LEGAL SILENCING VIA PRIVACY? AN ANALYSIS OF INDIA'S DPDP ACT AND INVESTIGATIVE JOURNALISM

Amiya Sharma[*] Paras Swaroop[*]

Investigative journalism, in its truest form, is the constitutional conscience of democracy. It penetrates institutional secrecy, interrogates power structures, and exposes corruption that conventional mechanisms either overlook or suppress. Whether it was Arun Shourie's fearless exposés on political corruption in Maharashtra, Chitra Subramaniam's seminal unearthing of the Bofors scandal that reshaped public discourse, or the more recent Adani-Hindenburg revelations that echoed across financial and political domains, such journalism depends fundamentally on the ability to collect and report personal data in the public interest. These landmark cases were possible only because journalists could navigate a legal ecosystem that, while imperfect, did not actively criminalize their pursuit. The arrival of the Digital Personal Data Protection Act, 2023 (hereinafter referred to as DPDP Act), however, introduces legal uncertainties that could institutionalize barriers to this kind of vital public interest reporting. The DPDP Act, which purports to give statutory effect to the fundamental right to privacy as affirmed in *Justice K.S. Puttaswamy v. Union of India*[1], creates a framework for consent-based data processing. While this objective is laudable in theory, its implementation lacks the nuance to distinguish between data misuse and data use in the democratic interest. Most notably, the Act is marked by three dangerous silences: the exclusion of journalism from exemption under Section 17[2], the absence of differentiation between personal and sensitive personal data and the sweeping override of transparency embedded in Section 44(3)[3], which dilutes the RTI Act's safeguards under Section 8(1)(j)[4]

and under Section 8(2).[5] These silences, as we shall explore, endanger both journalistic freedoms and the citizen's right to information. The most legally concerning lacuna in the

[*]ARMY INSTITUTE OF LAW, MOHALI.
[*]ARMY INSTITUTE OF LAW, MOHALI
[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India)
[2] Digital Personal Data Protection Act, 2023, §17 (India)
[3] Digital Personal Data Protection Act, 2023, §44(3) (India)
[4] Digital Personal Data Protection Act, 2023, §8(1) (j) (India)
[5] Digital Personal Data Protection Act, 2023, §8(2) (India)

DPDP Act is the deliberate omission of investigative journalism from the category of exempted activities under Section 17[6]. Previous drafts, including the 2018 Srikrishna Committee Bill, the 2019 MEITY draft, and the 2021 JPC report, explicitly carved out exemptions for journalistic activity, acknowledging that investigative reportage often relies on processing personal data without consent to uncover wrongdoing. Their omission in the enacted version of the law not only reflects a shift in legislative intention but also fails to accommodate the core democratic function served by the press. Section 6[7] of the DPDP Act requires consent that is *"free, specific, informed, unconditional and unambiguous"* before processing personal data, a demand that is often infeasible in investigative contexts. The 2025 Draft Rules[8] for the DPDP Act, which could have offered interpretative clarity, have maintained absolute silence on the issue of journalism. No interpretive safe harbours or limited-use exemptions for news reporting are provided, demonstrating a legislative and executive alignment in curbing investigative autonomy.

What further compounds this regulatory vagueness is the DPDP Act's undifferentiated treatment of all personal data. In contrast to the General Data Protection Regulation (hereinafter referred to as GDPR) and the United Kingdom's Data Protection Act, 2018, (hereinafter referred to as DPA) which define and treat sensitive personal data (hereinafter referred to as SPD) as a separate, more protected category, the Indian statute does not create this tiered framework. Under the GDPR, for instance, SPD includes information such as racial origin, political opinions, and health status, data whose misuse would result in significant harm. Processing such data requires heightened safeguards. However, non-sensitive personal data such as publicly available information about a public official's travel expenditure or parliamentary performance can, in defined contexts, be processed without consent where public interest is at stake. This absence of categorization in the DPDP Act leads to an overbroad application of consent and processing obligations even for information that is already in the public domain or accessible under statutory mandates.

Take, for example, a journalist attempting to investigate the irregular allocation of state contracts by correlating corporate donations with government tenders. Even if the information is gleaned from public registers or RTI disclosures, the use of that data in

[6] Digital Personal Data Protection Act, 2023, §17 (India)
[7] Digital Personal Data Protection Act, 2023, §6 (India)
[8] Ministry of Electronics and Information Technology, Draft Rules under the Digital Personal Data Protection Act, 2023 (Issued on Jan. 25, 2025) (India)

reporting could invite liability under the DPDP Act. Section 33[9] does not currently distinguish between unlawfully obtained data and data processed without consent but accessed legally. The act of publication itself becomes vulnerable to challenge, and journalists could be forced into litigation merely for doing their job. This ambiguity severely undermines press freedom and emboldens powerful actors to use privacy law as a shield against exposure.

The situation is exacerbated by Section 44(3)[10] of the DPDP Act, which proposes to amend Section 8(1) (j)[11] of the RTI Act, 2005. As it presently stands, Section 8(1) (j)[12] permits the denial of information that relates to personal matters unless the information pertains to public activity or interest, or is such that it cannot be denied to Parliament. This formulation reflects a balance, one that is consistent with the right to information being a facet of Article 19(1) (a)[13]. Moreover, Section 8(2)[14] of the RTI Act provides that even exempted information must be disclosed if the public interest in disclosure outweighs the harm to the protected interest. This jurisprudence has been reaffirmed by the Supreme Court in *Yashwant Sinha v. CBI*[15], which recognized the supremacy of democratic accountability over bureaucratic privacy. However, the DPDP's amendment seeks to delete the public interest test entirely, introducing a rigid protection for any personal information regardless of its context or implications. If implemented, this would effectively render Section 8(2)[16] otiose, making personal data automatically exempt from disclosure and removing discretion from Public Information Officers. Access to asset declarations, disciplinary records, and performance metrics of public servants, currently available under RTI in the public interest, would be legally closed off. This erasure of discretion could severely constrict investigative access to official documents and institutionalize bureaucratic opacity.

Even more troubling is the Act's silence on who is permitted to investigate under its legal framework. Section 17(1) (c)[17] permits exemptions for investigations and legal processes, but does not clarify whether this includes non-state actors such as journalists or civil society watchdogs. The provision appears to privilege state-led criminal investigations while

[9] Digital Personal Data Protection Act, 2023, §33 (India)
[10] Digital Personal Data Protection Act, 2023, §44(3) (India)
[11] Digital Personal Data Protection Act, 2023, §8(1)(j) (India)
[12] Id
[13] India Const. art 19, cl. 1(a)
[14] Digital Personal Data Protection Act, 2023, §8(2) (India)
[15] Yashwant Sinha v. Cent Bureau of Investigation, (2020) 2 SCC 392 (India)
[16] Digital Personal Data Protection Act, 2023, §8(2) (India)
[17] Digital Personal Data Protection Act, 2023, §17(1)(c) (India)

ignoring the parallel accountability role played by investigative journalism. This interpretative vacuum leaves journalists vulnerable to challenge if they rely on leaked documents or undercover methods to pursue a story. The absence of clarity around *"who may investigate"* gives rise to arbitrary enforcement and selective targeting, a threat that is particularly pronounced in politically sensitive investigations. The chilling effect created by these combined provisions cannot be overstated. Journalists are left to operate in legal uncertainty, where each story involving personal data carries potential regulatory, financial, and criminal consequences. This uncertainty disincentivizes bold reportage and fosters editorial risk-aversion, thereby weakening the democratic function of the press. If unamended, the DPDP regime may be weaponized not only by the State but also by private actors to suppress criticism, inhibit whistleblower disclosures, and delay publication of newsworthy content.

To address these concerns, legal reform must be immediate and purposeful. First, Section 17[18] should be amended to explicitly include journalism conducted in the public interest as an exempted category. This would align Indian law with global best practices under General Data Protection Regulation Article 85[19], which requires a reconciliation of data protection with freedom of expression. Second, the Act must be revised to create a statutory distinction between personal data and sensitive personal data, with the former being subject to more flexible rules in cases of public interest. The definition of personal data is provided under section 2(f)[20] of the act. This definition is very broad, so it can be narrowed down by excluding already available data in the public domain. This will reduce the burden on journalists while handling this data, and they will be able to draw a clear line between sensitive personal data and non-sensitive personal data. Third, the proposed amendment to Section 8(1) (j)[21] of the RTI Act must be withdrawn or revised to preserve the public interest override, thereby safeguarding the democratic ethos of transparency. Fourth, a clarification, either statutory or through delegated legislation, must be issued to ensure that investigative activities by non-state actors fall within the scope of Section 17(1) (c)[22]. And finally, a clear exemption should be created in the Rules under Section 17(5)[23] for recognized journalistic entities, pending legislative amendment, to prevent immediate misuse of the current

[18] Digital Personal Data Protection Act, 2023, §17 (India)
[19] Regulation 2016/679, art 85, 2016 O.J. (L 119) 1 (EU)
[20] Digital Personal Data Protection Act, 2023, §2(f) (India)
[21] Digital Personal Data Protection Act, 2023, §8(1)(j) (India)
[22] Digital Personal Data Protection Act, 2023, §17(1)(c) (India)
[23] Digital Personal Data Protection Act, 2023, §17(5) (India)

ambiguity. If these changes are implemented, the DPDP Act can achieve a balanced framework that protects individual privacy without stifling democratic accountability or journalistic freedom. The DPDP Act was envisioned as a milestone in the protection of individual autonomy in the digital age. Yet, if implemented in its present form, it risks being remembered as a law that enabled legal silencing through privacy rhetoric. While privacy is a fundamental right, so is the freedom of speech and expression. A democracy does not have to choose between the two; it must legislate in a manner that enables both. The path forward lies not in privileging privacy over transparency, but in harmonizing the two through intelligent legislative craftsmanship rooted in constitutional values. As the DPDP Rules of 2025[24] remain conspicuously silent, the time to legislate with clarity and courage is now.

[24] Ministry of Electronics and Information Technology, Draft Rules under the Digital Personal Data Protection Act, 2023 (Issued on Jan. 25, 2025) (India)