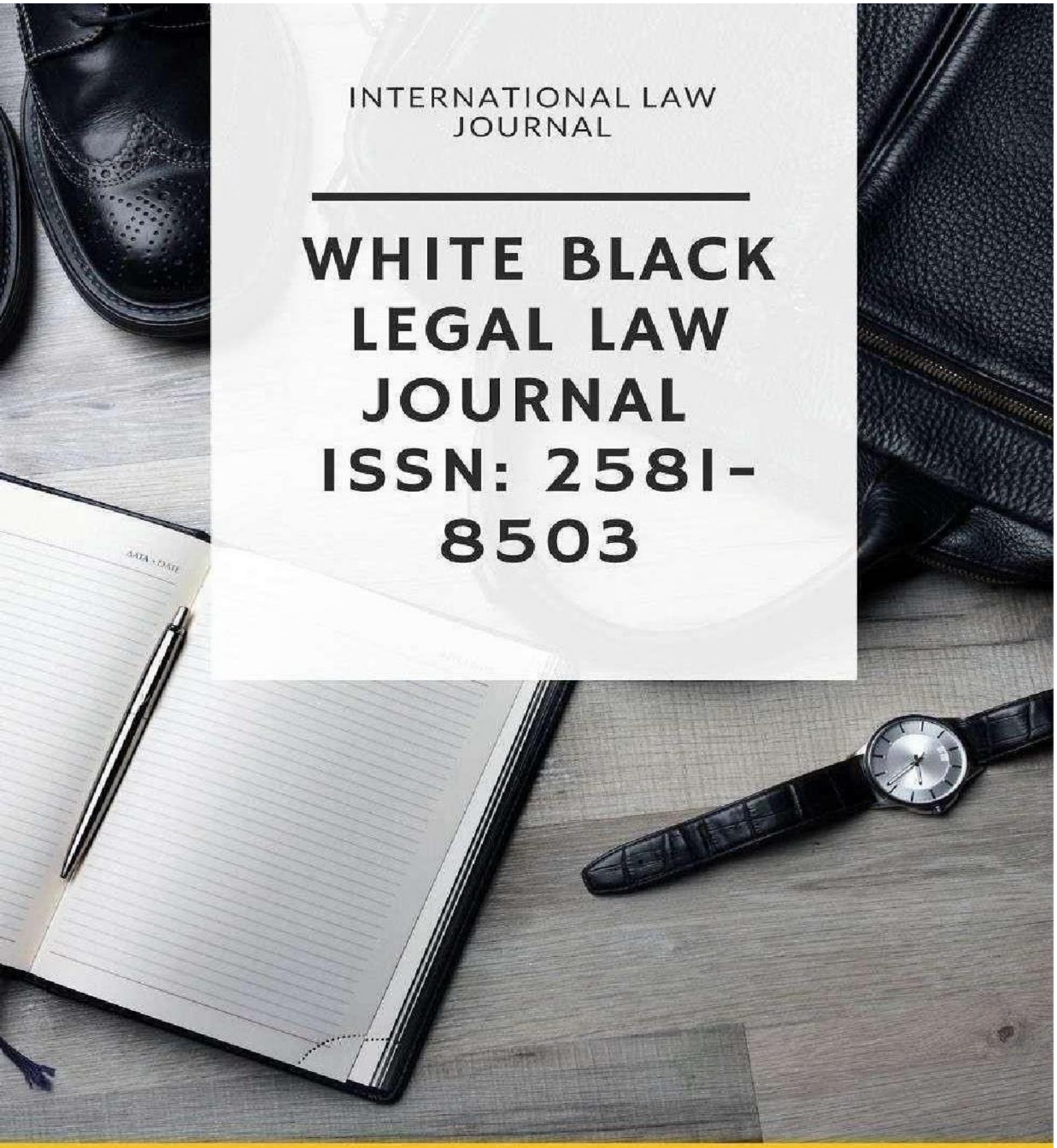

INTERNATIONAL LAW JOURNAL

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

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

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

BALANCING PRIVACY AND DIGITAL SURVEILLANCE: A CRITICAL ANALYSIS OF CRIMINAL INVESTIGATION POWERS UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023 AND THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - ATUL VERMA

ABSTRACT

India's criminal procedure and data-protection regimes were both fundamentally re-written within a span of weeks in December 2023: the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS") replaced the Code of Criminal Procedure, 1973, and the Digital Personal Data Protection Act, 2023 ("DPDP Act") gave India its first comprehensive data-protection statute. Both instruments came into force within two years of each other — the BNSS on 1 July 2024 and the DPDP Act in a phased manner through the DPDP Rules, 2025 — yet they embody starkly different regulatory philosophies: the BNSS substantially expands the investigative state's access to digital devices, electronic records, and forensic data, while the DPDP Act purports to entrench purpose limitation, consent, and data-minimisation as principles governing the processing of personal data. This paper undertakes a critical, doctrinal examination of the point at which these two philosophies collide: the exercise of criminal investigation powers — search and seizure of digital devices under Sections 94, 103, and 106–107 BNSS, interception of communications under Section 69 of the Information Technology Act, 2000, and forensic examination of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 — against the backdrop of the DPDP Act's blanket law-enforcement exemption under Section 17(1)(c). The paper traces the constitutional foundation of this inquiry to the Supreme Court's privacy jurisprudence in People's Union for Civil Liberties v Union of India and Justice K.S. Puttaswamy (Retd.) v Union of India, and to the unresolved judicial and legislative response to the 2021 Pegasus spyware controversy. It argues that while the BNSS introduces welcome transparency safeguards — principally mandatory audio-video recording of search and seizure — it does not import a requirement of prior judicial authorisation for digital device search comparable to a search warrant, and that the DPDP Act's law-enforcement exemption is drafted so broadly as to place executive data-processing largely

outside the statute's own accountability architecture. Drawing on comparative reference to the United Kingdom's Investigatory Powers Act, 2016 and the European Union's Law Enforcement Directive, the paper proposes a calibrated set of statutory and procedural safeguards — including judicial pre-authorisation for non-consensual digital device search, a statutory necessity-and-proportionality test for law-enforcement data processing, and an independent oversight mechanism for interception — designed to reconcile India's legitimate investigative needs with the constitutional guarantee of privacy under Article 21.

Keywords: *Digital Surveillance; Right to Privacy; Bharatiya Nagarik Suraksha Sanhita, 2023; Digital Personal Data Protection Act, 2023; Search and Seizure; Interception; Proportionality; Article 21; Criminal Investigation; Data Protection*

1. INTRODUCTION

The Indian criminal justice system underwent its most significant procedural overhaul in over half a century with the enactment, in December 2023, of a trilogy of statutes — the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS"), and the Bharatiya Sakshya Adhiniyam, 2023 ("BSA") — replacing the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973 ("CrPC"), and the Indian Evidence Act, 1872 respectively, with effect from 1 July 2024.[1]

Almost simultaneously, Parliament enacted the Digital Personal Data Protection Act, 2023 ("DPDP Act"), which received Presidential assent on 11 August 2023 and began phased implementation following the notification of the Digital Personal Data Protection Rules, 2025 on 13 November 2025, with full compliance obligations set to mature by May 2027.[2]

The near-simultaneous arrival of these two legislative families — one substantially expanding the investigative and evidentiary reach of the State into digital devices and communications, the other purporting to constrain how personal data may be processed — creates an unusual and under-examined point of legal tension. The BNSS explicitly contemplates production and search of 'electronic communication devices' likely to contain digital evidence, mandates

[1]PRS Legislative Research, 'The Bharatiya Nagarik Suraksha Sanhita, 2023' Bill Track Summary (2023); Bharatiya Nagarik Suraksha Sanhita, 2023, s.1.
[2]Digital Personal Data Protection Act, 2023, s.1; Digital Personal Data Protection Rules, 2025 (notified 13 November 2025).

audio-video recording of search and seizure, and expands the categories of property subject to police seizure. The DPDP Act, for its part, exempts processing of personal data for the 'prevention, detection, investigation or prosecution of any offence' from the ordinary obligations of the statute under Section 17(1)(c) — an exemption whose outer boundary remains, as this paper demonstrates, substantially undefined.

This tension is not merely theoretical. It surfaced during the legislative passage of the BNSS itself: in his dissent note appended to the Report of the Parliamentary Standing Committee on Home Affairs, Member of Parliament Derek O'Brien specifically flagged that the BNSS's provisions on summons for documents and search and seizure of digital devices — including phones and laptops — could violate both the right to privacy and the right against self-incrimination under Article 20(3) of the Constitution.[3]

The problem is compounded by India's unresolved institutional response to state-sponsored surveillance controversies, most prominently the 2021 Pegasus spyware allegations, in which a court-appointed technical committee found that several examined devices carried indicators of malware while the Union Government declined to confirm or deny procurement or use of the spyware, citing national security. The Supreme Court's own reticence in that matter — declining to compel disclosure while nonetheless describing the state's stance as incompatible with treating the court as a 'mute spectator' on fundamental rights — illustrates the structural difficulty of judicial oversight over covert digital surveillance in India.

1.1 Statement of the Problem

India's digital investigation and surveillance framework is presently governed by at least four distinct statutory regimes — the BNSS (search, seizure, and production of digital evidence), the Information Technology Act, 2000 (interception, monitoring, decryption, and blocking under Sections 69, 69A, and 69B), the BSA (admissibility and authentication of electronic evidence), and the DPDP Act (processing of personal data, subject to a law-enforcement exemption) — that were not drafted, and have not since been amended, to operate as a single coherent framework. Each regime prescribes its own (markedly different) standard of ex-ante authorisation, oversight, and remedial recourse, producing a fragmented and, in places,

[3]MediaNama, 'Device Seizure Rules in BNSS Violate Right to Privacy: Derek O'Brien' (18 November 2023), discussing the dissent note to the Report of the Standing Committee on Home Affairs on the Bharatiya Nagarik Suraksha Sanhita, 2023.

internally inconsistent structure of safeguards for the individual whose digital life is the subject of a criminal investigation.

1.2 Objectives of the Study

- To map the digital investigation and surveillance powers conferred by the BNSS, the IT Act, and the BSA, and to assess the ex-ante and ex-post safeguards attached to each.
- To critically examine the scope and adequacy of the DPDP Act's law-enforcement exemption under Section 17(1)(c) as a check on executive data-processing.
- To trace the constitutional foundation for privacy-protective limits on investigation and surveillance powers through the PUCL and Puttaswamy lines of Supreme Court jurisprudence.
- To evaluate the institutional response to the Pegasus controversy as a case study in the limits of judicial oversight over covert digital surveillance.
- To propose calibrated statutory and procedural safeguards that reconcile legitimate investigative necessity with the constitutional guarantee of privacy under Article 21.

1.3 Research Questions

- Do the search, seizure, and production powers under the BNSS incorporate safeguards functionally equivalent to prior judicial authorisation for digital device search?
- Does the DPDP Act's Section 17(1)(c) exemption meaningfully constrain, or effectively exclude, law-enforcement data processing from the Act's accountability architecture?
- Has the Puttaswamy proportionality standard been operationalised in statutory form, or does it remain an unenforced judicial aspiration in the digital investigation context?
- What institutional design — judicial, parliamentary, or independent — would best supply the oversight function that the Pegasus episode revealed to be structurally absent?

1.4 Research Methodology

This paper adopts a doctrinal legal research methodology, analysing primary sources (the BNSS, 2023; the IT Act, 2000; the BSA, 2023; the DPDP Act, 2023 and DPDP Rules, 2025; and relevant constitutional case law) alongside secondary sources (parliamentary committee reports, law-firm commentary, and peer-reviewed literature). The paper employs a comparative method with reference to the United Kingdom's Investigatory Powers Act, 2016 (which introduced judicial commissioners for interception approval) and the European Union's Law

Enforcement Directive (EU) 2016/680, to benchmark the adequacy of India's safeguard architecture. The analysis is current to August 2026.

1.5 Scope and Limitations

This paper confines its analysis to criminal investigation and law-enforcement surveillance; it does not examine the DPDP Act's application to private commercial data processing except insofar as necessary to explain the structure of the Section 17 exemptions. Similarly, while the paper references the Pegasus controversy as an illustrative case study, it does not purport to establish factual findings regarding the extent of spyware deployment in India, relying instead on the reported findings of the court-appointed technical committee.

2. LITERATURE REVIEW

Scholarship bearing on this paper's inquiry can be organised along three axes: constitutional privacy jurisprudence, procedural criminal law reform, and data-protection exemption design.

2.1 Constitutional Privacy Jurisprudence

The doctrinal starting point for any analysis of Indian surveillance law is the Supreme Court's 1997 decision in People's Union for Civil Liberties v Union of India, in which the Court held that unregulated telephone tapping under Section 5(2) of the Indian Telegraph Act, 1885 infringed the fundamental right to privacy, and issued detailed procedural guidelines — including a requirement of authorisation by the Home Secretary and periodic review by a committee of senior secretaries — later codified in Rule 419A of the Indian Telegraph Rules.[4] Two decades later, the nine-judge bench in Justice K.S. Puttaswamy (Retd.) v Union of India unanimously recognised privacy as an intrinsic facet of the right to life and personal liberty under Article 21, and articulated a four-fold proportionality standard — legality, legitimate aim, rational nexus (suitability), and necessity (least restrictive means) — that any state measure restricting privacy must satisfy.[5]

Scholarly commentary on Puttaswamy has consistently observed that while the judgment supplies a normatively rich standard, subsequent legislation — including the BNSS and the

[4]People's Union for Civil Liberties v Union of India (1997) 1 SCC 301; Indian Telegraph Rules, 1951, r.419A (inserted 2007).

[5]Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; the four-fold test was further refined in Justice K.S. Puttaswamy v Union of India (Aadhaar) (2019) 1 SCC 1 (Chandrachud J, dissenting on some points but concurring on the proportionality framework) and in Internet and Mobile Association of India v RBI (2020) 10 SCC 274.

DPDP Act — has not consistently operationalised that standard in statutory text, leaving courts to apply the proportionality test on a case-by-case, post-hoc basis rather than through ex-ante statutory design.

2.2 Procedural Reform Literature on the BNSS

Early commentary on the BNSS, including PRS Legislative Research's bill-track analysis, has focused on the statute's headline reforms: mandatory forensic investigation for offences punishable by seven years' imprisonment or more, electronic filing of first information reports, provision for trial in absentia against proclaimed offenders, and the restructuring of erstwhile Section 102 CrPC (police power to seize suspect property) into a two-part scheme under Sections 106 (power to seize) and 107 (post-seizure procedure) of the BNSS.[6]

A more critical strand of literature, exemplified by the dissent note of MP Derek O'Brien and subsequent commentary, has focused specifically on Section 94 BNSS (successor to Section 91 CrPC), which empowers a court or police officer in charge of an investigation to summon 'any document or thing' — a formulation broad enough to encompass mobile phones, laptops, and cloud-linked accounts — without an accompanying requirement of prior judicial authorisation analogous to a search warrant, and without an express carve-out for privileged or self-incriminatory digital content.[7]

Judicial commentary predating the BNSS had already begun to develop procedural safeguards for digital search independent of statute: the Karnataka High Court's 2021 guidelines on search and seizure of electronic records required the presence of a qualified forensic examiner, prohibited investigating officers from operating seized devices, and mandated use of Faraday bags to prevent remote wiping — safeguards that remain judicially, rather than statutorily, sourced even after the BNSS.[8]

2.3 Data-Protection Exemption Design Literature

Literature on the DPDP Act's Section 17 exemptions is comparatively young, reflecting the Act's own delayed phased implementation. Commentary converges on the observation that Section 17(1)(c) — exempting processing 'necessary for the purpose of prevention, detection,

[6]PRS Legislative Research (n 1); RVR Attorneys, 'Seizure, Safeguards and Transparency: How the BNSS Rewrites Police Seizure Law' (29 December 2025).
[7]MediaNama (n 4).
[8]Karnataka High Court guidelines (2021), discussed in PRS Legislative Research, 'The Bharatiya Sakshya Bill, 2023' Bill Track Summary, citing Report No. 248, Standing Committee on Home Affairs, Rajya Sabha (10 November 2023).

investigation or prosecution of any offence or contravention of any law' — is markedly broader than comparable exemptions in foreign data-protection statutes: the United Kingdom's Data Protection Act, 2018, for instance, confines equivalent law-enforcement processing to a defined class of 'competent authorities' and subjects such processing to a distinct statutory Part (Part 3) with its own principles, rather than a blanket carve-out from the general Act.[9]

Further commentary has noted the breadth of the Central Government's residual exemption power under Section 17(2) and the open-ended, time-unlimited transitional exemption power under Section 17(5) — as of early 2026 unexercised, but structurally capable of exempting an entire class of government data processing from the Act for a specified duration without requiring Parliamentary approval of the individual notification.[10]

2.4 Research Gap

Existing literature treats the BNSS's search-and-seizure reforms, the IT Act's interception regime, and the DPDP Act's law-enforcement exemption as largely separate subjects, each analysed within its own statutory silo. No sustained doctrinal work yet reads these regimes together as a composite 'digital investigation and surveillance framework' and tests that composite framework against the Puttaswamy proportionality standard as a unified benchmark. This paper undertakes that integration, and further situates the analysis within the unresolved institutional lessons of the Pegasus episode.

3. ANALYSIS AND DISCUSSION

3.1 Mapping the Digital Investigation and Surveillance Toolkit

Contemporary Indian criminal investigation of any offence with a digital dimension draws on a composite toolkit spanning four statutes. Table 1 maps the principal powers, the authorising authority, and the associated safeguard gaps.

Table 1: Digital Investigation and Surveillance Powers under Indian Law

Provision	Nature of Power	Authorising Authority	Principal Safeguard Gap
S.94, BNSS, 2023	Summons to produce document or thing (including digital	Court or officer in charge of a police station	None express; no prior judicial authorisation requirement; broad enough to capture mobile

[9]Cyril Amarchand Mangaldas Dispute Resolution Blog, 'Internal Investigations Under the Digital Personal Data Protection Act, 2023' (23 January 2025), comparing DPDP Act s.17(1)(c) with UK Data Protection Act 2018, ss.22–42 (Part 3) and Sch.2 para.2(1)(a).
[10]ComplyZero, 'DPDP Act Exemptions: When the Law Does Not Apply' (6 February 2026).

	devices) for investigation, inquiry or trial.		phones, laptops, and cloud-linked accounts.
S.103, BNSS, 2023	Search of place suspected to contain stolen property, forged documents, etc.; extends to digital storage.	Magistrate warrant (general) / police officer (specified circumstances)	Warrant generally required, but police officers retain circumstances for warrantless search; mandatory audio-video recording introduced as a new safeguard.
Ss.106–107, BNSS, 2023	Power of police officer to seize property (including electronic/digital assets) and post-seizure procedure.	Police officer, reported to Magistrate	Restructured from single s.102 CrPC clause into two provisions for greater procedural clarity; audio-video recording of seizure now mandatory.
S.176, BNSS, 2023	Mandatory forensic investigation (including of digital devices) for offences punishable by 7+ years.	Forensic expert visiting crime scene	Improves evidentiary quality but does not itself constrain the initial seizure decision; silent on chain-of-custody for cloud/remote data.
S.69, IT Act, 2000	Interception, monitoring, or decryption of information transmitted through a computer resource.	Secretary, Ministry of Home Affairs (Central) / State Home Secretary	Executive (not judicial) authorisation; oversight via a Review Committee of senior secretaries under IT (Procedure and Safeguards for Interception) Rules, 2009, following PUCL guidelines — no independent judicial commissioner.
S.69A, IT Act, 2000	Blocking of public access to online information/content.	Designated officer, Central Government	Distinct procedure under the Blocking Rules, 2009; limited transparency, as blocking orders are typically confidential.
S.69B, IT Act, 2000	Monitoring and collection of traffic data for cyber security.	Central Government-authorised agency	Broadly worded 'cyber security' purpose; minimal statutory definition of scope or retention

			limits.
S.63, BSA, 2023	Certification requirement for admissibility of electronic evidence.	Person in charge of the relevant device/system	Addresses admissibility, not the propriety of the underlying seizure; does not itself constrain investigative overreach.
S.17(1)(c), DPDP Act, 2023	Exemption of law-enforcement data processing from the Act's general obligations.	Self-assessed by the processing authority	No requirement of independent prior authorisation, necessity/ proportionality assessment on the record, or ex-post reporting to the Data Protection Board.

Source: Compiled by author from the Bharatiya Nagarik Suraksha Sanhita, 2023; Information Technology Act, 2000; Bharatiya Sakshya Adhiniyam, 2023; and Digital Personal Data Protection Act, 2023.

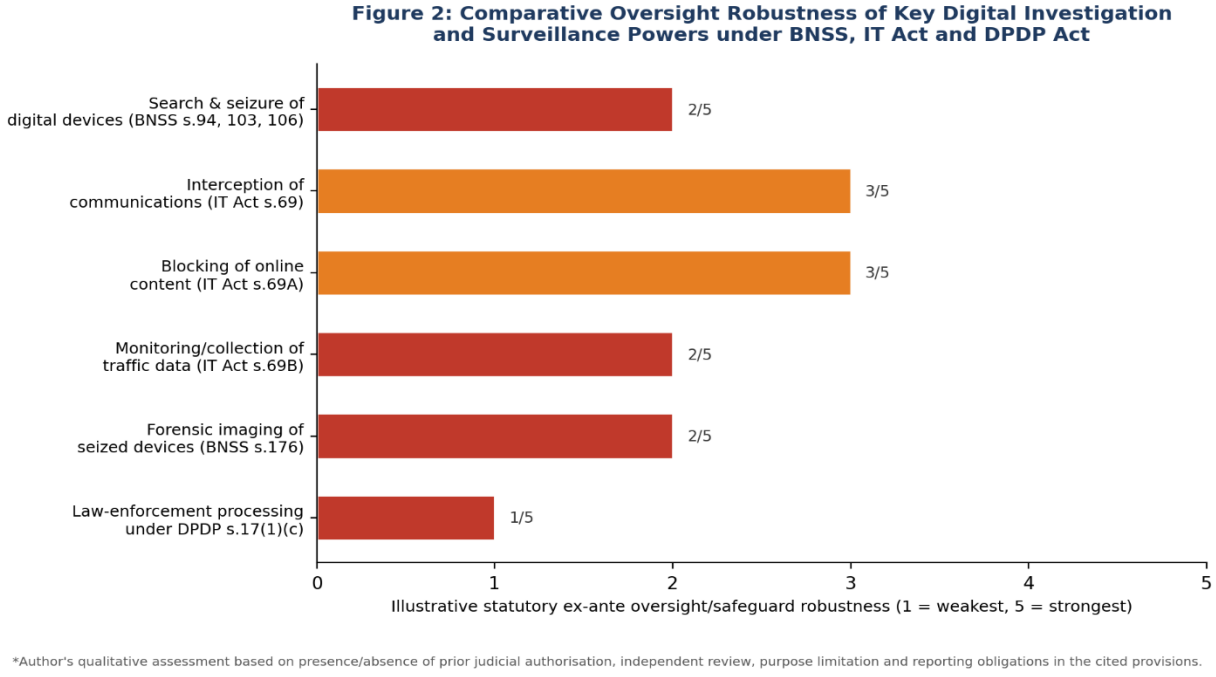

Figure 2: Comparative oversight robustness of key digital investigation and surveillance powers (author's qualitative assessment).

The composite picture is one of markedly uneven safeguard design. Physical search of a residence under Section 103 BNSS generally still requires a Magistrate's warrant, echoing the CrPC's traditional structure; but summons for a digital device or account under Section 94 BNSS — which as a practical matter is now the more common and often more revealing form of evidence-gathering — requires no equivalent prior judicial sign-off. This asymmetry is

significant precisely because a smartphone or cloud account today typically contains a far more comprehensive and intimate record of a person's life than the physical premises a warrant would traditionally have authorised searching.

3.2 Search, Seizure, and Production of Digital Devices under the BNSS

The BNSS retains the CrPC's basic architecture for search and seizure while introducing two principal digital-era reforms. First, Section 105 (and related provisions) mandate that search and seizure be recorded through 'audio-video electronic means', preferably by mobile phone, and that such recordings be forwarded to the Magistrate — a transparency safeguard entirely absent from the CrPC.[11]

Second, Sections 106 and 107 BNSS restructure the erstwhile Section 102 CrPC power of seizure into a bifurcated scheme — a power to seize (Section 106) followed by a distinct post-seizure procedure (Section 107) — explicitly recognising 'digital or electronic form' as a category of seizeable property and requiring the seizing officer to report the seizure to the officer-in-charge and, through them, to a Magistrate.[12]

These reforms are genuine improvements over the CrPC's comparative silence on digital evidence. They do not, however, address the central concern raised in the parliamentary dissent note: neither Section 94 (summons for documents/things) nor Sections 106–107 (seizure) requires prior judicial authorisation — of the kind a search warrant represents for physical premises — before a police officer may compel production of, or seize, a digital device. Audio-video recording is a valuable ex-post transparency and accountability measure; it operates, however, after the search has already been authorised and conducted, and does not substitute for an independent, ex-ante assessment of necessity and proportionality specific to the volume and sensitivity of data typically held on a personal digital device.

This gap is thrown into relief by comparison with the judicially developed (but non-statutory) Karnataka High Court guidelines, which required a qualified forensic examiner's presence, prohibited the investigating officer from personally operating the seized device, and mandated Faraday-bag isolation to prevent remote wiping or tampering — protections that exist today only as persuasive precedent in one High Court's jurisdiction rather than as a uniform, BNSS-mandated national standard.[13]

[11]Bharatiya Nagarik Suraksha Sanhita, 2023, s.105; Obhan & Associates, 'Introduction of the Bharatiya Nagarik Suraksha Sanhita, 2023: A Step Towards Digital India' (9 December 2025).
[12]RVR Attorneys (n 8).
[13]PRS Legislative Research, 'The Bharatiya Sakshya Bill, 2023' (n 6).

3.3 Interception under Section 69 of the IT Act: Executive Authorisation without Judicial Oversight

Interception, monitoring, and decryption of electronic communications continues to be governed by Section 69 of the IT Act, 2000, read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, which require an authorising order from the Union Home Secretary (or the State Home Secretary, as applicable) rather than a judicial officer.[14]

This structure directly descends from the Supreme Court's 1997 PUCL guidelines, which — in the absence of any judicial-authorisation requirement in the Indian Telegraph Act, 1885 — devised an executive safeguard: a Review Committee comprising the Cabinet Secretary, the Law Secretary, and the Secretary of Telecommunications (at the Central level) tasked with examining, within two months, whether an interception order complies with the statutory conditions.[15]

Twenty-nine years after PUCL, this remains an entirely executive-internal safeguard: the authorising Secretary and the reviewing Committee are all part of the executive branch, with no judicial officer or independent commissioner in the chain of approval. The Puttaswamy court's proportionality standard — particularly its necessity and least-restrictive-means limb — has not, on this record, been translated into a requirement of independent (as distinct from purely internal-executive) authorisation for interception, notwithstanding that interception is, on any view, among the most privacy-invasive investigative techniques available to the State.

3.4 The Pegasus Episode as a Case Study in Oversight Failure

The 2021 Pegasus spyware controversy — in which independent forensic reporting suggested that NSO Group's Pegasus spyware may have targeted the devices of journalists, opposition politicians, and civil society figures in India — tested the adequacy of this executive-oversight model under real conditions. The Supreme Court constituted a technical committee headed by former Justice R.V. Raveendran; the committee's report, submitted in 2022, found that five of twenty-nine examined phones showed indicators of possible malware infection, while noting that the Union Government had declined to cooperate with the inquiry.[16]

The Court itself observed that the government's refusal to confirm or deny use of the spyware,

[14]Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r.3.
[15]People's Union for Civil Liberties (n 2); PRS Legislative Research, 'FAQs on Telephone Tapping' (2026).
[16]Deccan Herald, 'Pegasus Snooping Case: Malware Found in 5 Phones But No Conclusive Proof That It Had Spyware, Says Supreme Court' (2022).

on national-security grounds, in proceedings 'which touches upon the fundamental rights of the citizens of the country, cannot be accepted', and that mere invocation of national security does not render the Court 'a mute spectator.' Notwithstanding this observation, the matter did not result in either a definitive finding on Pegasus's use by Indian agencies or legislative reform of Section 69 to introduce independent oversight.[17]

The episode is instructive for this paper's purposes because it demonstrates, in a concrete instance, the structural limitation of the existing safeguard model: even the apex constitutional court, exercising its broadest fact-finding powers through a specially constituted technical committee, could not compel executive disclosure sufficient to resolve the central factual question, still less to test the proportionality of any interception against the Puttaswamy standard in a specific case. If judicial review at the level of the Supreme Court itself faces this constraint, the case for embedding independent, ex-ante oversight directly into the statutory authorisation process — rather than relying on post-hoc litigation — is considerably strengthened.

3.5 The DPDP Act's Law-Enforcement Exemption: A Second, Parallel Gap

Section 17(1)(c) of the DPDP Act exempts from the Act's general obligations any 'processing of personal data necessary for the purpose of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force.' Unlike the United Kingdom's Data Protection Act, 2018, which confines equivalent law-enforcement processing to defined 'competent authorities' and subjects it to a distinct statutory Part with its own principles (data-quality, purpose-limitation, and security duties specific to law-enforcement processing), the DPDP Act's exemption operates as a blanket carve-out from Chapter II of the Act altogether, with no substituted law-enforcement-specific data-protection principles filling the resulting gap.[18]

Commentary has further noted that the DPDP Rules, 2025 neither define the outer boundary of what qualifies as processing 'necessary' for investigation nor prescribe any documentation, proportionality-assessment, or reporting obligation that a law-enforcement authority must satisfy before invoking the exemption — leaving the determination effectively self-assessed by the very authority whose processing is in question.[19]

[17]CSOHate.org, 'Indian Supreme Court's Silence on Pegasus Legitimizes Spying on Critics' (2024), quoting the Supreme Court's October 2021 order.
[18]Cyril Amarchand Mangaldas Dispute Resolution Blog (n 12); Digital Personal Data Protection Act, 2023, s.17(1)(c).
[19]Cyril Amarchand Mangaldas Dispute Resolution Blog (n 12).

This gap is compounded by the residual and transitional exemption powers under Sections 17(2) and 17(5), the latter permitting the Central Government to exempt any class of Data Fiduciary from any provision of the Act for a specified duration during a five-year transitional window running to August 2028, without a requirement of Parliamentary approval for each individual notification.[20]

Read together, Sections 17(1)(c), 17(2), and 17(5) mean that the DPDP Act's core accountability architecture — consent, purpose limitation, data-minimisation, the Data Protection Board's grievance jurisdiction — does not meaningfully reach the government's own investigative and security-related data processing, precisely the domain in which, per the PUCL and Pegasus experience, independent oversight has historically been weakest. The DPDP Act, in other words, was a missed legislative opportunity to close the safeguard gap that PUCL identified in 1997 and that Pegasus illustrated in 2021; instead, it largely reproduces that gap in a new statutory form.

3.6 Applying the Puttaswamy Proportionality Standard

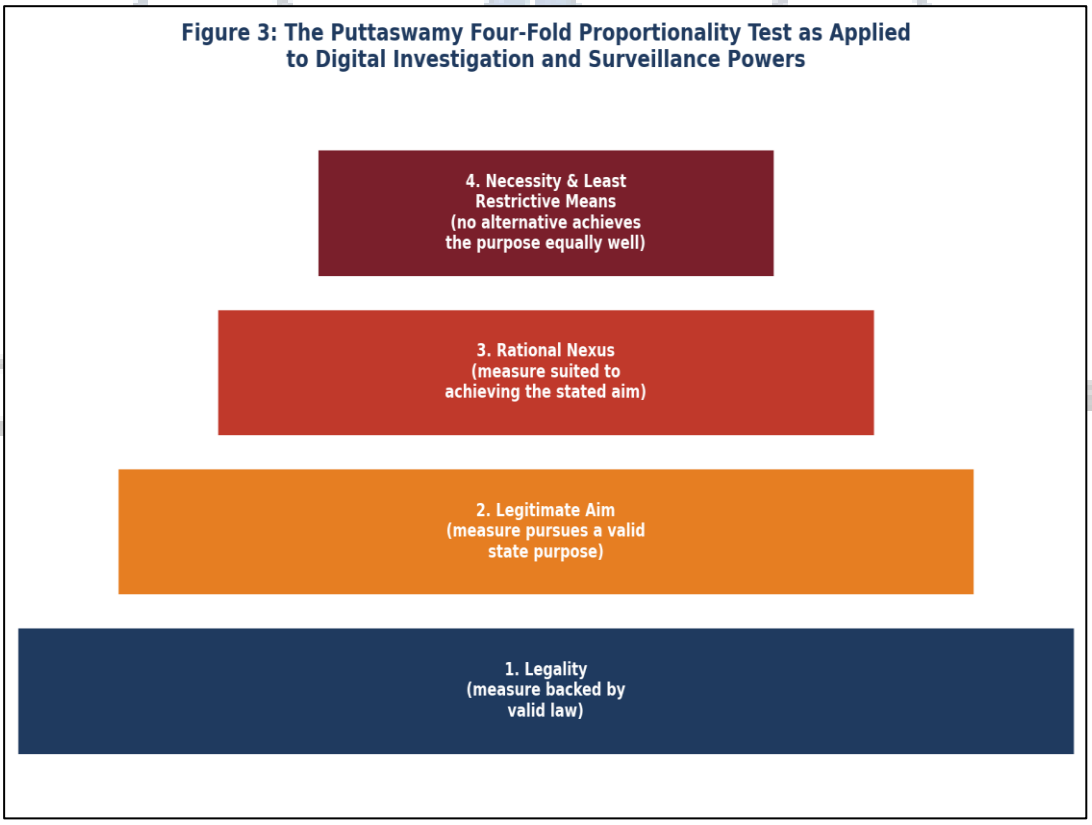

Figure 3: The Puttaswamy four-fold proportionality test applied to digital investigation and surveillance powers.

[20] ApniLaw, 'DPDP Act Penalties and Exemptions' (2026); ComplyZero (n 13).

The Puttaswamy court's four-fold test — legality, legitimate aim, rational nexus (suitability), and necessity (least restrictive means) — supplies a workable analytical framework for evaluating each power mapped in Table 1.[21]

Applying this framework: (i) Legality is broadly satisfied across the BNSS, IT Act, and DPDP Act powers, each having a clear statutory basis. (ii) Legitimate aim is similarly satisfied — crime prevention, investigation, and national security are undisputedly legitimate state purposes. (iii) Rational nexus (suitability) is generally satisfiable on a case-specific basis, though the breadth of Section 94 BNSS ('any document or thing') and Section 17(1)(c) DPDP Act ('necessary for... investigation') means that the suitability of a given exercise of power to its stated purpose is not tested at the point of authorisation, but only if and when the matter is later litigated. (iv) Necessity (least restrictive means) is the limb most consistently unaddressed at the statutory level: none of Section 94 BNSS, Section 69 IT Act, or Section 17(1)(c) DPDP Act requires the authorising or exempting authority to consider, on the record, whether a less privacy-invasive method could achieve the same investigative objective before exercising the power.

This paper's central analytical finding, elaborated further in Part 4, is therefore that the necessity/least-restrictive-means limb of the constitutionally mandated proportionality test has not been operationalised in statutory form across any of the three principal digital investigation and surveillance regimes examined — a gap that leaves the burden of enforcing this limb of Puttaswamy entirely on post-hoc constitutional litigation, an avenue the Pegasus episode shows to be slow, resource-intensive, and frequently inconclusive.

3.7 Comparative Perspective

The United Kingdom's Investigatory Powers Act, 2016 offers an instructive comparative model: it introduced a 'double-lock' authorisation mechanism for the most intrusive surveillance warrants (including interception), requiring both ministerial authorisation and approval by an independent Judicial Commissioner — a serving or former senior judge — applying judicial review principles before a warrant takes effect.[22]

The European Union's Law Enforcement Directive (EU) 2016/680 similarly requires that law-enforcement data processing be subject to purpose limitation, data-minimisation, and independent supervisory-authority oversight functionally equivalent to that applicable to

[21] Justice K.S. Puttaswamy (Retd.) v Union of India (n 3), per Chandrachud J.
[22] Investigatory Powers Act 2016 (UK), ss.19–23 (Judicial Commissioner approval for interception warrants).

general data processing — in contrast to the DPDP Act's approach of exempting law-enforcement processing from equivalent principles altogether.[23]

Neither the 'double-lock' judicial-commissioner model nor the EU's law-enforcement-specific principles-based model has been adopted in India's BNSS/IT Act/DPDP Act framework. India's model remains, by comparison, executive-centric at the authorisation stage (Home Secretary approval for interception; no judicial pre-authorisation for digital device summons/seizure) and largely exemption-based at the data-protection stage (blanket Section 17(1)(c) carve-out rather than a parallel law-enforcement-specific principles regime).

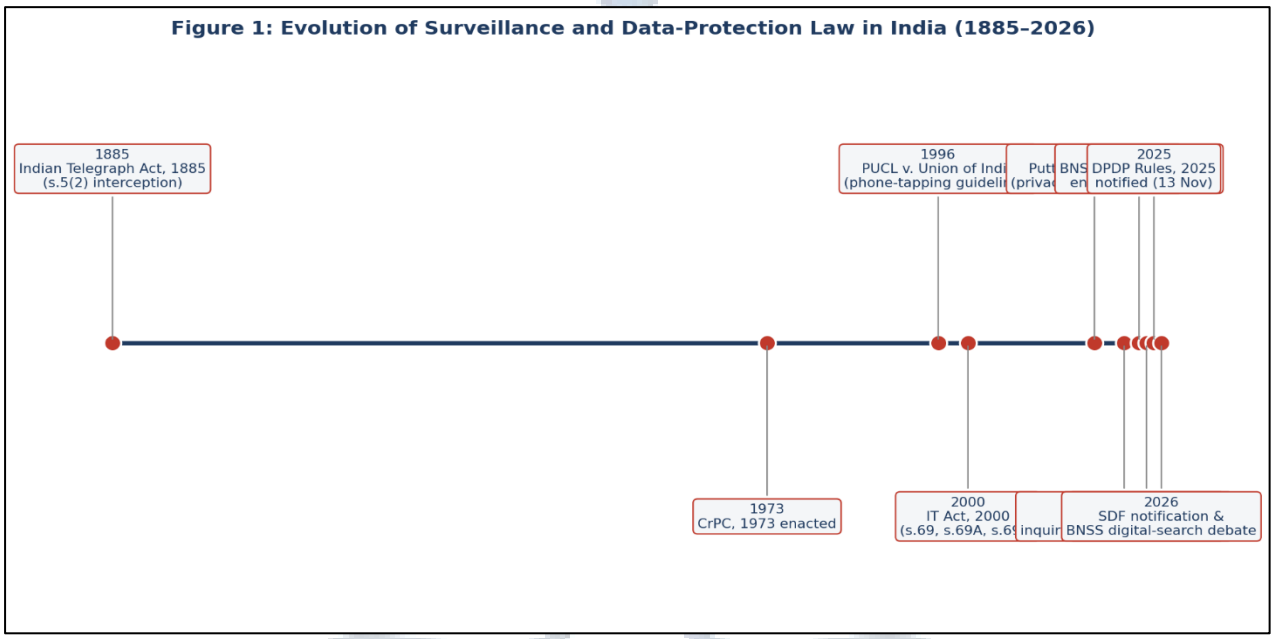

Figure 1: Evolution of surveillance and data-protection law in India (1885–2026).

4. FINDINGS

Finding 1: Digital Device Search Lacks a Judicial Pre-Authorisation Requirement

Unlike the search of physical premises under Section 103 BNSS, which generally requires a Magistrate's warrant, the summons power for digital devices and 'things' under Section 94 BNSS, and the seizure power under Sections 106–107 BNSS, do not require prior judicial authorisation, notwithstanding that digital devices today typically contain a far more comprehensive record of private life than physical premises.

Finding 2: Audio-Video Recording Is a Valuable but Purely Ex-Post Safeguard

The BNSS's mandatory audio-video recording of search and seizure is a genuine transparency

[23]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (Law Enforcement Directive), arts.4, 8, 41–47.

improvement over the CrPC, but it documents the conduct of a search after authorisation has already occurred; it does not substitute for an ex-ante necessity and proportionality assessment.

Finding 3: Interception Oversight Remains Executive-Internal, Unchanged Since 1997

The Section 69 IT Act interception framework continues to rely on Home Secretary authorisation and executive Review Committee oversight, a structure inherited from the 1997 PUCL guidelines and not updated to introduce independent (judicial or quasi-judicial) approval, notwithstanding the Puttaswamy court's subsequent articulation of a more demanding proportionality standard in 2017.

Finding 4: The Pegasus Episode Demonstrates the Limits of Post-Hoc Judicial Oversight

Even Supreme Court-level fact-finding, through a specially constituted technical committee, could not compel executive cooperation sufficient to resolve factual disputes regarding spyware use, illustrating that reliance on post-hoc litigation is an inadequate substitute for embedded, ex-ante procedural safeguards.

Finding 5: The DPDP Act's Law-Enforcement Exemption Is Broader Than Comparable Foreign Models and Largely Unaccountable

Section 17(1)(c) DPDP Act exempts law-enforcement processing from the Act's general obligations without substituting a parallel, law-enforcement-specific set of principles (as in the UK Data Protection Act, 2018 or the EU Law Enforcement Directive), and without any documentation, necessity-assessment, or reporting requirement, leaving the exemption's application effectively self-assessed.

Finding 6: The Necessity/Least-Restrictive-Means Limb of Puttaswamy Remains Statutorily Unoperationalised

Across the BNSS, IT Act, and DPDP Act regimes examined, no provision requires the authorising or exempting authority to consider, on the record, whether a less privacy-invasive method could achieve the same investigative objective — the specific proportionality limb the Supreme Court itself has emphasised as central to Article 21 privacy protection.

Finding 7: India's Model Diverges from Comparable Democracies on Independent Authorisation

Neither the UK's judicial-commissioner 'double-lock' model nor the EU's law-enforcement-

specific principles regime has an Indian statutory analogue; India's framework remains comparatively executive-centric at both the authorisation stage (interception, digital device summons) and the accountability stage (DPDP Act exemption).

5. RECOMMENDATIONS

Recommendation 1: Introduce Judicial Pre-Authorisation for Non-Consensual Digital Device Search

Section 94 BNSS should be amended to require, save in genuine exigent circumstances (to be narrowly defined and subject to prompt post-facto judicial ratification within 24–48 hours), a Magistrate's prior authorisation before a digital device or cloud-linked account may be compelled to be produced or searched, mirroring the existing warrant requirement for physical premises under Section 103 BNSS.

Recommendation 2: Codify the Karnataka High Court Digital-Search Safeguards Nationally

The presence of a qualified forensic examiner, the prohibition on investigating officers personally operating a seized device, and mandatory Faraday-bag isolation should be codified as uniform, nationally applicable BNSS Rules rather than remaining persuasive precedent confined to one High Court's jurisdiction.

Recommendation 3: Establish an Independent Judicial Commissioner for Interception Approval

Section 69 of the IT Act and the 2009 Interception Rules should be amended to introduce a UK-style 'double-lock' mechanism: ministerial (Home Secretary) authorisation should remain a necessary but no longer sufficient condition, with a serving or retired High Court/Supreme Court judge, appointed as an independent Judicial Commissioner, required to approve each interception order applying judicial-review-equivalent scrutiny before it takes effect.

Recommendation 4: Statutorily Operationalise the Necessity/Least-Restrictive-Means Test

A cross-cutting provision — whether inserted into the BNSS, the IT Act, or as a standalone Digital Investigation Safeguards Act — should require every authorising authority (Magistrate, Home Secretary, or Judicial Commissioner) to record, in writing, why no less privacy-invasive investigative method was reasonably available, operationalising the necessity limb of the Puttaswamy proportionality test as an enforceable procedural precondition rather than a

standard invoked only in subsequent litigation.

Recommendation 5: Replace the DPDP Act's Blanket Law-Enforcement Exemption with a Parallel Principles-Based Regime

Section 17(1)(c) DPDP Act should be narrowed and supplemented, along UK/EU lines, with a distinct chapter setting out law-enforcement-specific data-protection principles — purpose limitation, data minimisation, defined retention periods, and a duty to document the necessity of processing — applicable to processing that would otherwise fall within the exemption, rather than exempting such processing from the Act's accountability architecture altogether.

Recommendation 6: Empower the Data Protection Board with Law-Enforcement Oversight Jurisdiction

The Data Protection Board of India's jurisdiction should be extended to receive and adjudicate complaints regarding law-enforcement data processing under the proposed narrowed exemption, with appropriate safeguards for genuinely sensitive operational information, rather than leaving such processing entirely outside the Board's grievance-redressal mechanism.

Recommendation 7: Institute Periodic Parliamentary Reporting on Interception and Digital Search Powers

An annual, aggregate (non-case-specific) report on the volume and categories of interception orders under Section 69 IT Act and digital device search/seizure orders under the BNSS should be tabled before Parliament's Standing Committee on Home Affairs, providing a structural, ongoing accountability mechanism independent of ad hoc litigation of the kind that arose in the Pegasus matter.

Recommendation 8: Sunset and Parliamentary Review of Section 17(5) DPDP Act Exemptions

Any exemption notified under the transitional power in Section 17(5) DPDP Act should be subject to a defined sunset period and mandatory tabling before Parliament, closing the presently open-ended character of that provision identified in Part 3.5 above.

6. CONCLUSION

India's near-simultaneous enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Digital Personal Data Protection Act, 2023 presented an unusual opportunity to design, from

first principles, a coherent statutory architecture reconciling the investigative needs of the State with the constitutional guarantee of privacy articulated in Puttaswamy. That opportunity has been only partially realised. The BNSS introduces genuine, welcome transparency reforms — mandatory audio-video recording of search and seizure chief among them — but stops short of requiring prior judicial authorisation for the search of digital devices, notwithstanding that such devices now typically hold a far more revealing record of private life than the physical premises to which warrant requirements have traditionally applied. The DPDP Act, for its part, exempts law-enforcement data processing from the Act's own accountability architecture through a blanket provision considerably broader than comparable exemptions in the United Kingdom or the European Union, without substituting a parallel set of law-enforcement-specific safeguards.

The 2021 Pegasus episode remains the clearest illustration of what is at stake in this gap: even the Supreme Court's own specially constituted technical committee could not secure the executive cooperation needed to resolve, conclusively, whether Indian agencies deployed a globally controversial surveillance tool against journalists and civil society actors. If judicial oversight at the apex level faces this constraint, the case for embedding independent, ex-ante safeguards directly into the statutory text — rather than relying on litigation after the fact — is considerably strengthened.

This paper has proposed a calibrated set of reforms — judicial pre-authorisation for digital device search, codified national forensic-search safeguards, an independent Judicial Commissioner for interception approval, statutory operationalisation of the Puttaswamy necessity test, and a narrowed, principles-based replacement for the DPDP Act's law-enforcement exemption — designed not to impede legitimate criminal investigation, but to ensure that the exercise of digital investigation and surveillance powers is, in the Puttaswamy court's own words, consistently 'just, fair, and reasonable', tested against a genuine necessity standard rather than left to the self-assessment of the very authorities exercising the power.

REFERENCES

A. Statutes and Delegated Legislation

1. Constitution of India, 1950, arts.19, 20(3), 21.
2. Indian Telegraph Act, 1885, s.5(2).
3. Indian Telegraph Rules, 1951, r.419A (inserted 2007).

4. Code of Criminal Procedure, 1973 (repealed) s.91, s.102 [historical reference].
5. Information Technology Act, 2000 (as amended), ss.69, 69A, 69B.
6. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
7. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
8. Bharatiya Nagarik Suraksha Sanhita, 2023, ss.94, 103, 105, 106, 107, 176.
9. Bharatiya Sakshya Adhiniyam, 2023, s.63.
10. Digital Personal Data Protection Act, 2023, ss.17(1)(c), 17(2), 17(5).
11. Digital Personal Data Protection Rules, 2025 (notified 13 November 2025).
12. UK Data Protection Act, 2018, ss.22–42 (Part 3), Sch.2 para.2(1)(a).
13. Investigatory Powers Act 2016 (UK), ss.19–23.
14. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (Law Enforcement Directive), arts.4, 8, 41–47.

B. Cases

15. People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.
16. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
17. Justice K.S. Puttaswamy v Union of India (Aadhaar) (2019) 1 SCC 1.
18. Internet and Mobile Association of India v Reserve Bank of India (2020) 10 SCC 274.
19. Manohar Lal Sharma v Union of India (Pegasus matter) (2021) SCC OnLine SC 985; Report of the Technical Committee (2022).

C. Books and Journal Articles

20. Report No. 248, 'The Bharatiya Sakshya Bill, 2023', Standing Committee on Home Affairs, Rajya Sabha (10 November 2023).
21. Report of the Standing Committee on Home Affairs on the Bharatiya Nagarik Suraksha Sanhita, 2023, including dissent note of MP Derek O'Brien.

D. Reports, Advisories and Online Sources

22. PRS Legislative Research, 'The Bharatiya Nagarik Suraksha Sanhita, 2023' Bill Track Summary (2023).
23. PRS Legislative Research, 'The Bharatiya Sakshya Bill, 2023' Bill Track Summary (2023).

24. PRS Legislative Research, 'FAQs on Telephone Tapping' (2026).
25. MediaNama, 'Device Seizure Rules in BNSS Violate Right to Privacy: Derek O'Brien' (18 November 2023).
26. RVR Attorneys, 'Seizure, Safeguards and Transparency: How the BNSS Rewrites Police Seizure Law' (29 December 2025).
27. Obhan & Associates, 'Introduction of the Bharatiya Nagarik Suraksha Sanhita, 2023: A Step Towards Digital India' (9 December 2025).
28. Corrida Legal, 'The Bharatiya Nagarik Suraksha Sanhita, 2023 – Executive Summary and Bare Act' (31 March 2026).
29. Grokipedia, 'Bharatiya Nagarik Suraksha Sanhita' (26 February 2026).
30. Cyril Amarchand Mangaldas Dispute Resolution Blog, 'Internal Investigations Under the Digital Personal Data Protection Act, 2023' (23 January 2025).
31. dpdpa.com, 'Digital Personal Data Protection Act, 2023 – Section 17 with Interpretation' (9 January 2026).
32. Matters.ai, 'DPDP Act 2023: India's Digital Personal Data Protection Law Explained' (2 March 2026).
33. CADP, 'DPDP Act Key Provisions Explained: A Detailed Analysis' (30 January 2026).
34. ApniLaw, 'DPDP Act Penalties and Exemptions' (2026).
35. ComplyZero, 'DPDP Act Exemptions: When the Law Does Not Apply' (6 February 2026).
36. Mondaq, 'Installation of Pegasus Spyware and Breach of Privacy' (7 September 2021).
37. Supreme Court Observer, 'State Surveillance: From Phone-Tapping to Pegasus' (9 October 2023).
38. CSOHate.org, 'Indian Supreme Court's Silence on Pegasus Legitimizes Spying on Critics' (8 December 2024).
39. Neuroamicus, 'Supreme Court's Pegasus Spyware Case: Key Legal Questions on Privacy, Surveillance, and Rule of Law' (3 October 2025).
40. Deccan Herald, 'Pegasus Snooping Case: Malware Found in 5 Phones But No Conclusive Proof That It Had Spyware, Says Supreme Court' (2022).
41. Lawctopus Academike, 'Law on Phone Tapping in India in Light of Public Safety' (2020).