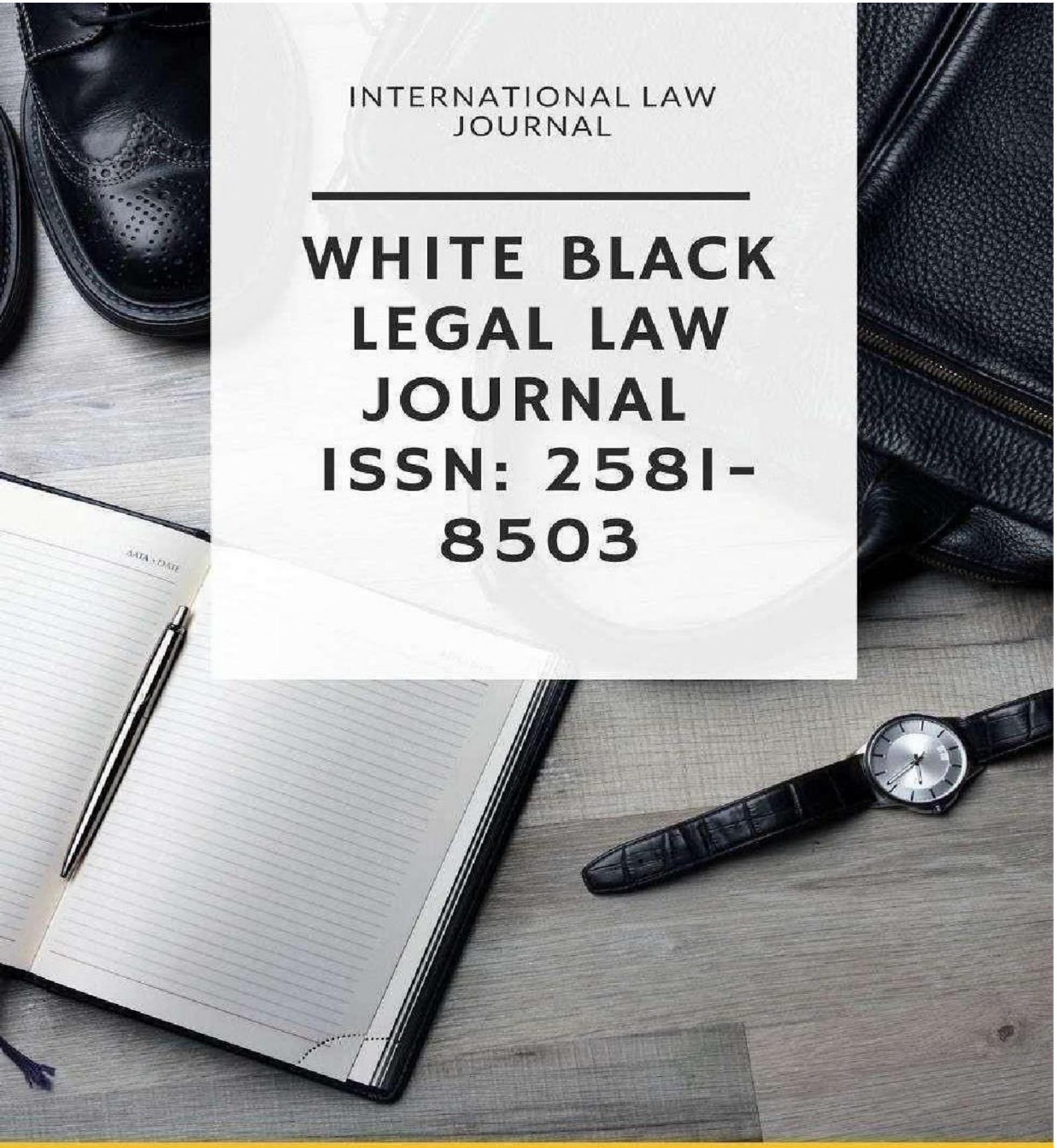


INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

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.

www.whiteblacklegal.co.in
Volume 3 Issue 9 | Aug 2026 ISSN: 2581-8503

CYBER CRIME, NATIONAL SECURITY AND CONSTITUTIONAL RIGHTS IN INDIA: BALANCING SECURITY WITH INDIVIDUAL LIBERTIES

AUTHORED BY - UMANG KAMBOJ

ABSTRACT

The proliferation of cybercrime and the corresponding expansion of State cyber-surveillance and interception capability have placed India's constitutional commitment to individual liberty under sustained and increasingly visible strain. This paper undertakes a critical, doctrinal analysis of the constitutional balance between national-security-oriented cyber powers and individual rights in India, examining the statutory architecture of interception, monitoring and content-blocking under Sections 69, 69A and 69B of the Information Technology Act, 2000, the Indian Telegraph Act, 1885, and the Digital Personal Data Protection Act, 2023's state-exemption provisions, against the constitutional benchmark the Supreme Court established in People's Union for Civil Liberties v. Union of India and, definitively, in Justice K.S. Puttaswamy v. Union of India's three-part proportionality test. The paper undertakes a detailed case study of the Pegasus spyware litigation before the Supreme Court, commenced in 2021 following allegations that Indian citizens, including journalists, activists, opposition politicians and constitutional functionaries, were targeted using Israeli-origin surveillance software, and traces the litigation's protracted and, this paper argues, doctrinally troubling trajectory through the constitution of a court-appointed Technical Committee under Justice R.V. Raveendran, the government's persistent non-cooperation with that Committee's inquiry, and the Supreme Court's April 2025 ruling declining to disclose the Committee's findings on national-security confidentiality grounds while remarking that the State's use of spyware was not, in principle, objectionable. The paper argues that this trajectory illustrates a structural weakness in India's constitutional balancing framework: the absence of independent, judicially or quasi-judicially administered ex-ante authorisation for interception, in contrast to comparator regimes such as the United Kingdom's Investigatory Powers Act, 2016, leaves the proportionality assessment Puttaswamy demands practically difficult to enforce once the State invokes national-security confidentiality, even before a court exercising its own supervisory jurisdiction. Employing doctrinal legal research methodology, the paper concludes with recommendations for statutory reform introducing independent authorisation and oversight

mechanisms, without which the constitutional balance between cybersecurity and individual liberty in India risks tilting structurally, and perhaps irreversibly, towards unaccountable executive discretion.

Keywords: *Cybercrime; national security; right to privacy; surveillance; Pegasus; proportionality; Article 21; India.*

1. INTRODUCTION

The digital transformation of Indian society has produced a corresponding transformation in the character and capability of both criminal threat and State response. Cybercrime, encompassing financial fraud, identity theft, critical-infrastructure attacks and cyber-terrorism, has grown in scale and sophistication to the point where the National Crime Records Bureau's Crime in India 2024 report documented a seventeen percent year-on-year surge in cybercrime registrations even as overall cognisable crime declined.[1] The State's response to this threat landscape has correspondingly expanded: Sections 69, 69A and 69B of the Information Technology Act, 2000 grant the government wide-ranging powers to intercept, monitor, decrypt and block digital communications and content on grounds including sovereignty, security, public order and crime prevention, while Section 70A establishes the National Critical Information Infrastructure Protection Centre and Section 70B empowers the Indian Computer Emergency Response Team to mandate cybersecurity incident reporting within six hours of detection.[2] This expansion of State cyber-security capability, however necessary its underlying security rationale, raises an enduring and increasingly urgent constitutional question: how does India's constitutional order ensure that powers justified by reference to national security remain proportionate to, and do not eviscerate, the individual liberties — privacy, free expression, due process — the Constitution guarantees under Part III.

This question has moved from abstract constitutional theory to concrete, high-stakes litigation through the Pegasus spyware controversy, which has occupied the Supreme Court's docket, in various procedural postures, since 2021. Following a July 2021 international investigative consortium report alleging that Indian ministers, politicians, activists, businesspersons and journalists were among individuals whose phone numbers appeared on a list of potential surveillance targets associated with the Israeli NSO Group's Pegasus spyware, a batch of writ

[1]National Crime Records Bureau, Crime in India 2024, Ministry of Home Affairs, Government of India (2026).
[2]Information Technology Act, 2000, ss. 69, 69A, 69B, 70A, 70B.

petitions sought judicial investigation into whether Indian government agencies had deployed the software and, if so, under what legal authority.[3] The Supreme Court's October 2021 order constituting an independent Technical Committee, supervised by former Supreme Court Justice R.V. Raveendran, to investigate these allegations represented a significant assertion of judicial oversight capacity in the surveillance context; yet the litigation's subsequent trajectory — marked by persistent governmental non-cooperation with the Committee's inquiry and the Supreme Court's own April 2025 decision to withhold the Committee's findings from public and even petitioner disclosure on national-security confidentiality grounds — illustrates, this paper argues, a structural difficulty in translating constitutional proportionality doctrine into practically enforceable oversight once national-security claims are invoked.[4]

This paper undertakes a critical, doctrinal examination of the constitutional balance between cyber-security-oriented State power and individual liberty in India, using the Pegasus litigation as a central case study through which to assess whether India's existing legal and institutional framework adequately operationalises the proportionality principle Puttaswamy established, or whether, as this paper contends, structural gaps in independent oversight leave that principle substantially aspirational in the national-security surveillance context specifically.

1.1 Statement of the Problem

India's constitutional framework recognises both the legitimacy of State action to protect national security and the fundamental character of individual privacy and liberty, and the Supreme Court has articulated a proportionality-based methodology, developed in PUCL and Puttaswamy, intended to reconcile these values. Yet the practical operation of this framework in the cyber-surveillance context, most starkly illustrated by the Pegasus litigation's protracted and inconclusive trajectory, raises the question whether existing statutory and institutional mechanisms provide meaningful, independently enforceable proportionality review, or whether they leave the balance substantially within unreviewed executive discretion once national-security claims are advanced.

1.2 Objectives of the Study

- To map the statutory architecture governing State cyber-surveillance, interception and content-blocking powers in India and their constitutional foundations.

[3]Manohar Lal Sharma v. Union of India, W.P.(Crl.) No. 314 of 2021, and connected matters.
[4]"Pegasus Spyware Probe #7: Technical Committee Granted More Time to Submit Final Report," Supreme Court Observer (2022); "Supreme Court's Pegasus Spyware Case: Key Legal Questions on Privacy, Surveillance, and Rule of Law," NeuroAmicus (2025).

- To critically analyse the doctrinal development of proportionality review in the surveillance context from PUCL through Puttaswamy.
- To undertake a detailed case study of the Pegasus spyware litigation as an illustration of the practical operation, and limitations, of judicial oversight of national-security-justified surveillance.
- To compare India's surveillance oversight framework with comparator regimes offering independent ex-ante authorisation mechanisms.
- To recommend legislative and institutional reforms strengthening the constitutional balance between cybersecurity and individual liberty in India.

1.3 Research Questions

- Does India's statutory framework for State cyber-surveillance and interception provide adequate procedural safeguards to satisfy the Puttaswamy proportionality test in practice, or only in principle?
- What does the Pegasus litigation's trajectory reveal about the practical limits of judicial oversight of national-security-justified surveillance, including the courts' own capacity to compel governmental transparency?
- How does India's executive-internal review model for surveillance authorisation compare to independent judicial or tribunal pre-authorisation models such as the UK's Investigatory Powers Act, and what does this comparison suggest for reform?
- What legislative and institutional reforms would strengthen the practical, and not merely doctrinal, protection of individual liberty against disproportionate national-security-justified cyber powers?

1.4 Research Methodology

This study adopts a doctrinal legal research methodology, involving critical analysis of the IT Act, the Telegraph Act, the DPDP Act, constitutional provisions, and judicial precedent, including the ongoing Pegasus litigation, supplemented by secondary literature, media reporting on the litigation's procedural history, and comparative reference to the UK's oversight model. The case-study method is used to ground the doctrinal proportionality analysis in a concrete, high-stakes example of its practical application.

1.5 Scope and Limitations

The paper is confined to the constitutional balance between State cyber-security powers and

individual liberty within India's domestic legal framework, with the Pegasus litigation serving as the principal case study. It does not undertake detailed technical analysis of spyware capability, nor comprehensive comparative analysis of foreign surveillance law beyond the UK reference point used for illustrative contrast. The Pegasus litigation remained procedurally unresolved as of August 2026, and the analysis reflects the publicly available record as understood at that date, given the confidentiality maintained around significant portions of the Technical Committee's findings.

2. LITERATURE REVIEW

2.1 The Statutory Foundations of Cyber-Surveillance Power

India's legal authority for State interception and surveillance derives principally from two statutes: the Indian Telegraph Act, 1885, whose Section 5(2) permits interception of messages in circumstances of public emergency or in the interest of public safety, and the Information Technology Act, 2000, whose Sections 69, 69A and 69B, introduced through the 2008 amendment, extend comparable powers specifically to digital communications and computer resources.[5] Section 69 empowers the Central or State Government to direct interception, monitoring or decryption of information transmitted through a computer resource on grounds including sovereignty, defence, State security, friendly relations with foreign States, public order, and prevention or investigation of offences; Section 69A empowers content-blocking on a similarly enumerated set of grounds; and Section 69B authorises monitoring and collection of traffic data for cybersecurity purposes, with contravention of Section 69B directions attracting imprisonment up to one year and fines up to one crore rupees.[6] These powers are elaborated through the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, which establish an internal executive review process involving a designated competent authority and periodic review by a Review Committee, but do not provide for independent judicial or quasi-judicial pre-authorisation of interception orders.[7]

2.2 PUCL v. Union of India: The Foundational Procedural Safeguards Case

The doctrinal starting point for judicial oversight of Indian surveillance power is People's

[5]Indian Telegraph Act, 1885, s. 5(2); Information Technology Act, 2000, ss. 69, 69A, 69B (as inserted by the Information Technology (Amendment) Act, 2008).
[6]"Navigating Digital Surveillance in India: Balancing Security and Privacy," The LawGist (2024).
[7]Mondaq, "State Surveillance and Privacy Rights: Legal Frameworks and Challenges in India" (2025).

Union for Civil Liberties v. Union of India, in which the Supreme Court, confronting the absence of any procedural safeguards in the Telegraph Act's then-unstructured Section 5(2) power, read a set of minimum procedural protections into the provision, including a requirement that interception orders be issued only by specified senior officials, be subject to periodic review by a Review Committee, and remain valid only for a limited, renewable period.[8] These PUCL safeguards were subsequently incorporated into the 2009 Interception Rules framework governing IT Act surveillance powers, representing the principal judicially mandated procedural constraint on India's surveillance apparatus prior to Puttaswamy's later constitutional elaboration.[9]

2.3 Puttaswamy and the Proportionality Standard

Justice K.S. Puttaswamy (Retd.) v. Union of India's recognition of privacy as a fundamental right under Article 21 supplied the constitutional foundation against which all subsequent State surveillance action must now be tested, articulating a three-part proportionality standard requiring the presence of a valid law, a legitimate State aim, and proportionality between the means employed and the aim pursued.[10] Contemporary commentary describes this test as the "grundnorm of Indian cyber law," observing that it is "the reason India could not simply legislate its way to a surveillance state," since every surveillance measure, data mandate, and content-blocking action must now, at least in principle, survive proportionality scrutiny.[11] Yet the same commentary, and the broader literature this paper surveys, observes that India continues to lack a dedicated statutory framework for bulk or programmatic surveillance comparable to the United Kingdom's Investigatory Powers Act, 2016, leaving a structural gap between the constitutional proportionality standard Puttaswamy demands and the statutory and institutional mechanisms available to enforce it in practice.[12]

2.4 The DPDP Act's State Exemptions

The Digital Personal Data Protection Act, 2023 introduces a further dimension to this analysis through Section 17's broad exemptions permitting government processing of personal data without consent for purposes including national security, sovereignty and integrity, public order, and law-enforcement, alongside Section 36's power (read with Rule 23 of the DPDP

[8]People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[9]LexOrbis, "Cybersecurity Laws and Regulations India 2025" (2025).
[10]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[11]"Cybersecurity Laws and Regulations in India – July 2026," Prashant Mali Cyber Law Blog (2026).
[12]Journalism University, "Strengthening India's Cybersecurity Framework: IT Laws and Rules" (2026).

Rules, 2025) enabling the government to call for information from data fiduciaries.[13] Analysis of these provisions observes that while such exemptions ensure operational flexibility for legitimate State functions, they have "triggered concerns over mass surveillance, lack of judicial oversight, and limited accountability," with the Data Protection Board's jurisdiction over complaints of surveillance-related misuse remaining unclear, and judicial review under Articles 32 and 226 remaining available only reactively, after an alleged violation has already occurred, rather than through built-in ex-ante procedural safeguards.[14] Comparative commentary observes that, unlike the UK's Investigatory Powers Act, the DPDP Act "lacks rigorous necessity and proportionality safeguards, raising entirely valid fears of unchecked mass surveillance, as painfully highlighted by controversies surrounding the deployment of Pegasus spyware."[15]

2.5 The Pegasus Litigation: Procedural History

The Pegasus litigation's procedural history, as documented by contemporaneous reporting, illustrates the practical difficulty of judicial oversight in this domain. Following the July 2021 allegations, the Supreme Court's October 2021 order constituted a Technical Committee, supervised by Justice R.V. Raveendran, directed to determine whether Pegasus had been used against Indian citizens, by whom, and under what legal authority.[16] The Committee's work was substantially hindered by the government's documented non-cooperation: the Supreme Court itself noted, upon reviewing the Committee's findings in 2022, that "the Government of India has not cooperated" with the inquiry, and the Committee's report concluded that five of twenty-nine examined mobile phones showed possible malware infection without conclusive attribution to Pegasus specifically, an outcome the Court attributed partly to this lack of governmental cooperation.[17] The litigation's most recent and, this paper argues, most doctrinally significant development occurred on 29 April 2025, when a bench comprising Justices Surya Kant and N. Kotiswar Singh ruled that the Technical Committee's report would not be made public, reasoning that any report touching upon "security and sovereignty" could not be disclosed, while remarking, in terms that attracted considerable public attention, that there was "nothing wrong" in principle with the country using spyware, and that the operative

[13]Digital Personal Data Protection Act, 2023, ss. 17, 36; DPDP Rules, 2025, r. 23.
[14]"Government Access to Data under the DPDP Act, 2023: Exemptions, Surveillance Concerns, and Safeguards," KSandK (2025).
[15]"Data Rights and Surveillance: A Global Perspective," Nitishastra Substack (2026).
[16]Manohar Lal Sharma v. Union of India, supra note 3; Supreme Court Observer, supra note 4.
[17]Deccan Herald, "Pegasus Snooping Case: Malware Found in 5 Phones but No Conclusive Proof That It Had Spyware, Says Supreme Court" (2022).

legal question was "against whom it is used."[18]

2.6 Critical Commentary on the Pegasus Litigation's Trajectory

Legal commentary on this trajectory has been notably critical of its implications for meaningful judicial oversight of national-security-justified surveillance. Analysis published shortly after the April 2025 ruling observes that the outcome leaves petitioners — including journalists and activists who submitted their own devices for examination — unable to learn the substantive findings concerning their own alleged surveillance, undermining the practical value of judicial review as an accountability mechanism even where, as here, the Court itself initiated and supervised the investigative process.[19] The same commentary situates the ruling against the Puttaswamy proportionality framework, observing that the constitutional requirement that State action be "just, fair, and reasonable" and satisfy proportionality review becomes practically difficult to police where the very findings necessary to assess proportionality are themselves withheld from disclosure on the same national-security grounds the underlying surveillance action was said to serve — a structural circularity this paper examines further in Part 3.[20]

2.7 Research Gap

Existing literature tends either to provide doctrinal commentary on India's surveillance statutory framework and the PUCL/Puttaswamy proportionality standard in the abstract, or to report on the Pegasus litigation's procedural developments without systematically analysing what that litigation reveals about the structural adequacy of India's constitutional balancing framework as a whole. This paper integrates both strands, using the Pegasus case study to ground a broader critical assessment of the security-liberty balance in India's cyber-security legal architecture.

3. ANALYSIS AND DISCUSSION

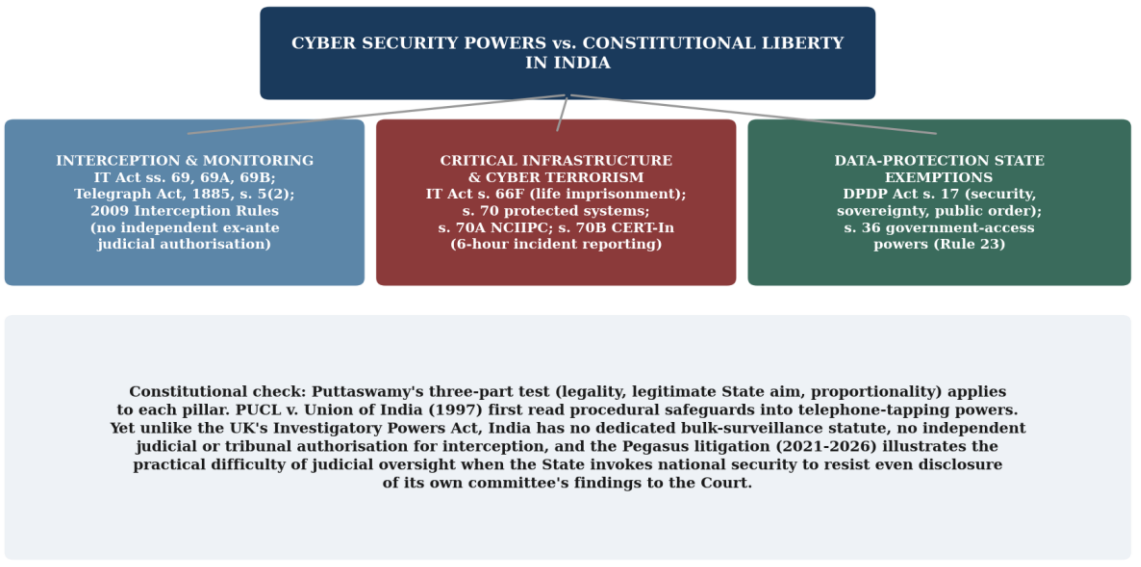
3.1 Mapping the Security-Liberty Legal Architecture

As illustrated in Figure 1, India's cyber-security legal architecture comprises three principal pillars bearing on the security-liberty balance: interception and monitoring powers under the

[18]Business Standard, "'Nothing Wrong in Country Using Spyware': Supreme Court on Pegasus Row" (2025); The Mooknayak, "'What's Wrong': Supreme Court Backs Spyware Use" (2025).
[19]NeuroAmicus, supra note 4.
[20]Id.

IT Act and Telegraph Act, critical-infrastructure and cyber-terrorism provisions under IT Act Sections 66F, 70, 70A and 70B, and the DPDP Act's state-exemption and government-access provisions. Each pillar is, in principle, subject to the Puttaswamy proportionality standard, yet each also exhibits the same structural feature this paper identifies as central to the Pegasus litigation's difficulties: procedural safeguards operate substantially through executive-internal review (a designated competent authority, an internal Review Committee) rather than through independent judicial or quasi-judicial ex-ante authorisation, leaving the practical enforcement of proportionality review dependent on the same executive branch whose action is under scrutiny.[21]

Figure 1: The Cybersecurity-Liberty Legal Architecture in India



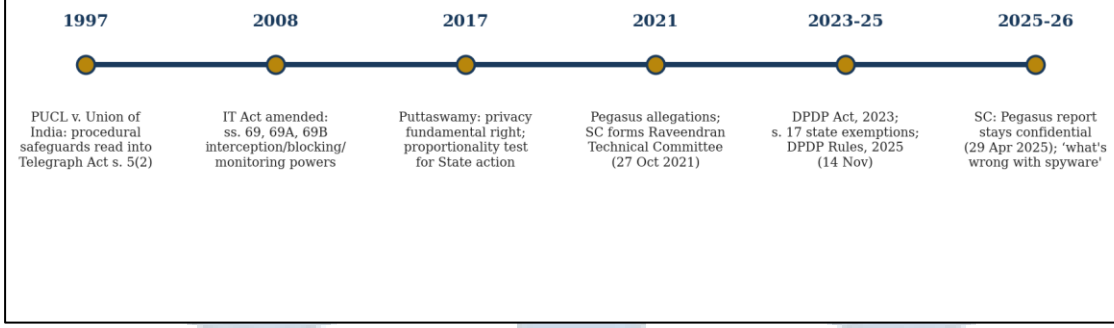
3.2 From PUCL to Puttaswamy: The Doctrinal Trajectory

As Figure 2 illustrates, the doctrinal trajectory governing India's surveillance-liberty balance spans nearly three decades, from PUCL's 1997 introduction of minimum procedural safeguards into an otherwise unstructured interception power, through the IT Act's 2008 extension of comparable powers to digital communications, to Puttaswamy's 2017 constitutional elevation of privacy and articulation of the proportionality test that now formally governs this entire domain.[22] This trajectory reflects genuine doctrinal development: each stage responded to a recognised gap in the preceding framework, and Puttaswamy in particular represents a considered, unanimous constitutional statement that State surveillance power, however

[21]Information Technology Act, 2000, ss. 69, 69A, 69B, 70A, 70B; DPDP Act, 2023, ss. 17, 36.
[22]PUCL, supra note 5; Puttaswamy, supra note 7.

legitimate its underlying security rationale, cannot escape proportionality scrutiny merely by invoking national security as its justification.[23] Yet, as the Pegasus case study examined in Part 3.3 demonstrates, the doctrinal sophistication of this trajectory has not been matched by a correspondingly robust set of institutional mechanisms capable of enforcing it in practice, particularly once national-security confidentiality claims are advanced not merely to justify the underlying surveillance but to resist disclosure of the very findings necessary to assess that justification's proportionality.

Figure 2: Evolution of Cyber-Security and Constitutional Liberty Jurisprudence in India, 1997–2026



3.3 Case Study: The Pegasus Litigation as a Proportionality Stress Test

The Pegasus litigation offers an unusually detailed, publicly documented illustration of how the Puttaswamy proportionality framework operates — or fails to operate — in a high-stakes national-security surveillance controversy. As illustrated in Figure 3, the proportionality test's fourth stage requires an assessment of whether the specific means employed (surveillance via sophisticated spyware capable of near-total access to a target's device) were proportionate to the legitimate aim pursued. This assessment is, by its nature, fact-intensive: it requires knowing who was targeted, on what basis, and pursuant to what legal authorisation. The Pegasus litigation's trajectory reveals that each of these factual predicates proved practically inaccessible to the very court charged with conducting the proportionality assessment. The government's documented non-cooperation with the Court's own Technical Committee meant the Committee itself could not conclusively determine whether Pegasus had been deployed, by whom, or under what authority — the foundational facts any proportionality analysis would

[23] Puttaswamy, supra note 7, at paras 310, 325.

require.[24] The Supreme Court's own subsequent decision to withhold even the Committee's eventual findings from public and petitioner disclosure compounds this difficulty: an accountability mechanism whose findings are inaccessible even to the parties whose own devices were examined provides, at most, an assurance that internal executive-judicial review occurred, without the transparency ordinarily understood as integral to meaningful proportionality accountability.[25]

The April 2025 bench's observation that there was "nothing wrong" in the country using spyware, with the operative question being "against whom it is used," is doctrinally significant in a further respect: it appears to accept, without extended proportionality analysis on the public record, that the mere existence of State spyware capability raises no independent constitutional concern, locating the entire constitutional inquiry instead at the point of specific deployment against specific individuals — precisely the factual question the litigation's own procedural history shows to be practically unascertainable given the government's non-cooperation and the Court's own confidentiality ruling.[26] This creates what this paper terms a proportionality accountability gap: a constitutional standard (proportionality) that formally applies but whose practical enforcement depends on factual transparency that the very national-security justification invoked to defend the underlying State action is simultaneously used to withhold.

3.4 Comparative Perspective: Independent Authorisation Models

Figure 4 presents an illustrative comparison between India's executive-internal review model and the independent authorisation framework established under the United Kingdom's Investigatory Powers Act, 2016, which requires most interception warrants to be approved not only by a Secretary of State but also by an independent Judicial Commissioner exercising a substantive "double-lock" review, and establishes a statutorily empowered Investigatory Powers Commissioner's Office to conduct ongoing, published oversight of surveillance activity.[27] This comparative contrast illuminates the structural gap this paper identifies in the Indian framework: whereas the UK model subjects surveillance authorisation to a check genuinely independent of the executive branch seeking to exercise the power, India's Review Committee under the 2009 Interception Rules is itself constituted from within the executive branch, providing internal procedural discipline but not the kind of independent, adversarially

[24]Deccan Herald, supra note 12.
[25]NeuroAmicus, supra note 4.
[26]Business Standard, supra note 13; The Mooknayak, supra note 13.
[27]Journalism University, supra note 9; Mondaq, supra note 6.

tested review capable of meaningfully constraining executive discretion in contested cases such as Pegasus.[28]

3.5 The DPDP Act's Compounding Effect

The DPDP Act's broad state exemptions under Section 17 and government-access powers under Section 36, examined in Part 2.4, compound rather than mitigate the structural gap this paper identifies. Where the IT Act's interception provisions at least nominally incorporate the PUCL-derived Review Committee safeguard, the DPDP Act's exemption framework does not clearly specify an equivalent internal review mechanism for government data-access requests justified by reference to national security, leaving this parallel and increasingly significant channel of State access to personal data with, on the current literature's account, even less institutional oversight structure than the comparatively more developed interception framework.

3.6 Toward a Structural Diagnosis

Read together, the doctrinal trajectory examined in Part 3.2 and the Pegasus case study examined in Part 3.3 support a structural diagnosis: India's constitutional framework for balancing cybersecurity and individual liberty suffers not from an absence of the relevant legal standard — Puttaswamy's proportionality test is doctrinally well-developed and widely invoked — but from an absence of the institutional mechanisms necessary to enforce that standard against a resistant executive branch in genuinely contested national-security cases. This diagnosis suggests that further doctrinal elaboration of the proportionality standard itself is unlikely, on its own, to resolve the accountability gap the Pegasus litigation exposes; what is required instead is institutional reform introducing a genuinely independent authorisation or oversight mechanism of the kind Part 3.4's comparative analysis identifies as absent from the current framework.

3.7 The Cybercrime Dimension: A Parallel Legitimacy Concern

It is worth noting, in concluding this analysis, that the same institutional gap this paper identifies in the national-security surveillance context carries implications for cybercrime investigation more broadly, even outside the specifically national-security-justified surveillance context Pegasus illustrates. Ordinary cybercrime investigation increasingly relies

[28]Mondaq, supra note 6.

on interception, device-monitoring and data-access powers exercised under the same statutory provisions examined in this Part, and the same absence of independent ex-ante authorisation that Part 3.3 identifies as problematic in the high-stakes Pegasus context applies, in principle, equally to routine cybercrime investigations, even though the latter typically attract far less public scrutiny. This suggests that the institutional reforms this paper recommends in Part 5 would strengthen constitutional accountability not merely in exceptional national-security controversies but across the much larger, day-to-day volume of cyber-investigative activity conducted under the same statutory authority, a consideration that should inform the scope and design of any future independent oversight mechanism.

Figure 3: The Puttaswamy Proportionality Test Applied to State Cyber-Surveillance

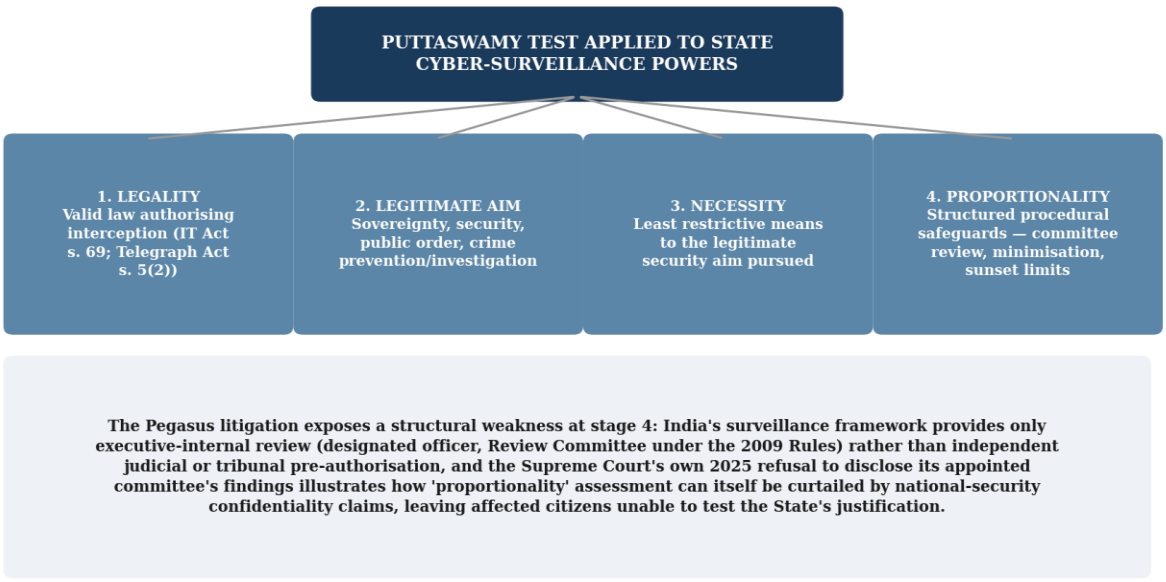
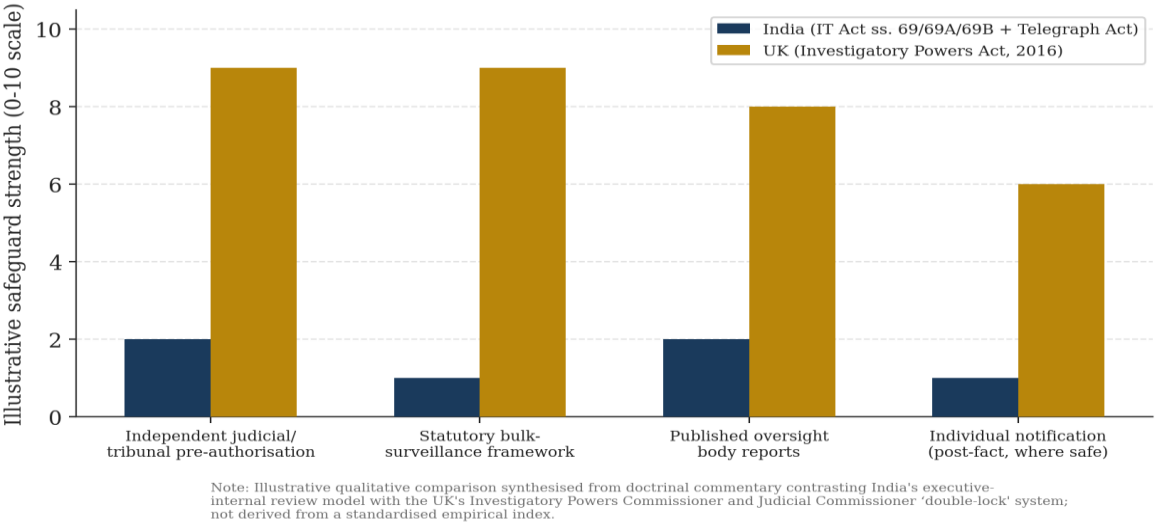


Figure 4: Illustrative Comparison of Surveillance Oversight Safeguards — India and the United Kingdom



3.8 Comparative Snapshot: Security-Liberty Safeguards in India and the UK

Table 1 summarises the principal structural differences between India's current framework and the UK's independent-authorisation model.

Safeguard	India (IT Act ss. 69/69A/69B + Telegraph Act)	United Kingdom (Investigatory Powers Act, 2016)
Pre-authorisation	Designated competent authority (executive)	Secretary of State + independent Judicial Commissioner (‘double-lock')
Ongoing oversight body	Internal Review Committee (executive-constituted)	Investigatory Powers Commissioner's Office (independent statutory body)
Published oversight reporting	Not routinely published	Annual public reports by the Commissioner
Bulk/programmatic surveillance statute	No dedicated statute; addressed through general IT Act/Telegraph Act powers	Dedicated statutory framework with distinct bulk-power safeguards
Individual notification (post-fact)	Not provided for	Limited notification mechanism in defined circumstances
Judicial recourse for affected individuals	Reactive, via Arts. 32/226, after alleged violation; Pegasus shows practical access difficulty	Investigatory Powers Tribunal with dedicated jurisdiction

Table 1: Comparative snapshot of security-liberty safeguards in India and the United Kingdom.

4. FINDINGS

- India's statutory framework for State cyber-surveillance, spanning the Telegraph Act, the IT Act, and now the DPDP Act, formally incorporates the PUCL-derived procedural safeguards and is, in principle, subject to the Puttaswamy proportionality standard, but relies substantially on executive-internal review mechanisms rather than independent judicial or quasi-judicial ex-ante authorisation.
- The Pegasus litigation's protracted and, on its public record, inconclusive trajectory illustrates a structural proportionality accountability gap: the factual transparency

necessary to assess whether specific surveillance action was proportionate to its stated national-security aim proved practically inaccessible even to the Supreme Court's own court-appointed Technical Committee, due to documented governmental non-cooperation.

- The Supreme Court's April 2025 decision to withhold the Technical Committee's findings from public and petitioner disclosure on national-security confidentiality grounds compounds this accountability gap, denying affected individuals — including journalists and activists who submitted their own devices for examination — access to findings concerning their own alleged surveillance.
- The bench's accompanying observation that there was "nothing wrong" in principle with State spyware use reflects an implicit acceptance of surveillance capability's legitimacy that was not, on the public record, accompanied by the kind of detailed proportionality analysis Puttaswamy's framework contemplates, given the confidentiality maintained around the underlying factual findings.
- Comparative analysis with the United Kingdom's Investigatory Powers Act reveals that India's framework lacks the independent Judicial Commissioner pre-authorisation, dedicated oversight body, and published reporting mechanisms that structure meaningful, institutionally enforced proportionality review in comparator jurisdictions.
- The DPDP Act's Section 17 state exemptions and Section 36 government-access powers compound this structural gap by extending State access to personal data through a parallel channel with even less clearly specified internal oversight than the comparatively more developed IT Act interception framework.
- The cumulative effect of these findings is that India's constitutional proportionality standard, while doctrinally well-developed, currently depends for its practical enforcement substantially on the same executive branch whose action is under scrutiny, a structural feature the Pegasus litigation's trajectory illustrates can produce a practically unenforceable, if formally applicable, constitutional safeguard in contested national-security cases.

5. RECOMMENDATIONS

5.1 Legislative Reforms

- Enact a dedicated surveillance and interception statute, distinct from the general-purpose IT Act and Telegraph Act provisions, establishing an independent judicial or quasi-

judicial pre-authorisation requirement for interception orders, modelled on the UK's Judicial Commissioner 'double-lock' system, at least for surveillance targeting journalists, activists, opposition politicians and other individuals whose surveillance raises heightened democratic-accountability concerns.

- Establish a statutorily empowered, genuinely independent oversight body, analogous to the UK's Investigatory Powers Commissioner's Office, tasked with ongoing review of surveillance activity and publication of periodic, appropriately redacted public reports on the scale and character of State interception activity.
- Amend the DPDP Act to specify a clearer internal and, ideally, independent oversight mechanism governing the exercise of Section 17 state exemptions and Section 36 government-access powers, addressing the current oversight gap this paper identifies in the data-protection-specific channel of State access to personal information.

5.2 Institutional Reforms

- Develop, potentially through Supreme Court rule-making or Law Commission recommendation, a structured protocol for future court-supervised technical investigations into surveillance allegations, addressing the government non-cooperation difficulty the Pegasus Technical Committee's own findings identified as a significant obstacle to its inquiry.
- Establish a mechanism, calibrated to protect genuinely sensitive national-security information while preserving meaningful individual accountability, for notifying individuals whose devices or communications were subject to court-ordered technical examination of the relevant findings concerning their own case specifically, even where broader systemic findings remain confidential.

5.3 Judicial Development

- Encourage future judicial engagement with national-security confidentiality claims in the surveillance context to articulate more explicit, reasoned criteria distinguishing information genuinely requiring confidentiality from information whose disclosure would serve accountability without compromising legitimate security interests, rather than treating national-security invocation as effectively dispositive of the disclosure question.
- Develop clearer appellate guidance on the practical content of Puttaswamy's proportionality test in the surveillance context specifically, addressing how courts should

proceed where, as in Pegasus, the factual predicate for proportionality assessment is itself contested or inaccessible due to non-cooperation or confidentiality claims.

5.4 Broader Reform: Toward Institutionally Enforceable Proportionality

- Recognise, as a guiding principle for future legislative and institutional development, that constitutional proportionality standards require not merely doctrinal articulation but institutional mechanisms capable of independent, adversarially tested enforcement against a potentially resistant executive branch, and that India's continued reliance on executive-internal review structures represents the primary obstacle to closing the accountability gap this paper identifies.

6. CONCLUSION

The constitutional balance between national-security-oriented cyber powers and individual liberty in India rests, in doctrinal terms, on a well-developed foundation: PUCL's procedural safeguards, subsequently incorporated into the IT Act's interception framework, and Puttaswamy's rigorous three-part proportionality test together articulate a constitutional standard genuinely capable, in principle, of constraining disproportionate State surveillance action. Yet this paper's detailed examination of the Pegasus spyware litigation demonstrates that doctrinal sophistication alone cannot guarantee practical constitutional protection where the institutional mechanisms necessary to enforce that doctrine remain substantially confined to executive-internal review. The litigation's protracted trajectory — documented governmental non-cooperation with the Supreme Court's own Technical Committee, and the Court's own subsequent decision to withhold the Committee's findings on national-security confidentiality grounds — reveals a structural proportionality accountability gap that no amount of further doctrinal refinement of the proportionality standard itself is likely to close. What India's constitutional order requires, this paper has argued, is not a new legal test but new institutional architecture: independent, judicially or quasi-judicially administered ex-ante authorisation for interception, a genuinely independent ongoing oversight body, and clearer, more principled limits on the use of national-security confidentiality claims to resist disclosure of findings necessary to assess proportionality after the fact. Absent such institutional reform, the constitutional balance between cybersecurity and individual liberty in India risks tilting, gradually but perhaps decisively, towards an executive discretion that formally acknowledges but practically evades the very proportionality constraints the Constitution, through

Puttaswamy, was understood to have definitively established.

REFERENCES

A. *Statutes and Regulatory Instruments*

1. *Information Technology Act, 2000 (Act No. 21 of 2000), ss. 66F, 69, 69A, 69B, 70, 70A, 70B.*
2. *Indian Telegraph Act, 1885, s. 5(2).*
3. *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.*
4. *Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 17, 36.*
5. *Digital Personal Data Protection Rules, 2025, r. 23.*
6. *Constitution of India, arts. 14, 19, 21, 32, 226.*
7. *Investigatory Powers Act, 2016 (United Kingdom).*

B. *Cases*

8. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*
9. *People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.*
10. *Manohar Lal Sharma v. Union of India, W.P.(Crl.) No. 314 of 2021, and connected matters (Pegasus litigation).*
11. *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*

C. *Government Reports*

12. *National Crime Records Bureau, Crime in India 2024, Ministry of Home Affairs, Government of India (2026).*

D. *Web and Institutional Sources*

13. *"Pegasus Spyware Probe #7: Technical Committee Granted More Time to Submit Final Report," Supreme Court Observer (2022), https://www.scobserver.in.*
14. *"Supreme Court's Pegasus Spyware Case: Key Legal Questions on Privacy, Surveillance, and Rule of Law," NeuroAmicus (2025).*
15. *"'Nothing Wrong in Country Using Spyware': Supreme Court on Pegasus Row," Business Standard (29 April 2025).*

16. *"'What's Wrong': Supreme Court Backs Spyware Use—Everything You Need to Know About the Pegasus Controversy," The Mooknayak (2025).*
17. *"Pegasus Snooping Case: Malware Found in 5 Phones but No Conclusive Proof That It Had Spyware, Says Supreme Court," Deccan Herald (2022).*
18. *"SC Gives More Time to Pegasus Probe Panel to Submit Report," Deccan Herald (2022).*
19. *"Pegasus: Supreme Court Extends Time for Submitting Probe Report on Use of Israeli Spyware," The Tribune (2022).*
20. *"Supreme Court Committee Monitoring Pegasus Matter, Report Awaited: Govt Source," The Tribune (2022).*
21. *"Cybersecurity Laws in India: Gaps and Future Prospects," Legal Service India (2026).*
22. *"Strengthening India's Cybersecurity Framework: IT Laws and Rules," Journalism University (2026).*
23. *"Cybersecurity Laws and Regulations India 2025," LexOrbis (2025).*
24. *"Navigating Digital Surveillance in India: Balancing Security and Privacy," The LawGist (2024).*
25. *"State Surveillance and Privacy Rights: Legal Frameworks and Challenges in India," Mondaq (2025).*
26. *"Cybersecurity Laws and Regulations in India – July 2026," Prashant Mali Cyber Law Blog (2026).*
27. *"Government Access to Data under the DPDP Act, 2023: Exemptions, Surveillance Concerns, and Safeguards," KSandK (2025).*
28. *"Data Rights and Surveillance: A Global Perspective," Nitishastra Substack (2026).*