization, and the requirement of a legitimate justification for processing personal information. These indicate different responses to the fundamental question of whose values a democratic legal order prioritizes; they are not just technical regulatory distinctions.

At a time when the stakes could hardly be higher, India is setting its own route. The Digital Personal Data Protection Act, 2023 (DPDP Act), which establishes a statutory framework for the processing of digital personal data and creates binding obligations for data fiduciaries and enforceable rights for data principals, is India's largest legislative intervention in the privacy space to date. The DPDP Act, which was passed in response to the Supreme Court's historic

ruling in Justice K.S. Puttaswamy v. Union of India (2017), which acknowledged privacy as a fundamental right under Article 21 of the Constitution, aims to operationalize that constitutional guarantee in the digital sphere. However, the question of how it relates to free expression, which is protected by Article 19(1)(a), is still unresolved and extremely challenging. The Act provides exclusions for state security and journalistic purposes, but the limits of those exemptions are not clearly defined, and there is still a conflict between the press's right to disclose and preserve information and the data principal's right to erasure.

The structure of the DPDP Act also poses issues that go beyond press freedom in the traditional sense. Consent requirements, purpose limitation principles, and data retention restrictions now apply to data fiduciaries, which include media platforms, news aggregators, and social media companies operating in India. These regulations have a direct impact on the collection, storage, and distribution of personal data. Regulatory advice and, eventually, litigation will be used to determine if and how these requirements interact with the constitutional protection of speech and the press. Even if the decisions made by the Data Protection Board under the Act are phrased in terms of data regulation, they are fundamentally constitutional in nature.

This essay makes the case that, when considered collectively in the American, European, and Indian contexts, these developments necessitate a reconsideration of how constitutional free speech doctrine addresses its concerns with media power and privacy rights. With a focus on the unresolved conflicts between data protection and press freedom in the Indian constitutional context, the research paper analyzes the DPDP Act in detail, looks at the structural flaws in American First Amendment doctrine when applied to privacy disputes, evaluates the GDPR model and what it offers as an alternative framework, and suggests a set of principles derived from comparative analysis that might direct more cogent and rights-respecting approaches to these conflicts. The point made throughout is not that free speech should be restricted for its own sake, but rather that a legal system that is truly dedicated to both expression and dignity needs to create more advanced instruments than it does now to negotiate the area where those ideals collide.

LITERATURE REVIEW

Although the literature on the precise connection with digital data protection is still relatively new, the relationship between free expression and privacy in Indian constitutional law has garnered consistent scholarly attention. In his groundbreaking contribution to the Journal of

the Indian Law Institute, Sorabjee established the doctrinal foundation by pointing out that the Indian approach's primary flaw was the lack of a structured balancing test and contending that neither Article 19(1)(a) nor the then-emerging privacy right could be regarded as wholly superior to one another. This diagnosis is still accurate and serves as the conceptual foundation for the current investigation.

Scholarship turned to examining the constitutional ramifications of a freestanding right to privacy after the Supreme Court's historic decision in Puttaswamy. Bhatia studied how private entities, such as media organizations, might be constrained by the horizontal application of the privacy guarantee and argued that any restriction of the right must be subject to proportionality analysis.[1] A more skeptical interpretation of the legislative answers was provided by Matthan, who questioned whether the subsequent draft data protection laws were sufficient to carry out the constitutional obligation they claimed to.[2] By extending the research to the big data setting, Basheer and Kochupillai found fundamental conflicts that the current framework had failed to address between data-driven journalism and individual informational sovereignty.[3]

Bhandari and Rahman offer the most thorough analysis of the DPDP Act, 2023 from a statutory perspective to date, pointing out the Board's institutional structure and the journalistic exemption gap as its main flaws.[4] Because it examines how constitutional free expression standards limit regulation design in the digital sphere, Ganz's past work on intermediary responsibility following Shreya Singhal is still pertinent.[5] In the comparative register, Nissenbaum's contextual integrity framework[6] and Rosen's critique of the right to be forgotten[7] together frame the principal theoretical tensions that Indian law must now confront. The present article builds on this body of work by analysing how the DPDP Act specifically alters the speech-privacy equilibrium and what constitutional principles should govern its interpretation.

[1]Gautam Bhatia, 'Horizontal Rights and the Right to Privacy in India' (2018) 13(1) Asian Journal of Comparative Law 115.
[2]Rahul Matthan, 'The Privacy (Protection) Bill: A Critique' (2018) 53(3) Economic and Political Weekly 14.
[3]Shamnad Basheer and Mrinalini Kochupillai, 'The Privacy Paradox in the Age of Big Data: Indian and Comparative Perspectives' (2019) 61(4) Journal of the Indian Law Institute 435.
[4]Vrinda Bhandari and Faiza Rahman, 'The Digital Personal Data Protection Act 2023: A Critical Analysis' (2024) 59(1) Journal of the Indian Law Institute 1.
[5]Kian Ganz, 'Intermediary Liability and Free Speech in India after Shreya Singhal' (2016) 28(2) National Law School of India Review 45.
[6]Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).
[7]Jeffrey Rosen, 'The Right to Be Forgotten' (2012) 64 Stanford Law Review Online 88.

RESEARCH METHODOLOGY

This study uses a doctrinal research approach, mainly analyzing statute texts, court rulings, and constitutional clauses. The Indian Constitution, the Digital Personal Data Protection Act of 2023, and rulings from the Supreme Court, including Justice K.S. Puttaswamy (Retd.) v. Union of India, are examples of primary sources. Peer-reviewed articles from the Journal of the Indian Law Institute and comparative legislation resources, such as the GDPR, are examples of secondary sources. To place the Indian framework in the context of the worldwide conversation on free expression and privacy, a comparative method is used. There was no attempt to gather empirical data.

CONSTITUTIONAL FREE SPEECH AND PRIVACY: MAPPING THE CONFLICT

The tension between free expression and privacy is not novel in Indian constitutional jurisprudence, but the digital environment has rendered it acute in ways that existing doctrine was not designed to address. Article 19(1)(a) of the Constitution of India guarantees to every citizen the right to freedom of speech and expression.[8] Article 21 guarantees the right to life and personal liberty, which the Supreme Court has progressively read to encompass a wide range of unenumerated rights, including the right to privacy.[9] The relationship between these two provisions — and the manner in which they are to be balanced when they conflict — remained unsettled for decades. It was only with the nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v Union of India*[10] that the Court placed that relationship on a coherent constitutional footing, recognising privacy as a fundamental right and acknowledging that it would require proportionality-based balancing against other fundamental freedoms.

Justice D.Y. Chandrachud, in the leading concurring opinion, identified informational privacy — the right of individuals to control the dissemination of material that is personal to them — as a distinct dimension of the Article 21 guarantee.[11] He was careful, however, to note that privacy is not an absolute right and that its assertion must be weighed against competing constitutional interests, including the freedom of speech and expression and the public interest

[8]Constitution of India, art. 19(1)(a).
[9]Constitution of India, art. 21.
[10]Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.
[11]Ibid., para 169 (Chandrachud J, concurring).

in access to information.[12] This acknowledgment of the need for balancing is significant, but the Court did not prescribe how that balancing should proceed in the specific context of media publication or digital data processing. That task has been left, in large part, to the legislature — and the legislature has responded with the DPDP Act — and to the courts that will inevitably be asked to interpret it.

Before the *Puttaswamy* judgment, the primary judicial treatment of the privacy–expression tension in the Indian media context was found in the Supreme Court's decision in *R. Rajagopal v State of Tamil Nadu*,[13] which recognised a constitutional right to privacy capable of limiting press publication of private facts. The Court held that a citizen has a right to safeguard the privacy of their own, their family, marriage, procreation, motherhood, child-bearing and education, among other matters, and that no one may publish anything concerning these matters without consent.[14] However, it also recognised that this right yields in relation to public officials and public figures acting in their official capacities, anticipating the distinction between the private sphere and the public role that later doctrine would develop. *Rajagopal* thus established the conceptual architecture within which the DPDP Act must now be read: privacy as a real and enforceable limit on expression, but one that admits of qualification in the public interest.

The intermediary liability framework under Section 79 of the Information Technology Act, 2000[15] added a further dimension to this landscape by granting conditional immunity to online intermediaries — including news platforms and social media companies — for third-party content, subject to compliance with government takedown directions. In *Shreya Singhal v Union of India*,[16] the Supreme Court struck down Section 66A of the IT Act as an unconstitutional restriction on free speech and narrowed the scope of mandatory takedowns under Section 79, requiring that removal of content be authorised by a court order or government notification in accordance with established legal procedure. The decision reinforced the constitutional primacy of Article 19(1)(a) in the digital context, but it did not address how that primacy is to be reconciled with privacy interests — a gap that the DPDP Act

[12]Ibid., para 179.
[13]R. Rajagopal v State of Tamil Nadu, (1994) 6 SCC 632, 649.
[14]Ibid., 650.
[15]Information Technology Act 2000 (Act 21 of 2000) (India), s 79.
[16]Shreya Singhal v Union of India, (2015) 5 SCC 1, para 81.

now enters to fill, at least in part.

THE DPDP ACT, 2023: ARCHITECTURE AND CONSTITUTIONALFOUNDATIONS

A. Legislative History and Constitutional Mandate

The Digital Personal Data Protection Act, 2023[17] received presidential assent on 11 August 2023, following nearly five years of legislative deliberation that began with the Justice B.N. Srikrishna Committee's report and draft Personal Data Protection Bill of 2018. The Act constitutes India's first comprehensive statutory framework for the protection of digital personal data and is the legislature's principal response to the constitutional mandate articulated in *Puttaswamy*. Its enactment was also prompted by India's obligations under bilateral and multilateral trade arrangements, the growing importance of data flows to the Indian digital economy, and the absence of any sector-neutral privacy legislation capable of regulating the conduct of both state and private actors in the data space.

The Act's territorial scope is defined by Section 3, which applies it to the processing of digital personal data within India and, in notified circumstances, to processing outside India where the processing relates to offering goods or services to data principals within India.[18] This extraterritorial limb is significant for media organisations with international operations and for foreign-owned digital platforms that serve Indian users — it brings them within the regulatory perimeter of the Act regardless of where their servers or editorial offices are located. The Act applies to personal data that has been collected online and to personal data collected offline and subsequently digitised, ensuring that legacy print media archives that have been converted to digital form are not excluded from its scope.

B. Data Fiduciaries, Data Principals, and Core Obligations

The Act's regulatory architecture is built around the obligations of *data fiduciaries* — defined as persons who alone or in conjunction with other persons determine the purpose and means of processing personal data[19] — and the corresponding rights of *data principals*, meaning the individuals to whom personal data relates. News organisations, digital media platforms, data brokers, and social media companies all fall within the definition of data fiduciary to the extent

[17]Digital Personal Data Protection Act 2023 (Act 22 of 2023) (India) [hereinafter DPDP Act].
[18]DPDP Act, s 3.
[19]DPDP Act, s 4.

that they determine how personal data about individuals is collected and used. This is a deliberately broad category, and its application to journalism and media activity is one of the Act's most significant and least resolved dimensions.

Data fiduciaries are required under Section 4 to process personal data only for lawful purposes either with the consent of the data principal or for certain specified legitimate uses set out in the Act.[20] The consent requirement is modelled on international data protection norms and requires that consent be free, specific, informed, unconditional, and unambiguous — a standard that most existing media data collection practices were not designed to meet. Data principals are granted rights under Sections 11 to 14 to obtain information about their personal data, to correct inaccurate or incomplete data, to erase their data in defined circumstances, and to nominate a representative to exercise these rights on their behalf.[21] The erasure right is of particular salience in the media context and is addressed further in Section IV below.

The Act creates an additional tier of regulation for *significant data fiduciaries*, to be designated by the Central Government on the basis of the volume or sensitivity of personal data processed, or the risk posed to the rights of data principals.[22] Significant data fiduciaries bear heightened obligations, including the appointment of a data protection officer, the engagement of an independent data auditor, and the conduct of data protection impact assessments. Large digital news platforms and social media companies operating in India may reasonably expect to be designated as significant data fiduciaries, with correspondingly greater compliance burdens.

C. The Data Protection Board: Institutional Design and Independence

The Act establishes a Data Protection Board of India under Sections 18 and 19 as the primary adjudicatory body for complaints and breaches.[23] The Board is empowered to receive complaints from data principals, conduct inquiries, impose financial penalties, and issue directions for remediation. The chairperson and members of the Board are to be appointed by the Central Government, and the Act's provisions on appointment, tenure, and removal give the executive significant influence over the composition of the body. This has attracted criticism from scholars who argue that a body adjudicating conflicts between fundamental rights — including freedom of expression and privacy — must possess genuine structural

[21]DPDP Act, ss 11–14.
[22]DPDP Act, s 9.
[23]DPDP Act, ss 18–19.

independence from the executive if its decisions are to carry constitutional legitimacy.[24]

The concern is not merely theoretical. A Board that is susceptible to executive influence may exercise its jurisdiction in ways that chill investigative journalism by imposing data protection liability on reporters, or conversely may defer to state and corporate interests by failing to protect data principals against media exposure of private information. Either failure would be inconsistent with the constitutional mandate of *Puttaswamy*, which requires that privacy be treated as a fundamental right subject to proportionate limitation rather than an administrative convenience to be traded off against other interests at the executive's discretion.

PRESS FREEDOM AND THE DPDP ACT: UNRESOLVED CONSTITUTIONAL TENSIONS

A. The Journalistic Exemption and Its Incomplete Architecture

Section 17(1) of the DPDP Act empowers the Central Government to exempt specified data fiduciaries or classes of data processing from the Act's provisions in the interests of the security of the state, public order, prevention of incitement to cognisable offences, or sovereignty and integrity of India.[25] Section 17(2)(b) separately contemplates the notification of exemptions for processing for purposes such as research, archiving, and journalism.[26] Neither provision, however, specifies the conditions under which a journalistic exemption will be available, the test to be applied in determining whether particular processing qualifies, or the procedural safeguards that will govern the exemption's exercise. Those matters are delegated to subordinate legislation that remained outstanding at the time of this writing.

This delegation is constitutionally significant. In *Shreya Singhal*,[27] the Supreme Court's invalidation of Section 66A turned in large part on the provision's failure to provide clear and narrowly drawn criteria for restricting speech, leaving the exercise of state power over expression insufficiently constrained by law. An exemption framework that leaves to executive notification the determination of which journalistic activities are protected raises an analogous concern in reverse: a media organisation that cannot ascertain in advance whether its data processing is exempt from the Act's obligations cannot meaningfully exercise editorial judgment. Legal uncertainty of this kind has a chilling effect on reporting that is constitutionally equivalent to direct restriction, and courts applying the proportionality

[24]DPDP Act, s 18(3).
[25]DPDP Act, s 17(1).
[26]DPDP Act, s 17(2)(b).

framework of *Puttaswamy* may be required to hold that an exemption framework without judicially reviewable criteria is constitutionally inadequate.

Comparative experience suggests the importance of a clearly drawn journalistic exemption with defined criteria. The European General Data Protection Regulation requires member states, under Article 85, to reconcile data protection with freedom of expression and to provide for exemptions or derogations only insofar as they are necessary to reconcile the right to protection of personal data with freedom of expression and information.[28] While India is not bound by European norms, the GDPR's approach illustrates that a functional exemption must specify the types of processing covered, the conditions of necessity and proportionality, and the remedies available to individuals whose data has been processed in reliance on the exemption. The subordinate legislation issued under Section 17(2)(b) of the DPDP Act must achieve at minimum an equivalent standard if it is to survive constitutional scrutiny.

B. The Data Erasure Right and Media Archives

Section 12 of the DPDP Act grants data principals the right to request erasure of their personal data, and imposes on data fiduciaries an obligation to erase data that is no longer necessary for the purpose for which consent was given or for which the legitimate use was specified.[29] Applied to the media context, this provision raises a direct conflict with the press's interest in maintaining comprehensive and permanently accessible archives of published reporting. A news report that names an individual in connection with an event of public significance — a criminal trial, a corporate fraud, a political controversy — is published for the purpose of contemporaneous reporting. Once that purpose has been served, the individual may argue that the data is no longer necessary and request erasure. If the media organisation cannot identify a continuing legitimate use or a separate legal basis for retention, it may be obliged to comply.

The constitutional dimensions of this conflict are acute. The freedom of the press under Article 19(1)(a)[30] includes not only the right to publish but the right to maintain and make accessible a record of what has been published. Compelled erasure of accurate historical reporting — even in response to an individual's legitimate interest in escaping the past — is a restriction on expression that must be justified under Article 19(2).[31] Article 19(2) permits restrictions on free speech in the interests of, among other things, decency, morality, contempt of court,

[28]Commission Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data [2016] OJ L 119/1 (GDPR), art 17.

[29]DPDP Act, s 12.

[31]Constitution of India, art. 19(2).

defamation, and incitement to an offence, but it does not list privacy as a permissible ground of restriction. Whether privacy interests capable of justifying compelled erasure of truthful reporting can be brought within an Article 19(2) category — or whether the erasure right as applied to the press is simply unconstitutional — is a question that has not been addressed by any Indian court and that the DPDP Act leaves entirely open.

Soli Sorabjee, writing on the tension between press freedom and privacy in the Indian constitutional context, observed that the resolution of this conflict requires a contextual approach that asks not merely whether information is true and published, but whether publication genuinely serves the public interest or whether it merely inflicts private harm in the guise of public discourse.[32] That observation retains its force in the DPDP Act context. A framework that requires data fiduciaries to erase personal data on demand, without any mechanism for courts or regulators to assess the democratic value of the publication in question, fails to perform that contextual inquiry and will produce results that are arbitrary from a constitutional standpoint.

A COMPARATIVE PERSPECTIVE: PRINCIPLES FOR CONSTITUTIONAL RESOLUTION

A comparative survey of how other jurisdictions have addressed the speech–privacy tension does not yield a ready-made solution, but it does suggest the principles that any constitutionally adequate resolution must incorporate. Three principles are of particular relevance to the Indian context.

The first is what the American scholar Helen Nissenbaum has called contextual integrity.[33] Privacy, on this account, is not violated whenever information that was once private is disclosed; it is violated when information flows in a manner inconsistent with the norms of the context in which it was originally shared. Information shared with a medical professional flows appropriately to other treating clinicians but not to journalists. Personal communications shared within a domestic setting are not rendered public simply because they were not encrypted. This principle reorients the analysis from the binary question of whether information is secret to the more nuanced question of whether its disclosure respects the reasonable expectations of the

[32]Soli J Sorabjee, 'Freedom of Expression and the Right to Privacy: Resolving the Conflict' (2009) 51(1) Journal of the Indian Law Institute 1, 9.

[33]Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010) 127–28.

person to whom it relates. In the DPDP Act context, it provides a framework for assessing whether the processing of personal data by a media organisation is consistent with the contextual norms in which the data was generated — a more principled basis than the current Act provides for distinguishing legitimate journalism from intrusive exposure.

The second principle concerns the standard for justifying press publication of private facts. Gautam Bhatia, writing on horizontal rights and privacy in India, has argued that the proportionality framework requires not merely that a countervailing interest exist, but that the restriction of the opposing right be the least restrictive means of achieving the legitimate objective.[34] Applied to the press–privacy balance, this means that a media organisation seeking to publish personal information must be able to demonstrate that the publication contributes to a genuine democratic objective — holding power to account, enabling informed civic participation, or documenting events of historical significance — and that the specific information disclosed is no more than is necessary to achieve that objective. A reformed newsworthiness test along these lines, incorporated into the journalistic exemption rules issued under Section 17(2)(b) of the DPDP Act, would give the exemption the constitutional content it currently lacks.

The third principle concerns the structure of institutional review. Vrinda Bhandari and Faiza Rahman, in their critical analysis of the DPDP Act, argue that the Board's dependence on executive appointment is inconsistent with the requirements of constitutional adjudication in the privacy space.[35] They contend that, at minimum, the Board's jurisdiction over cases involving press freedom should be subject to expedited judicial review, and that the standard of review should be one of proportionality rather than the deferential reasonableness standard applicable to ordinary administrative decisions.[36] This argument is correct. The constitutional values at stake — Article 19(1)(a) and Article 21 — are of the highest order. An adjudicatory framework that does not reflect their weight will inevitably produce decisions that are constitutionally inadequate, regardless of the quality of the individuals who occupy the Board.

The surveillance and telephone-tapping jurisprudence of the Supreme Court in *PUCL v Union*

[34]Gautam Bhatia, 'Horizontal Rights and the Right to Privacy in India' (2018) 13(1) Asian Journal of Comparative Law 115, 130.

[35]Vrinda Bhandari and Faiza Rahman, 'The Digital Personal Data Protection Act 2023: A Critical Analysis' (2024) 59(1) Journal of the Indian Law Institute 1, 18.

[36]Ibid., 22.

of India[37] establishes that state action impinging on the right to privacy must satisfy the requirements of legality, legitimate aim, and proportionality. There is no principled reason why the same framework should not govern private action — including media activity — when it impinges on the privacy rights of individuals. The DPDP Act, the journalistic exemption rules, and the Board's adjudicatory practice all provide opportunities to institutionalise that framework. Whether those opportunities are taken will determine whether the Act fulfils its constitutional mandate or merely adds a layer of regulatory complexity to a tension that remains substantively unresolved.

CONCLUSION

The conflict between constitutional free speech and privacy interests is not a problem that admits of a single legislative or judicial solution. It is a structural feature of any legal order that takes both values seriously. The DPDP Act, 2023 is significant precisely because it represents India's first serious attempt to manage that conflict through a comprehensive statutory framework grounded in the constitutional mandate of *Puttaswamy*. Its importance lies not only in what it does — establishing consent requirements, data principal rights, and the Data Protection Board — but in the questions it leaves open: the scope of the journalistic exemption, the interaction between the erasure right and press archives, and the constitutional constraints on the Board's jurisdiction over media activity.

The analysis in this article suggests three conclusions. First, the DPDP Act's journalistic exemption framework, as currently structured through Section 17(2)(b), is constitutionally incomplete and must be given substantive content through subordinate legislation that incorporates a necessity and proportionality standard. Second, the erasure right as applied to media archives raises a genuine Article 19(1)(a) question that has not been addressed by the Act or by any Indian court, and that will require resolution either through the exemption framework or through direct constitutional litigation. Third, the Data Protection Board must be constituted and operated with a degree of institutional independence consistent with the constitutional significance of the rights it is called upon to adjudicate.

The Indian constitutional framework — with its co-equal fundamental rights to speech and privacy, its mature proportionality jurisprudence, and its tradition of creative judicial

[37]PUCL v Union of India, (1997) 1 SCC 301.

interpretation — is well positioned to develop a principled resolution of these tensions. The DPDP Act has created the institutional occasion for that development. Whether the occasion is taken will depend on the quality of the subordinate legislation, the composition and independence of the Board, and the willingness of courts to engage with the constitutional dimensions of the speech–privacy conflict with the seriousness they demand.