Social Media Monitoring by State Police under the Digital Personal Data Protection Act, 2023

Uma Shanmugab Priyaa, M[1], Laxmi Priya M[2]
[1,2] *Assistant Professor, Department of Legal Studies, School of Law, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai*

***Abstract*—This paper examines the monitoring of social media by State police in India with reference to the Digital Personal Data Protection Act, 2023. The practice is now routine, but no statute expressly authorises or regulates it. The DPDP Act, India's first general data protection law, was expected to fill some of that space. It does so only to a limited extent. Data that a person has herself made public falls outside the Act, processing for the prevention and investigation of offences is largely exempt from it, and the Central Government may exempt an instrumentality of the State from it altogether. Against that background, the paper considers the constitutional standard of proportionality, the statutory powers on which police presently rely, and the gaps in oversight and retention that result. It concludes with observations on reform.**

***Index Terms*—Digital Personal Data Protection Act; Social media monitoring; Police surveillance; Proportionality; Section 17 exemptions.**

I. INTRODUCTION

In *K.S. Puttaswamy v. Union of India*, the Supreme Court held that privacy is a fundamental right, and that any intrusion by the State must rest on law, pursue a legitimate aim and be proportionate to that aim (*K.S. Puttaswamy v. Union of India*, 2017). The Digital Personal Data Protection Act, 2023 received assent on 11 August 2023, and its Rules were notified on 13 November 2025. The substantive provisions, however, commence only in May 2027 (Digital Personal Data Protection Act, 2023; MeitY, 2025; S&R Associates, 2025).

Police in India now monitor social media to anticipate disturbances to public order, to identify offenders and to respond to misinformation. The methods range from the reading of public posts to commercial software that scrapes, geolocates and links accounts across platforms. The practice nonetheless rests on no dedicated statute. This paper considers what legal authority presently supports it, how far the DPDP Act will regulate it, and whether Indian law supplies the safeguards that the constitutional standard requires. The law is stated as at 24 November 2026.

II. THE LEGAL FRAMEWORK

The Court has since refined the standard set in *Puttaswamy*. In the Aadhaar judgment, the majority asked whether a measure pursues a legitimate goal, whether it is rationally connected to that goal, whether a less intrusive measure would serve equally well, and whether it strikes a proper balance between the right and the public interest (*K.S. Puttaswamy v. Union of India*, 2019).

Proportionality is not the only constitutional constraint, since the monitoring of public speech also engages the freedom of expression (Constitution of India, 1950, art. 19(1)(a)). In *Anuradha Bhasin v. Union of India*, the Court required orders restricting expression to be reasoned, published and open to review (*Anuradha Bhasin v. Union of India*, 2020). In *Shreya Singhal v. Union of India*, it upheld the blocking power in Section 69A of the Information Technology Act, 2000 largely because of the procedural safeguards attached to it (*Shreya Singhal v. Union of India*, 2015). The Court had earlier required a written order by a senior official, and review by a committee, before a telephone could be tapped (*People's Union for Civil Liberties v. Union of India*, 1997). In this line of cases, procedure forms part of constitutionality itself.

It may be argued that a person who posts publicly has no reasonable expectation of privacy in what she posts. The concern, however, lies less in the reading of a

single post than in aggregation, where accounts, locations and associations are linked into a profile of the individual. It is useful, therefore, to distinguish three activities: the reading of a public post in response to a particular complaint, the monitoring of public discourse by keyword or sentiment, and the sustained profiling of identified individuals. Each is more intrusive than the last, and each calls for a correspondingly stronger justification.

The Supreme Court has remarked on this risk before. In 2018, hearing a challenge to a proposed Social Media Communication Hub, the Court observed that such monitoring would be akin to creating a "surveillance state"; the Union withdrew its tender, and the petition was disposed of without a reasoned judgment (LiveLaw, 2018).

No Indian statute expressly authorises police to monitor public social media content. Section 23 of the Police Act, 1861 places a general duty on police to collect intelligence, but says nothing about method, retention or oversight (Police Act, 1861, S.23). Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023 permits the production of electronic records, but only in a particular investigation (Bharatiya Nagarik Suraksha Sanhita, 2023, S.94). Section 69 of the IT Act governs directed interception, and Section 69A governs blocking (Information Technology Act, 2000, Ss.69, 69A). Section 79(3)(b), read with Rule 3(1)(d) of the Intermediary Rules, supports takedown notices to platforms (Information Technology Act, 2000, S.79(3)(b); Information Technology [Intermediary Guidelines] Rules, 2021, r. 3(1)(d)).

The Karnataka High Court has upheld the Sahyog portal through which ministries and police issue such notices (*X Corp v. Union of India*, 2025), and an appeal against that decision has been admitted (LiveLaw, 2026). It has been argued that this parallel route bypasses the safeguards of Section 69A on which *Shreya Singhal* relied (The Leaflet, n.d.). None of these provisions, however, describes the systematic monitoring of public content.

The legality limb of the *Puttaswamy* test is therefore difficult to satisfy, since executive instructions are unlikely to be treated as law for this purpose. The question is further complicated by the division of legislative power. Police and public order are State subjects (Constitution of India, 1950, Seventh Schedule, List II, entries 1 and 2), while the IT Act is a Union statute, and no single legislature is therefore responsible for the safeguards.

III. THE DPDP ACT AND ITS LIMITS

Police who determine the purpose and means of processing personal data are data fiduciaries under the Act (Digital Personal Data Protection Act, 2023, S.2(i)). The Act nevertheless removes much of their activity from its scope, in three ways.

First, Section 3(c)(ii) provides that the Act does not apply to personal data made publicly available by the data principal herself, and the statutory illustration is of a person who blogs her views on social media (Digital Personal Data Protection Act, 2023, S.3(c)(ii)). Police reading public posts are therefore outside the Act altogether. This is a narrower position than that of the General Data Protection Regulation, which continues to apply to data that a person has made public (General Data Protection Regulation, 2016; J. Sagar Associates, 2024). It has also been observed that the exclusion sits uneasily with official statements that the scraping of public data requires compliance (IAPP, n.d.). The exclusion does not, on its terms, extend to data posted about a person by someone else, nor does it obviously extend to the profiles and inferences that police derive from public data.

Second, Section 17(1)(c) disapplies most of Chapter II, the whole of Chapter III and Section 16 where personal data is processed in the interest of the prevention, detection, investigation or prosecution of any offence (Digital Personal Data Protection Act, 2023, S.17(1)(c)). The exemption requires no notification, no showing of necessity and no designated competent authority (Tech Policy Press, n.d.). Since prevention precedes any offence, it is capable of covering general monitoring where there is no suspect at all. Only the general duty of compliance, and the duty to maintain security safeguards under Section 8(5), survive (Digital Personal Data Protection Act, 2023, S.8(5)), together with the safeguards in Rule 6 such as restricted access and the keeping of logs (MeitY, 2025, r. 6; NUALS Law Journal, 2026).

Third, Section 17(2)(a) permits the Central Government to exempt any instrumentality of the State from the entire Act, on grounds that include the maintenance of public order (Digital Personal Data Protection Act, 2023, S.17(2)(a)). The Act sets no

criteria, duration or review for such a notification, and the only procedural provision is Rule 23, which specifies who may call for information (ELP, 2026; MeitY, 2025, r. 23). A Central notification could thus remove State police from the Act entirely. A petition challenging Sections 17(1)(c) and 17(2), among other provisions, was reported to have been filed in the Supreme Court in February 2026 (Tech Policy Press, n.d.).

Three gaps follow from this position. The first concerns oversight. Interception requires a written direction and review by a committee, but the monitoring of public content requires neither. The Data Protection Board is appointed, and may be removed, by the Central Government, which has raised doubts about its independence (ELP, 2026; Digital Personal Data Protection Act, 2023, Ss.19, 21). Since Section 17(1)(c) also dispenses with notice, a person whose data has been processed may never learn of it, and so cannot complain (NUALS Law Journal, 2026).

The second concerns retention. The duty to erase data is disapplied for offence-related processing, and nothing limits how long police may keep data gathered from public sources. The Rules, moreover, require certain fiduciaries to retain personal data for at least one year for purposes that include the security of the State (MeitY, 2025, Seventh Schedule; Rana et al., 2025).

The third concerns misinformation. Falsity is not in itself a ground of restriction (Constitution of India, 1950, art. 19(2)), and *Shreya Singhal* distinguished the discussion and advocacy of ideas from incitement, protecting the former (*Shreya Singhal v. Union of India*, 2015). Monitoring for misinformation is legitimate only where it is tied to a listed ground such as public order. Because monitoring frequently leads to takedown requests, a gap in the law on monitoring becomes, in practice, a gap in the protection of speech.

The European approach is different. The Law Enforcement Directive and Part 3 of the UK Data Protection Act 2018 regulate police processing through a separate regime confined to competent authorities, which retains the requirements of necessity, storage limitation, logging and independent supervision (Directive (EU) 2016/680, 2016; Data Protection Act 2018, pt. 3). The European Court of Human Rights has also required safeguards at every stage of bulk interception, including independent authorisation (*Big Brother Watch v. United Kingdom*, 2021). Policing is thus regulated differently there, rather than left outside the law.

IV. CONCLUSION

In light of these gaps, several measures may be suggested. A statute defining the digital-monitoring powers of police, their purposes and their limits would address the requirement of legality. Authorisation could follow the three levels of intrusiveness identified above, with logging for the reading of posts in a particular case, written authorisation by a senior officer for a fixed period for keyword monitoring, and prior independent approval before identified individuals are profiled. Section 17(1)(c) could be confined to competent authorities and made subject to necessity, and notifications under Section 17(2)(a) could be required to be reasoned, time-limited and open to review.

Data collected from public sources could be deleted when an inquiry closes without charge, and aggregate annual reporting, with delayed notice to the persons monitored, would supply a measure of transparency. Concerns about operational secrecy need not prevent these measures, since the interception regime already shows that authorisation can be confidential and yet independent.

The DPDP Act is a significant step in Indian data protection law, but it does little to regulate the monitoring of social media by police. Most such monitoring falls outside the Act, either because the data is public or because the processing is exempt. What remains is the constitutional standard of proportionality, and in the absence of a law defining the power, even its first requirement is uncertain. Since the substantive provisions commence only in May 2027, and the challenge to Section 17 remains pending, these questions are still open. The concern is that a power exercised daily continues to rest on no law that names it.

REFERENCES

[1] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

[2] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, Acts of Parliament (India).

[3] Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14 and 24960/15 (Eur. Ct. H.R. Grand Chamber, 25 May 2021).
[4] Constitution of India, 1950.
[5] Data Protection Act 2018, c. 12 (UK).
[6] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India).
[7] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, 2016 O.J. (L 119) 89.
[8] ELP. (2026, July). Government exemptions and the balance between privacy and State interests. https://elplaw.in/wp-content/uploads/2026/07/Government-Exemptions-and-the-Balance-between-Privacy-and-State-Interests.pdf
[9] IAPP. (n.d.). Scraping public data in India: Innovation enabler or privacy threat? https://iapp.org/news/a/scraping-public-data-in-india-innovation-enabler-or-privacy-threat-
[10] Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament (India).
[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[12] J. Sagar Associates. (2024). KM JSA DPDPA compendium 2024. https://www.jsalaw.com/wp-content/uploads/2025/03/KM-JSA-DPDPA-Compendium-2024.pdf
[13] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
[14] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (India).
[15] LiveLaw. (2018, August 3). Plan to set up hub for monitoring social media dropped: Centre to SC. https://www.livelaw.in/plan-to-set-up-social-media-hub-for-monitoring-social-media-dropped-centre-to-sc-hearing-on-plea-against-it-closed/
[16] LiveLaw. (2026, March 10). Karnataka High Court issues notice to Centre on X Corp's appeal against Sahyog portal. https://www.livelaw.in/high-court/karnataka-high-court/karnataka-high-court-x-corp-challenges-it-act-framework-525827
[17] Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E), 13 November 2025). Government of India.
[18] NUALS Law Journal. (2026, March 26). When the State forgets to forget: Tiered exemptions under the DPDPA. https://nualslawjournal.com/2026/03/26/when-the-state-forgets-to-forget-tiered-exemptions-under-the-dpdpa/
[19] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
[20] Police Act, 1861, No. 5 of 1861 (India).
[21] Rana, V., Gandhi, A., & Chandgothia, P. (2025, November 14). MeitY notifies final Digital Personal Data Protection Rules 2025. S.S. Rana & Co. https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/
[22] 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.
[23] S&R Associates. (2025, November 24). India's Digital Personal Data Protection regime takes effect. https://www.snrlaw.in/indias-digital-personal-data-protection-regime-takes-effect/
[24] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[25] Tech Policy Press. (n.d.). India's GDPR-inspired privacy law leaves State power unchecked. https://techpolicy.press/indias-gdprinspired-privacy-law-leaves-state-power-unchecked
[26] The Leaflet. (n.d.). An exhaustive takedown of Karnataka HC's decision upholding Sahyog portal in X Corp v. Union of India. https://theleaflet.in/digital-rights/law-and-technology/an-exhaustive-takedown-of-karnataka-hcs-decision-upholding-sahyog-portal-in-x-corp-v-union-of-india
[27] X Corp v. Union of India, W.P. No. 7405 of 2025 (Kar. HC, 24 September 2025) (India).