INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

SURVEILLANCE LAW IN INDIA: CONSTITUTIONAL FRAMEWORKS, STATUTORY POWERS, AND THE CRISIS OF ACCOUNTABILITY

AUTHORED BY - E YESHVANT NEMALAN
(2nd Year B.Com,LLB(hons.))
Affiliation: Sastra University Thanjavur

ABSTRACT

"State Surveillance Privacy Accountability Crisis"

This research paper critically analyses the constitutional and statutory framework governing surveillance law in India, focusing on the balance between national security and the fundamental right to privacy. The study examines the evolution of privacy jurisprudence through landmark judgments such as Justice K.S. Puttaswamy v. Union of India and People's Union for Civil Liberties v. Union of India, which established constitutional limitations on state surveillance powers. It evaluates the interception and monitoring powers granted under the Indian Telegraph Act, 1885 and the Information Technology Act, 2000, highlighting concerns relating to executive control, absence of judicial oversight, and lack of accountability. The paper further studies the development of modern surveillance infrastructure including the Central Monitoring System, NATGRID, Aadhaar-linked databases, facial recognition technologies, and spyware controversies such as Pegasus. Comparative analysis with international surveillance frameworks is also undertaken to identify global standards of transparency and proportionality. The study concludes that India's surveillance regime requires substantial legal reform to ensure constitutional compliance, safeguard civil liberties, and establish effective mechanisms for transparency, oversight, and protection of individual privacy in the digital era.

Introduction

Of all the powers that the modern state exercises over its citizens, the power of surveillance is among the most intimate and the most dangerous. To observe, intercept, and record the private communications and movements of an individual is to penetrate the innermost sphere of her life — the domain of thought, association, political belief, and personal relationship that the

ISSN: 2582-6433

Constitution of India, under Article 21, protects as the core of human dignity and liberty. Yet surveillance is also indispensable to the security state: no credible system of law enforcement or national security can function without intelligence gathered through the interception of communications, the monitoring of movements, and the collection of data about persons who pose genuine threats to public order and national security. The tension between these imperatives — the individual's right to privacy against the state's duty to protect — is the defining problematic of surveillance law. In India, this tension is acute. The country confronts genuine and severe security challenges: insurgency, terrorism, cross-border infiltration, and organised crime. It also confronts the challenges of democratic accountability, judicial independence, and the prevention of state overreach. A surveillance apparatus that operates without meaningful legal constraint is not merely a privacy threat; it is a threat to political pluralism, press freedom, civil society, and the constitutional order itself. India's surveillance law framework is characterised by three features that together constitute a crisis of constitutional governance. First, the statutory powers of interception and surveillance are extraordinarily broad, authorising surveillance on grounds — 'public order,' 'sovereignty,' 'friendly relations with foreign states' — that are capable of encompassing virtually any conduct the executive chooses to designate as threatening. Second, the oversight mechanisms are institutionally weak Judicial authorisation is not required before interception; parliamentary oversight is minimal; and independent review is essentially absent. Third, the technological capacity of the Indian state — and of private actors deploying surveillance technology against Indian citizens — has expanded exponentially, while the legal framework has remained largely unchanged since 1885. This paper undertakes a systematic analysis of India's surveillance law. It examines the constitutional foundation of the right to privacy, the statutory architecture of interception powers, the role of mass data collection in enabling state surveillance, the Pegasus spyware controversy, the interface between surveillance and the right to information, comparative perspectives from global surveillance law, and the reform agenda necessary to bring Indian surveillance law into conformity with constitutional values and international human rights standards.

The Constitutional Framework:

The Right to Privacy as a Fundamental Right The constitutional foundation of India's surveillance law is the right to privacy, declared a fundamental right by the nine-judge Constitution Bench of the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of

ISSN: 2582-6433

India.[1] The Puttaswamy judgment is the most significant constitutional pronouncement on privacy in the Court's history, and its implications for surveillance law are profound and far-reaching. The Court held, unanimously, that the right to privacy is intrinsic to life and liberty under Article 21, and that it encompasses informational privacy — the right of the individual to control information about herself — as well as the right to the privacy of the home and of personal communication. Of particular relevance to surveillance law is the Court's articulation of the test for permissible restrictions on the right to privacy. Drawing upon the proportionality doctrine developed in European constitutional jurisprudence, the Court held that any state action that infringes the right to privacy must satisfy three requirements: it must be authorised by law (the requirement of legality); it must serve a legitimate state aim; and the means employed must be necessary and proportionate to that aim. This tripartite test — legality, legitimate aim, proportionality — establishes the constitutional standard against which India's surveillance powers must be evaluated. Justice D.Y. Chandrachud's concurring opinion in Puttaswamy contains the most sustained analysis of the implications of the right to privacy for surveillance. The learned judge observed that 'metadata' — data about communications rather than their content — is itself entitled to privacy protection, as the aggregation of metadata can reveal information about an individual's associations, movements, political beliefs, and personal relationships that is at least as sensitive as the content of any individual communication. This observation is of particular significance in the age of mass data collection and algorithmic profiling.

Telephone Tapping and the Pre-Puttaswamy Jurisprudence The Supreme Court's engagement with the constitutionality of telephone interception predates the Puttaswamy judgment by more than two decades. In People's Union for Civil Liberties v. Union of India (1997),[2] the Court held that telephone tapping constitutes a 'serious invasion of an individual's privacy' and that the right to hold a telephone conversation in the privacy of one's home or office is an integral part of the right to life under Article 21. The Court upheld the constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885 — which authorises interception of communications — but subject to procedural safeguards. The Court accordingly laid down guidelines: orders must be made by the Home Secretary; each order must specify the grounds for interception; orders are valid for two months renewable to a maximum of six months; and a Review Committee must periodically scrutinise all interception orders. The PUCL guidelines were subsequently

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[2] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

ISSN: 2582-6433

codified by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Indian Telegraph (Amendment) Rules, 2007. However, these rules replicated the fundamental structural weakness of the PUCL framework: oversight is conducted by an executive Review Committee — chaired by a Cabinet Secretary or state Chief Secretary — rather than by an independent judicial authority. The fox, in effect, guards the henhouse. C. The Post-Puttaswamy Constitutional Landscape The Puttaswamy judgment has fundamentally altered the constitutional landscape of surveillance law. The judgment establishes that surveillance powers must satisfy the proportionality test: not merely that they serve a legitimate state aim, but that they are necessary to achieve that aim, and that the degree of privacy infringement is proportionate to the benefit obtained. A blanket interception power, exercisable by the executive without judicial authorisation and without meaningful oversight, cannot plausibly satisfy the proportionality requirement. The constitutional challenge to India's surveillance framework — which has been only partially mounted before the courts — remains to be fully adjudicated. The Supreme Court's constitution bench proceedings in Manohar Lal Sharma v. Union of India (the Pegasus case) represent the most recent and significant judicial engagement with these unresolved questions.

The Statutory Architecture of Surveillance Powers

The Indian Telegraph Act, 1885: A Colonial Relic The primary statutory authority for the interception of communications in India is Section 5(2) of the Indian Telegraph Act, 1885 — a statute enacted to regulate the telegraph network of British India.[3] Section 5(2) empowers the Central Government or a state government, 'on the occurrence of any public emergency, or in the interest of the public safety,' to direct that any message or class of messages be intercepted or detained 'in the interests of the sovereignty or integrity of India, the security of the State, the friendly relations with foreign States or public order or for preventing incitement to the commission of an offence.' The breadth of these grounds is extraordinary. 'Public order' — interpreted by the Supreme Court to encompass any disturbance of community life, however localised — is alone a ground expansive enough to authorise surveillance of virtually any political dissident, trade union organiser, or civil society advocate whose activities the executive characterises as a threat to order. 'Friendly relations with foreign states' is a ground without parallel in the surveillance law of any established democracy. The statute contains no

[3] Indian Telegraph Act, 1885, s. 5(2), No. 13, Acts of Parliament, 1885 (India).

ISSN: 2582-6433

requirement of individualised suspicion, no obligation to specify the target of interception, and no mandatory judicial review of interception orders. The statute's colonial provenance is significant. It was designed for an era in which the telegraph was the exclusive medium of long-distance communication, operated by a state monopoly. Its application by successive governments to modern telecommunications — satellite communications, internet data, mobile telephony — has been achieved by statutory interpretation and executive notification rather than by legislative reform. The Telecommunications Act, 2023, which is intended to replace the Telegraph Act, replicates the Section 5(2) interception power in substantially similar terms, representing a missed opportunity to modernise the legal framework for surveillance in light of the Puttaswamy judgment.

The Information Technology Act, 2000: Expanding Surveillance in the Digital Age Section 69 of the Information Technology Act, 2000 empowers the Central Government or a state government to direct any agency to intercept, monitor, or decrypt any information transmitted through any computer resource, 'in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognisable offence.'[4] The grounds are substantially identical to those under the Telegraph Act, and the statute similarly places no requirement of judicial authorisation. Section 69A of the IT Act empowers the Central Government to block public access to information on the internet — a power of extraordinary significance in an age where the internet is the primary medium of public communication, political organisation, and journalistic publication. Blocking orders under Section 69A are issued without notice to the affected party, and the reasons for blocking are not made public. The Supreme Court, in Shreya Singhal v. Union of India,[5] struck down Section 66A of the IT Act — which criminalised online speech causing 'annoyance' or 'inconvenience' — as an unconstitutional restriction on freedom of expression, but did not examine the constitutionality of Section 69A or Section 69's interception powers. Section 69B of the IT Act empowers the Central Government to direct any agency to monitor and collect traffic data and information through any computer resource for the purpose of enhancing 'cyber security.' This provision — which authorises bulk surveillance of internet traffic without any requirement of individualised suspicion or judicial oversight — is the statutory basis for the government's internet monitoring infrastructure, including the Central Monitoring System (CMS) and the NETRA (Network

[4] Information Technology Act, 2000, s. 69, No. 21, Acts of Parliament, 2000 (India).
[5] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

ISSN: 2582-6433

Traffic Analysis) system.

The Central Monitoring System and Mass Surveillance Infrastructure The Central Monitoring System (CMS), reportedly operational since 2013, is a centralised technical infrastructure that enables government agencies to directly access telephone calls, SMS messages, and internet communications of any user in India without the mediation of the telecommunications service provider. Under the CMS architecture, interception orders are transmitted electronically to the telecommunications network, and the intercepted data flows directly to the monitoring agency. The CMS eliminates the previous requirement that the telecom operator physically implement the interception — a step that, while imperfect, at least created a point of human review and potential resistance. The existence of the CMS was not publicly acknowledged by the government for several years after reports of its development first emerged. No legislation specifically authorises the CMS; its legal basis rests on the general interception powers under the Telegraph Act and the IT Act, applied to a technical infrastructure whose capabilities far exceed what those statutes contemplated. The CMS's capacity for bulk interception — the collection of communications across entire networks rather than the targeted interception of specific individuals — raises profound questions of proportionality that the existing legal framework is entirely unequipped to address.

The National Intelligence Grid (NATGRID) and Data Fusion The National Intelligence Grid (NATGRID) is a planned intelligence fusion architecture that would link the databases of twenty-one government agencies — including the Income Tax Department, banks, immigration records, credit card databases, train and airline booking records, and vehicle registration records — to provide authorised agencies with real-time access to integrated data profiles of individuals. NATGRID represents the apotheosis of the surveillance state's ambition: the conversion of the administrative data generated by citizens' ordinary activities into a comprehensive intelligence resource available to security agencies without judicial oversight or individualised suspicion. NATGRID has been under development for over a decade, with implementation repeatedly delayed. Its constitutional validity has never been judicially tested. The data fusion architecture that NATGRID represents — aggregating individually innocuous data points into a comprehensive surveillance profile — is precisely what Justice Chandrachud's analysis of metadata in Puttaswamy identifies as constitutionally problematic. The absence of a specific statutory framework governing NATGRID's operations, access protocols, and oversight mechanisms is a fundamental legal deficiency.

ISSN: 2582-6433

Aadhaar, Biometric Surveillance, and the Architecture of Identity

Aadhaar as a Surveillance Infrastructure The Aadhaar biometric identification system — now covering over 1.3 billion Indians — is the largest biometric database in the world. Aadhaar collects and stores the fingerprints, iris scans, and facial photographs of enrolled individuals, along with demographic information, and assigns each individual a unique twelve-digit identification number. The Aadhaar architecture was designed for the purpose of enabling efficient delivery of government services and welfare benefits; its designers and proponents have consistently maintained that it is not a surveillance tool. The Supreme Court's five-judge constitution bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (the Aadhaar judgment, 2018)[6] upheld the constitutional validity of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 with significant modifications. The Court held that the use of Aadhaar for government welfare delivery was constitutionally permissible, but struck down provisions requiring Aadhaar authentication for private sector purposes, the opening of bank accounts, obtaining SIM cards, and school enrolment. The majority held that the extensive linkage of Aadhaar to private transactions would create an infrastructure for surveillance and profiling inconsistent with the right to privacy. Justice D.Y. Chandrachud, dissenting, characterised the Aadhaar architecture as a 'surveillance state' in embryo, observing that the centralised storage of biometric data, the authentication logs generated by every Aadhaar transaction, and the potential for data sharing across government databases created conditions for pervasive surveillance of citizens' daily lives. The dissent's analysis — particularly its observation that authentication logs could be used to construct a detailed record of an individual's economic transactions, movements, and associations — has been widely regarded as the more prescient assessment of Aadhaar's surveillance potential.

Aadhaar Linkage and the Expansion of the Surveillance Network Notwithstanding the Supreme Court's partial restriction of mandatory Aadhaar linkage, the government has progressively expanded the scope of Aadhaar authentication through voluntary linkage programmes, legislative amendments, and regulatory requirements. The Crime and Criminal Tracking Network and Systems (CCTNS) — a national database linking the records of police stations across India — has been proposed for integration with Aadhaar, creating the potential for biometric matching of criminal suspects against the national population database. The National Automated Facial Recognition System (NAFRS), developed by the National Crime Records

[6] Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.), (2019) 1 SCC 1.

ISSN: 2582-6433

Bureau, is designed to enable real-time facial recognition across CCTV networks, with matching against Aadhaar's photograph database. The development of NAFRS without a specific legislative framework — without statutory authorisation, data protection standards, error rate requirements, or accountability mechanisms — exemplifies the pattern of technological surveillance deployment that characterises Indian governance: capabilities are developed and deployed administratively, without parliamentary authorisation, and the legal framework is constructed, if at all, after the fact. The Privacy International report on India's surveillance infrastructure has identified this pattern as a fundamental departure from the rule-of-law principles articulated in Puttaswamy.

The Pegasus Spyware Controversy:

The Pegasus Revelations In July 2021, a global investigative journalism consortium — the Pegasus Project — published findings indicating that the Pegasus spyware developed by the Israeli surveillance technology company NSO Group had been used to target the mobile devices of journalists, opposition politicians, human rights lawyers, academics, and business figures in India.[7] Pegasus is a zero-click spyware capable of gaining complete access to a target's smartphone — including its microphone, camera, messages, emails, photographs, and location data — without any action by the device's user, exploiting vulnerabilities in widely used applications including WhatsApp and Apple iMessage. Its use leaves minimal traces on the infected device, making forensic attribution difficult. The Pegasus Project's findings in relation to India were among the most extensive of any country in the investigation. The consortium identified over three hundred verified Indian mobile phone numbers on what it described as a list of potential targets of Pegasus surveillance. Those identified as potential targets included the mobile phones of Congress leader Rahul Gandhi, two serving cabinet ministers, three opposition leaders, a sitting Supreme Court judge, election commissioners, an official in the Prime Minister's Office, and numerous journalists and activists. The forensic examination of a subset of these devices by Amnesty International's Security Lab confirmed the presence of Pegasus spyware on several of them.

The Government's Response and the Supreme Court's Intervention The Indian government's response to the Pegasus revelations was characterised by neither denial nor admission. In proceedings before the Supreme Court, the government declined to file an affidavit confirming

[7] Forbidden Stories and Amnesty International, The Pegasus Project https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

ISSN: 2582-6433

or denying the use of Pegasus, asserting that disclosing whether the government used Pegasus would compromise national security. This position — that the government need not account to the Supreme Court for alleged surveillance of judges, politicians, and journalists — was fundamentally inconsistent with the constitutional principle that executive action is subject to judicial review. The Supreme Court, in Manohar Lal Sharma v. Union of India,[8] constituted an independent three-member Technical Expert Committee (TEC) to examine the Pegasus allegations and report to the Court. The Court expressed its deep concern at the potential chilling effect of spyware surveillance on press freedom and constitutional rights, observing that 'the mere existence of a surveillance device does not justify its use against every person.' The TEC's report — submitted in sealed cover to the Court in 2022 — has not been made public in its entirety, and the Court's final adjudication of the constitutional questions raised by the Pegasus case remains pending. The opacity of the proceedings has itself been criticised as inconsistent with the principles of open justice.

The Legal Vacuum Governing Spyware The deployment of spyware such as Pegasus against individuals in India reveals a fundamental gap in the legal framework. The interception powers under the Telegraph Act and the IT Act contemplate the interception of communications passing through telecommunications networks, with the cooperation of service providers. Spyware operates differently: it compromises the device itself, gaining access not only to communications in transit but to all data stored on or accessible from the device. The existing statutory regime does not clearly authorise — or regulate — the use of device-level intrusion tools. If the government used Pegasus, it either did so without any statutory authority or under a strained reading of Section 69 of the IT Act; in either case, the legal basis for such surveillance is deeply problematic. The absence of any legal framework specifically governing the acquisition, deployment, and oversight of offensive cyber tools by Indian intelligence and law enforcement agencies is a critical gap. Democratic states that use such tools — including the United Kingdom and Germany — have enacted specific legislation governing their use, requiring judicial authorisation and establishing independent oversight mechanisms. India has no equivalent framework.

[8] (July 2021), available at Manohar Lal Sharma v. Union of India, (2021) SCC OnLine SC 889.

ISSN: 2582-6433

Internet Shutdowns: Surveillance and the Control of Communication

India as the World's Internet Shutdown Capital Internet shutdowns — the deliberate disruption of internet access, whether total or partial, by government order — are a form of collective surveillance and communication control that has been used with increasing frequency in India. According to Access Now's annual Shutdown Tracker Optimisation Project (STOP) report, India has consistently ranked as the country with the highest number of internet shutdowns in the world, accounting for a disproportionate share of global shutdowns in every year between 2016 and 2023. Shutdowns have been imposed in the context of civil unrest, elections, examinations, communal violence, and protests — including the prolonged shutdown in Jammu and Kashmir following the abrogation of Article 370 in August 2019, which lasted over five months and constituted the longest internet shutdown in the history of any democracy. Internet shutdowns are ordered under Section 144 of the Code of Criminal Procedure (now Section 163 of the Bharatiya Nagarik Suraksha Sanhita, 2023), which empowers a magistrate to issue orders to prevent imminent danger to public order, or under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, framed under Section 5(2) of the Telegraph Act. The 2017 Rules require shutdown orders to be reviewed by a Review Committee within five working days — a requirement that has been widely observed in the breach.

Anuradha Bhasin v. Union of India and the Right to Internet Access The Supreme Court's decision in Anuradha Bhasin v. Union of India[9] — arising from the challenge to the internet shutdown in Jammu and Kashmir — is the leading authority on the constitutional limits of internet shutdowns. The Court held that the freedom of speech and expression under Article 19(1)(a), and the freedom to practice any trade or profession under Article 19(1)(g), extends to the internet, and that restrictions on internet access must satisfy the tests of necessity and proportionality. The Court further held that internet shutdown orders must be published, must be subject to judicial review, and that indefinite shutdowns are impermissible. While the Anuradha Bhasin decision represented a significant step forward, its practical impact has been limited. The Court stopped short of holding that internet access is itself a fundamental right (as distinct from holding that the exercise of fundamental rights through the internet is constitutionally protected), and the test of proportionality it articulated has proved difficult to operationalise in the absence of a legislative framework governing shutdowns. India continues

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

ISSN: 2582-6433

to impose internet shutdowns at a rate that is entirely inconsistent with the proportionality principle.

Surveillance and the Right to Information

Secrecy as the Handmaiden of Surveillance Effective surveillance depends on secrecy; its accountability depends on transparency. The tension between these imperatives is resolved, in India's legal framework, almost entirely in favour of secrecy. Interception orders under the Telegraph Act and the IT Act are classified; the identities of surveillance targets are not disclosed; the aggregate number of interception orders issued annually is not published; and the reasons for surveillance are shielded by broad national security exemptions from disclosure under the Right to Information Act, 2005. Section 24 of the RTI Act exempts from disclosure any information relating to the activities of the Intelligence Bureau, the Research and Analysis Wing, and seventeen other designated security and intelligence organisations. This blanket exemption — subject only to a narrow exception for allegations of corruption and human rights violations — means that citizens cannot use the RTI mechanism to discover whether they have been subjected to surveillance, on what grounds, or for how long. The RTI Act's transparency mandate is, in the surveillance context, almost entirely displaced by the security exemption.

The Absence of Notification A fundamental feature of surveillance law in democratic states — and one conspicuously absent from the Indian framework — is the requirement that persons who have been subjected to surveillance be notified after the surveillance has concluded, so that they may seek judicial redress if the surveillance was unlawful. Post-surveillance notification is required by the laws of Germany, the United States (under the Foreign Intelligence Surveillance Act), and the United Kingdom (under the Investigatory Powers Act, 2016). Notification enables the individual to challenge the legality of the surveillance before an independent tribunal and to seek suppression of unlawfully obtained material. Indian law imposes no obligation of post-surveillance notification. A person whose communications have been intercepted for months or years — including a journalist whose sources have been exposed, a lawyer whose client confidences have been compromised, or a political leader whose campaign strategy has been disclosed — has no legal mechanism through which to discover that she was surveilled, to challenge the legality of the surveillance, or to seek any remedy. This total absence of notification and redress mechanisms is inconsistent with the right to remedy under Article 32 of the Constitution and with India's obligations under the International Covenant on Civil and Political Rights.

ISSN: 2582-6433

Comparative Perspectives: Global Surveillance Law Standards

The United Kingdom: The Investigatory Powers Act, 2016 The United Kingdom's Investigatory Powers Act, 2016 (IPA) — enacted in response to the revelations of Edward Snowden about bulk surveillance by GCHQ and its partners in the Five Eyes intelligence alliance — is the most comprehensive surveillance law framework in the common law world, and provides an instructive comparator for the Indian framework.[10] The IPA consolidates the legal basis for all forms of official surveillance — targeted interception, bulk interception, equipment interference (spyware), bulk personal datasets — in a single statute, subjecting each to a clearly defined legal regime with specific authorisation requirements and oversight mechanisms. The most significant feature of the IPA's oversight architecture is the 'double lock' authorisation mechanism for targeted and bulk interception warrants: warrants are issued by the Secretary of State (executive authorisation) and then reviewed and countersigned by an independent Judicial Commissioner — a serving or retired senior judge — before taking effect. This mechanism ensures that executive judgment is subject to independent legal scrutiny before surveillance commences. A dedicated Investigatory Powers Tribunal — staffed by senior lawyers — adjudicates complaints by individuals who believe they have been subjected to unlawful surveillance, with the power to award remedies including the destruction of unlawfully obtained material.

The European Court of Human Rights: Privacy as a Constraint on Surveillance The European Court of Human Rights has developed an extensive body of jurisprudence on the compatibility of state surveillance with the right to private life under Article 8 of the European Convention on Human Rights. In Big Brother Watch v. United Kingdom,[11] the Grand Chamber of the ECtHR examined the UK's bulk interception regime and held that bulk surveillance is not per se incompatible with Article 8, provided that sufficient safeguards against abuse are in place — including clear rules on the categories of selectors used to filter intercepted communications, independent authorisation, and effective oversight. The Court's judgments have consistently emphasised that surveillance powers must be 'in accordance with law' in a sense that includes not only formal statutory authorisation but also foreseeability and accessibility — requirements that India's broadly drafted surveillance statutes struggle to satisfy.

[10] Investigatory Powers Act, 2016, c. 25 (United Kingdom).
[11] Big Brother Watch v. United Kingdom, App. No. 58170/13 (European Court of Human Rights, Grand Chamber, 2021).

ISSN: 2582-6433

The United States: Judicial Warrants and the Fourth Amendment The United States' surveillance law framework is anchored by the Fourth Amendment's prohibition on unreasonable searches and seizures, interpreted by the Supreme Court to require, in most circumstances, a judicial warrant supported by probable cause before the government may intercept private communications. The Electronic Communications Privacy Act, 1986 and the Foreign Intelligence Surveillance Act, 1978 (FISA) establish the statutory framework for electronic surveillance in domestic law enforcement and foreign intelligence contexts respectively. The FISA Court — a specialised federal court that reviews government applications for foreign intelligence surveillance warrants — provides a degree of judicial oversight absent from the Indian framework, though it has been criticised for operating largely in secret and for approving the vast majority of government applications without adversarial challenge. The Snowden revelations of 2013 exposed the extent to which the NSA's bulk surveillance programmes had operated beyond the framework that the public and many legislators understood FISA to authorise, prompting the USA FREEDOM Act, 2015, which ended bulk collection of domestic telephone metadata. The American experience illustrates both the importance of judicial and legislative oversight of surveillance and the persistent capacity of intelligence agencies to exploit legal ambiguities to expand their surveillance activities beyond publicly acknowledged limits — a lesson of particular relevance to the Indian context.

Surveillance of Journalists, Lawyers, and Political Opposition

The Chilling Effect on Press Freedom The surveillance of journalists — whether through interception of communications, monitoring of sources, or the deployment of spyware — constitutes one of the most serious threats to press freedom and democratic accountability. A journalist who knows, or fears, that her communications are being monitored cannot effectively protect the confidentiality of her sources. Sources who fear exposure will not come forward with information about official misconduct. The result is a systematic suppression of investigative journalism that serves the interests of those in power at the expense of the public's right to know. The Pegasus investigation identified numerous Indian journalists among the potential targets of surveillance. The targeting of journalists covering politically sensitive stories — including investigations into electoral bonds, government contracts, and official misconduct — is consistent with a pattern of surveillance directed not at genuine security threats but at the suppression of politically embarrassing information. The Press Freedom Index published by Reporters Without Borders has consistently rated India's press freedom

ISSN: 2582-6433

environment as poor, with surveillance identified as a significant contributing factor.

The Surveillance of Lawyers and Legal Professional Privilege The surveillance of lawyers — and in particular of lawyers representing clients in cases against the government or its agencies — strikes at the root of the right to a fair trial and legal professional privilege. A lawyer whose communications with her client are accessible to the prosecuting authority cannot provide effective legal representation. Legal professional privilege — the right of a client to communicate candidly with her lawyer without fear that those communications will be disclosed to adverse parties — is a fundamental principle of the rule of law, recognised by the Supreme Court as an important protection flowing from the right to fair trial under Article 21. The legal framework governing surveillance in India contains no specific protection for legally privileged communications. The Telegraph Act and the IT Act do not carve out any exemption for communications between lawyers and clients, and the procedural rules governing interception do not require any special scrutiny of intercepts that may include privileged material. This is a significant departure from the practice of mature rule-of-law jurisdictions: UK law, for example, requires specific authorisation for the interception of legally privileged communications and imposes strict restrictions on the use of intercepted privileged material.

Surveillance of Political Opposition and Civil Society The use of surveillance powers against political opponents, civil society organisations, and social movements is perhaps the most fundamental threat to democratic governance that an overreaching surveillance apparatus poses. The deployment of Pegasus against opposition leaders, the monitoring of activists and academics who participated in protests, and the use of the National Investigation Agency and the Enforcement Directorate against figures politically opposed to the ruling party have generated sustained concern — both domestically and internationally — about the instrumentalisation of security and financial investigation powers for political purposes. The Supreme Court has, in a series of decisions, affirmed that political dissent, peaceful protest, and criticism of government policy are constitutionally protected activities. In Romila Thapar v. Union of India,[12] a case arising from the arrest of academics and activists in connection with the Bhima Koregaon violence, the Court was called upon to examine allegations that digital evidence had been planted on the accused's devices by means of sophisticated malware — a claim supported by forensic analysis by independent experts. The case illustrated the deeply

[12] Romila Thapar v. Union of India, (2018) 10 SCC 753.

ISSN: 2582-6433

troubling intersection of offensive cyber capabilities, criminal prosecution, and political opposition.

The Telecommunications Act, 2023: Reform or Replication?

The Telecommunications Act, 2023 — enacted to replace the Indian Telegraph Act, 1885 and the Wireless Telegraphy Act, 1933 — represents the most significant legislative overhaul of India's telecommunications regulatory framework in over a century. The Act reorganises the licensing framework, provides for spectrum management, and consolidates the regulatory authority of the Telecom Regulatory Authority of India. In the specific context of surveillance law, however, the 2023 Act represents a deeply disappointing missed opportunity. Section 20 of the Telecommunications Act, 2023 replicates the interception and surveillance powers of Section 5(2) of the Telegraph Act in terms that are substantively identical, authorising interception on the same broad grounds — sovereignty, security, public order, friendly relations with foreign states — without any requirement of judicial authorisation, without any obligation of post-surveillance notification, and without any independent oversight mechanism beyond the executive Review Committee. The Act was passed by Parliament with minimal public debate about its surveillance provisions, notwithstanding the extensive civil society commentary that had highlighted the constitutional inadequacy of the existing framework following Puttaswamy. The failure to introduce judicial authorisation as a prerequisite for interception in the 2023 Act — in the face of clear constitutional guidance from Puttaswamy — has been characterised by digital rights advocates as a deliberate choice to preserve executive control over surveillance rather than an oversight. The Act does introduce some modest procedural improvements, including requirements for the periodic publication of aggregate interception statistics — a step toward transparency — but these fall far short of the structural reform that constitutional principle demands.

Conclusion and Recommendations

India's surveillance law framework stands at a critical juncture. The Puttaswamy judgment has established the constitutional principles against which surveillance powers must be measured; the Pegasus revelations have exposed the extent to which those powers — and capabilities beyond their statutory scope — have been deployed against journalists, lawyers, judges, and political opponents; and the Telecommunications Act, 2023 has demonstrated the government's determination to preserve, rather than reform, a surveillance architecture rooted in colonial

ISSN: 2582-6433

legislation and executive discretion. The result is a constitutional crisis in slow motion: the formal law articulates principles of proportionality and privacy, while the operational framework systematically violates them. This paper advances the following recommendations for a surveillance law reform agenda consistent with India's constitutional commitments. First, mandatory judicial authorisation must be introduced for all targeted interception of communications, whether under the Telecommunications Act or the IT Act. Interception orders should be issued by a designated Surveillance Court — constituted on the model of the UK's Investigatory Powers Commissioner or the US FISA Court — composed of sitting or retired High Court judges, with the power to refuse or modify applications that do not satisfy the requirements of necessity and proportionality. Emergency interception pending judicial authorisation should be permitted for a maximum of forty-eight hours, with automatic lapse if judicial authorisation is not obtained. Second, the grounds for interception must be narrowed and made specific. 'Public order' and 'friendly relations with foreign states' should be removed as independent grounds for surveillance, which should be restricted to genuinely serious threats to national security, terrorism, and serious organised crime.

Each interception order should be required to specify the identity of the target, the specific threat necessitating surveillance, and the anticipated duration of interception. Third, an independent Surveillance Commissioner — a senior judicial officer — should be appointed to oversee all surveillance activities, receive reports on the use of interception powers, conduct unannounced inspections of interception facilities, and publish an annual report to Parliament on the aggregate use of surveillance powers. The Commissioner should have the power to refer suspected abuse of surveillance powers to the appropriate prosecutorial authority. Fourth, a post-surveillance notification requirement should be introduced. Persons who have been subjected to surveillance should be notified, within a reasonable period following the conclusion of surveillance, that their communications were intercepted, unless the Surveillance Commissioner certifies that notification would jeopardise an ongoing investigation. Notified individuals should have access to a Surveillance Tribunal before which they may challenge the lawfulness of the surveillance and seek remedies including the destruction of unlawfully obtained material. Fifth, the deployment of offensive cyber tools — spyware, device implants, and network compromise tools — by any government agency must be placed on an explicit statutory footing, with specific authorisation requirements (including individual judicial warrants), operational safeguards, and independent oversight. The use of any spyware tool that has not been specifically authorised by the Surveillance Court should be a criminal offence.

ISSN: 2582-6433

Sixth, internet shutdowns should be removed from the jurisdiction of executive magistrates under Section 163 BNSS and placed under a statutory framework requiring judicial authorisation, specification of the geographic scope and duration of the shutdown, a mandatory proportionality assessment, and automatic periodic judicial review. The legislative framework should expressly prohibit blanket shutdowns of indefinite duration, consistent with the proportionality principle affirmed in Anuradha Bhasin. Surveillance is, ultimately, a question of power — who wields it, against whom, on what authority, and subject to what accountability. A democracy that permits its security apparatus to surveil judges, journalists, lawyers, and opposition politicians without judicial oversight and without accountability has compromised the foundations of its own constitutional order. The reform of India's surveillance law is not merely a technical legal project; it is a constitutional imperative, and its urgency is proportionate to the sophistication of the surveillance technologies that the state now commands.

Bibliography:

- Legislation Telecommunications Act, 2023, No. 44, Acts of Parliament, 2023 (India).
- Indian Telegraph Act, 1885
- Information Technology Act, 2000
- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
- Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (India).
- Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).
- Investigatory Powers Act, 2016, c. 25 (United Kingdom).
- Foreign Intelligence Surveillance Act, 50 U.S.C. sections 1801-1885c (1978) (United States).
- https://internetfreedom.in.
- https://timesofindia.indiatimes.com
- https://wikipedia.com