

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Fifteen Years On: Revisiting India's Surveillance Safeguards from the IT Act to Puttaswamy, Pegasus, and the DPDP Act

VIBODH SINGH* AND NRIPANGANA DEKA**

ABSTRACT

In 2010, critiques of India's online surveillance regime rested on unstable doctrinal ground: privacy was, at best, a contested emanation of Article 21, and the procedural safeguards attached to interception under Section 69 of the Information Technology Act, 2000 existed without any independent authorisation requirement or a companion statute governing how gathered data could be processed. This article asks whether two intervening developments, the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India and the enactment of the Digital Personal Data Protection Act, 2023, have actually corrected the specific structural defect that animated the earlier critique, namely the absence of any check on the executive's own decision to intercept, prior to interception taking place. Tracing the doctrinal arc from Puttaswamy's proportionality standard through the Pegasus spyware litigation to the DPDP Act's exemption for state processing, this article argues that the constitutional and statutory landscape has been transformed while the operative architecture of Section 69 itself, an executive order followed only by a post-facto, non-judicial review committee, has remained essentially unchanged since 2009. Drawing a comparison with the judicial pre-authorisation, or "double lock", mechanism under the United Kingdom's Investigatory Powers Act, 2016, including its own recent narrowing, the article proposes a calibrated form of prior judicial authorisation for Section 69 interception orders as the specific reform needed to close the gap between India's proportionality doctrine and its surveillance practice.

Keywords: *Right to privacy, surveillance, Information Technology Act, Section 69, Puttaswamy, proportionality, Pegasus, Digital Personal Data Protection Act 2023, judicial pre-authorisation*

I. INTRODUCTION

Writing in 2010, commentators examining the newly amended Information Technology Act, 2000 ("IT Act") identified a structural defect running through India's surveillance law: procedural safeguards attached to interception existed on paper, but no independent authority

* Author is a Student at National Law Institute University, Bhopal, Madhya Pradesh, India.

** Author is a Student at National Law Institute University, Bhopal, Madhya Pradesh, India.

stood between the executive official who wished to intercept a communication and the decision to do so.¹ The right invoked to challenge this arrangement, privacy, was itself doctrinally uncertain: it rested on a line of post-*Gobind* precedent reading privacy into Article 21 of the Constitution, but had never been squarely tested against the two Supreme Court decisions, *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh*, that were widely read as denying any constitutional right to privacy at all.²

Fifteen years on, three developments have transformed this landscape. First, in *Justice K.S. Puttaswamy v. Union of India*, a nine-judge bench of the Supreme Court unanimously held that privacy is intrinsic to Article 21, overruling *M.P. Sharma* and *Kharak Singh* to the extent that they had held otherwise, and articulating a proportionality standard against which any state intrusion must be tested.³ Second, revelations that the Pegasus spyware may have been used against Indian journalists, politicians, and activists led the Supreme Court, in *Manohar Lal Sharma v. Union of India*, to appoint an independent technical committee and to confront, directly, the adequacy of India's surveillance oversight framework.⁴ Third, Parliament enacted the Digital Personal Data Protection Act, 2023 ("DPDP Act"), India's first comprehensive data protection statute, addressing a regulatory vacuum that had no equivalent in 2010.

This article asks a narrow but consequential question: have these three developments corrected the specific defect identified fifteen years ago, the absence of any check on the executive's own decision to intercept, prior to interception taking place? It argues that they have not, and that the gap between India's constitutional proportionality doctrine and its operative surveillance architecture remains, in this one specific respect, as wide as it was in 2010. Part II recalls the architecture of Section 69 as it was designed, and remains. Part III traces how *Puttaswamy* reconstructed privacy as a fundamental right subject to a proportionality standard. Part IV examines the Pegasus litigation as a live, and largely unsuccessful, test of that standard against actual surveillance practice. Part V considers why the DPDP Act, despite finally supplying a data protection statute, does not fill this particular gap. Part VI draws a comparison with the judicial pre-authorisation model used in the United Kingdom, including that model's own recent erosion. Part VII proposes a specific reform, and Part VIII concludes.

¹ See generally the procedural critique of § 69 of the Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), and of rule 419-A of the Indian Telegraph Rules, 1951, as representative of the scholarship of that period.

² *M.P. Sharma v. Satish Chandra*, 1954 SCR 1077 (India); *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).

³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

⁴ *Manohar Lal Sharma v. Union of India*, 2021 SCC OnLine SC 985 (India) (order dated Oct. 27, 2021).

II. THE ARCHITECTURE THAT HAS NOT CHANGED: SECTION 69 AND THE REVIEW COMMITTEE MODEL

Section 69 of the IT Act empowers the Central or a State Government to direct the interception, monitoring, or decryption of information through a computer resource where satisfied that it is necessary or expedient in the interests of the sovereignty or integrity of India, the defence of India, the security of the State, friendly relations with foreign States, or public order, or for preventing incitement to the commission of a cognizable offence relating to those grounds, or for the investigation of any offence.⁵ The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 govern the exercise of this power, and are closely modelled on Rule 419-A of the Indian Telegraph Rules, 1951, itself framed in response to the Supreme Court's directions in *People's Union for Civil Liberties v. Union of India*.⁶

The defining feature of this architecture, then and now, is that authorisation is entirely internal to the executive. An order is issued by the Union Home Secretary or a State-level equivalent, and reviewed, after the fact, by a Review Committee chaired by the Cabinet Secretary at the Union level or the Chief Secretary at the state level, a committee composed exclusively of serving bureaucrats from within the same executive branch that issued the order.⁷ No judge, and no person external to the executive, participates in the decision to intercept before it takes effect. The Supreme Court has held that non-compliance with these procedural safeguards does not, without more, render intercepted material inadmissible in evidence, a holding that further reduces the practical cost of procedural laxity.⁸ This is the precise structure that pre-2010 critiques identified as defective: safeguards that depend entirely on the same institution's willingness to police itself, with no independent check operating before the intrusion occurs.

It is worth recalling why this architecture took the shape it did. The Supreme Court's own directions in *People's Union for Civil Liberties* arose in response to a Central Bureau of Investigation study that had documented widespread, unauthorised telephone tapping of political figures, and the Court's remedy was procedural rather than institutional: it required

⁵ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 69(1).

⁶ Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India); *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (India).

⁷ Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 22 (India) (review of directions by the Review Committee, which is the committee constituted under rule 419-A of the Indian Telegraph Rules, 1951); Indian Telegraph Rules, 1951, r. 419-A (India) (constitution and composition of the Review Committee at the Central and State levels).

⁸ *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600, AIR 2005 SC 3820 (India) (discussing the parallel position under the Indian Telegraph Act, 1885).

documentation, a limit of two months on any single order, renewable in total to no more than six months, and review by a committee, but it did not require prior approval by any judge before an order could take effect.⁹ That choice was defensible in 1997, when telephone interception was a comparatively narrow and technically cumbersome exercise. Its transplantation, largely unaltered, into a 2009 framework governing interception of digital communications, where the volume, granularity, and retrospective searchability of intercepted material is incomparably greater, is the specific continuity this article treats as significant. The safeguards were designed for a different technological environment and have not been redesigned for the one in which they now operate.

III. *PUTTASWAMY*'S CONSTITUTIONAL RECONSTRUCTION

Puttaswamy did not merely declare privacy a fundamental right; it supplied a standard against which state intrusions into that right must be measured. The lead opinion articulated a three-part inquiry: the intrusion must be backed by law (legality), must pursue a legitimate state aim, and must be proportionate to that aim.¹⁰ In his separate concurring opinion, Justice Kaul went further, treating the existence of procedural safeguards against the abuse of an intrusive power as a distinct, necessary element of any permissible measure, a formulation that later commentary has read together with the three-part test as a four-fold inquiry.¹¹ When the Court returned to the proportionality standard in the Aadhaar litigation the following year, Justice Chandrachud's dissenting opinion applied this four-fold version explicitly, scrutinising not only whether the Aadhaar scheme pursued a legitimate aim but whether adequate procedural safeguards accompanied its implementation.¹²

The doctrinal significance of this development for surveillance law is direct. If procedural safeguards against abuse are a constitutional requirement, and if those safeguards must be assessed for their actual adequacy rather than their mere existence on paper, then a review mechanism confined entirely to the executive that authorised the intrusion in the first place is squarely the kind of arrangement *Puttaswamy*'s fourth limb was designed to test. What *Puttaswamy* supplied, in other words, was the constitutional vocabulary for exactly the critique that administrative and procedural scholarship had already made of Section 69 in 2010. What it did not supply, because constitutional adjudication of this kind requires a live challenge, was an

⁹ *People's Union for Civil Liberties*, *supra* note 6, at [35] (directions summarised).

¹⁰ *Justice K.S. Puttaswamy*, *supra* note 3 (three-fold test of legality, legitimate state aim and proportionality, as articulated in the lead opinion).

¹¹ *Justice K.S. Puttaswamy*, *supra* note 3 (Kaul, J., concurring).

¹² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1, at [264] (India) (Chandrachud, J., dissenting).

occasion to apply that vocabulary to Section 69 itself. That occasion arrived, four years later, with Pegasus.

IV. THE LIVE TEST: PEGASUS AND THE LIMITS OF POST-FACTO REVIEW

In 2021, international reporting alleged that Pegasus, a spyware suite developed by the Israeli firm NSO Group, had been used to target the mobile devices of Indian journalists, opposition politicians, and civil society figures.¹³ When the Union government's affidavit before the Supreme Court neither confirmed nor denied the use of Pegasus by Indian agencies, citing national security, the Court found the affidavit insufficient and, in *Manohar Lal Sharma v. Union of India*, appointed an independent Technical Committee, overseen by a retired judge of the Court, to investigate the allegations and to make recommendations on strengthening India's surveillance law.¹⁴

The Committee submitted its report in July 2022. It found no conclusive evidence of Pegasus on the small sample of devices it was able to examine, while noting that other spyware or malware could not be ruled out, and it recorded that the Union government had declined to cooperate meaningfully with its inquiry.¹⁵ Critically for the argument advanced here, the case exposed the practical consequence of an interception regime with no independent authorisation step: because no external body had ever needed to approve, or even know of, a given interception before it occurred, there was no contemporaneous record capable of confirming or disproving the allegations years later. The Review Committee mechanism under the 2009 Rules, being confined to the executive and operating without any public accountability, generated no evidentiary trail that the Technical Committee, or the Court, could examine. The Supreme Court's own frustration with the state of the record, and its emphasis on the pressing need to reform surveillance law to align with constitutional principles, reflects a direct, if implicit, application of *Puttaswamy*'s fourth limb to the very regime that scholarship had flagged as deficient over a decade earlier.¹⁶ Yet the Pegasus litigation, for all its significance, did not result in any amendment to Section 69 or the 2009 Rules. The architecture described in Part II remains exactly as it was before the case was filed.

¹³ See the reporting collated in the Supreme Court's own order, *Manohar Lal Sharma*, *supra* note 4.

¹⁴ *Manohar Lal Sharma*, *supra* note 4.

¹⁵ *Manohar Lal Sharma v. Union of India*, 2022 SCC OnLine SC 1085 (India) (order dated Aug. 25, 2022, recording that malware was found in five of the twenty-nine devices examined, that there was no conclusive evidence of Pegasus, and that the Union Government had not cooperated with the Technical Committee).

¹⁶ See *Manohar Lal Sharma*, *supra* note 15; *Manohar Lal Sharma*, *supra* note 4 (terms of reference of the Technical Committee, which included making recommendations on the enactment or amendment of the law governing surveillance).

V. THE DPDP ACT, 2023: A NEW STATUTE, THE SAME GAP

The DPDP Act finally gives India a general data protection statute, addressing the absence that earlier scholarship identified as a second structural defect, the lack of any rules governing how information, once gathered, is processed, retained, or secured.¹⁷ For private data fiduciaries, the Act will impose consent, purpose-limitation, and data-minimisation obligations enforceable by a new Data Protection Board of India once Sections 3 to 17 commence. But Section 17 of the Act allows the Central Government to exempt, by notification, any instrumentality of the State from the whole of the Act on grounds including the security of the State and public order, without requiring that exemption to be time-bound, judicially reviewed, or accompanied by recorded reasons specific to the processing in question.¹⁸

For present purposes, the significance of Section 17 is narrower than a full assessment of its constitutionality, which is not this article's focus. It is simply this: the one statute that could, in principle, have supplied the independent, external check that Section 69 has always lacked, by regulating what a government agency may do with intercepted data and by whom that processing is overseen, expressly declines to extend that check to state surveillance activity. The DPDP Act closes the information-processing gap that existed in 2010 for the private sector, and for most ordinary government functions, while leaving the specific defect this article is concerned with, the absence of any independent check on the decision to intercept, untouched. Reform of the exemption provision, whatever its merits, would not by itself supply prior authorisation for an interception order; it would, at most, regulate what happens to data after interception has already occurred. The gap identified in Part II therefore survives the DPDP Act intact, and requires a different kind of reform, directed at Section 69 itself, to which this article now turns via a comparative benchmark.

VI. A COMPARATIVE BENCHMARK: THE UK'S DOUBLE LOCK, AND ITS OWN EROSION

The United Kingdom's Investigatory Powers Act, 2016 offers the clearest comparative illustration of what an independent, prior check on interception can look like. Under the Act's "double lock" mechanism, an interception warrant issued by the Secretary of State cannot take

¹⁷ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), chs. II-III. The Act received assent on August 11, 2023, but its substantive obligations, §§ 3 to 17 among them, were brought into force only by the staggered commencement notified alongside the Digital Personal Data Protection Rules, 2025 on November 13, 2025, and take effect eighteen months from that date.

¹⁸ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), § 17(2)(a). For a detailed doctrinal examination of this specific provision against the *Puttaswamy* proportionality standard, see the existing literature on State exemptions under § 17(2)(a), which this article does not seek to duplicate.

effect until it is separately approved by an independent Judicial Commissioner, a serving or retired senior judge who reviews the necessity and proportionality of the warrant before, not after, interception begins.¹⁹ The mechanism allows for urgent warrants to proceed without prior approval in narrow circumstances, subject to Judicial Commissioner review within three working days, preserving operational flexibility without abandoning independent oversight altogether.²⁰

This model is not presented here as beyond criticism, nor as static. Reforms enacted in 2024 narrowed the scope of the double lock for certain categories of low-impact modifications to existing warrants, permitting some changes to proceed on Secretary of State authorisation alone, a development that has drawn criticism from civil liberties observers as an erosion of the very safeguard the 2016 Act was designed to entrench.²¹ This recent history is itself instructive: even a judicial pre-authorisation model, once established, faces continuing pressure toward executive convenience, and any reform proposed for India should anticipate and resist that pressure by design rather than treating a single legislative fix as self-sustaining.

VII. TOWARD JUDICIAL PRE-AUTHORISATION FOR SECTION 69

The reform this article proposes is narrower than a wholesale rewriting of India's surveillance law: a calibrated requirement of prior judicial approval for interception orders issued under Section 69, modelled on, but adapted from, the UK's double lock. Three design features would matter most.

First, approval should rest with a small panel of sitting High Court judges, nominated for this specific function on the recommendation of the Chief Justice of India, rather than with the existing Review Committee. This would supply the external, judicial character that *Puttaswamy*'s fourth limb contemplates, while avoiding the practical burden of routing every application through the Supreme Court itself.

Second, the standard applied by the panel should mirror the UK Judicial Commissioner's role: a review of whether the executive's own assessment of necessity and proportionality was one

¹⁹ Investigatory Powers Act 2016, c. 25, § 23 (UK) (approval of warrants by Judicial Commissioners); INVESTIGATORY POWERS COMM'R'S OFFICE, *The Double Lock*, <https://www.ipco.org.uk/what-we-do/the-double-lock/> (last visited Sept. 2, 2026).

²⁰ Investigatory Powers Act 2016, c. 25, § 24 (UK) (approval of warrants issued in urgent cases, which cease to have effect unless approved by a Judicial Commissioner before the end of the third working day after the day of issue).

²¹ See Investigatory Powers (Amendment) Act 2024, c. 9 (UK), and the discussion of its narrowing of double-lock requirements for certain warrant modifications; see also CTR. FOR STRATEGIC & INT'L STUDIES, *A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers*, <https://www.csis.org/analysis/new-investigatory-powers-act-united-kingdom-enhances-government-surveillance-powers> (last visited Sept. 17, 2026).

reasonably open to it, rather than a full re-hearing of the underlying intelligence, preserving institutional competence while still requiring the executive to justify its request to an outside decision-maker before, not after, interception occurs.

Third, and drawing directly on the lesson of the 2024 UK amendments, any statutory exception for urgent cases should be narrowly drawn, time-limited, and subject to mandatory retrospective judicial review within a fixed short period, so that urgency cannot become a routine substitute for prior authorisation. A regime that begins with a robust prior check but permits its own erosion through an expanding urgency exception would recreate, over time, precisely the executive-only architecture this article has criticised.

This proposal does not require a new constitutional amendment. It requires only that Parliament amend Section 69 and the 2009 Rules to substitute judicial approval for the existing Review Committee's post-facto role, a change squarely within the space *Puttaswamy*'s proportionality standard already contemplates and the Pegasus litigation already showed to be necessary in practice.

A predictable objection is that judicial pre-authorisation will slow down time-sensitive intelligence operations, and that India's security environment differs materially from the United Kingdom's. Two responses answer this without abandoning the proposal. First, the urgent-warrant exception described above is designed precisely to answer this concern: it permits interception to begin immediately, subject only to a short, mandatory retrospective check, so that no operational capability is lost in the ordinary case. Second, the volume argument cuts the other way once the Pegasus experience is taken seriously. If the objection to prior judicial review is that it would be administratively burdensome given the scale of interception activity in India, that scale is itself part of the case for review, not against it, since a mechanism justified by its low administrative cost is difficult to reconcile with a proportionality standard that treats procedural safeguards as necessary regardless of volume. A panel model, staffed by several designated judges working in rotation rather than a single commissioner, is one practical way to reconcile independent review with the caseload such a mechanism would need to absorb.

VIII. CONCLUSION

Fifteen years separate the procedural critique this article began with and the constitutional and statutory landscape as it now stands. In that time, the Supreme Court has constitutionalised privacy and supplied a proportionality standard that expressly demands procedural safeguards against abuse; a live controversy over spyware use has tested that standard against actual surveillance practice and found the existing record wanting; and Parliament has finally enacted

a comprehensive data protection statute. Each of these developments is significant, and none of them should be understated. But the specific defect that motivated the earliest critiques of India's surveillance law, an interception power exercised by the executive and checked only by the same executive after the fact, has passed through all three developments essentially unchanged. *Puttaswamy* supplied the doctrinal standard without an occasion to apply it to Section 69 directly; *Pegasus* supplied the occasion without a legislative remedy; and the DPDP Act supplied a remedy for a different problem, information processing, while expressly declining to reach this one. Closing that gap does not require another decade of doctrinal development. It requires Parliament to do what the United Kingdom did in 2016, imperfect and now partially eroded as that model has proven to be: insert an independent, judicial check between the decision to intercept and the interception itself, before rather than after the fact. Until that single structural change is made, India's privacy jurisprudence and India's surveillance practice will continue to speak two different languages, however far the doctrine on one side has travelled since 2010.
