INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

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.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

BEYOND INTERCEPTION: PEGASUS SPYWARE, AND CONSTITUTIONAL ACCOUNTABILITY IN INDIA

AUTHORED BY - VANSHIKA SHARMA
B.A. LL.B. (Hons.), Third Year,
Dr. B.R. Ambedkar National Law University, Sonepat.

ABSTRACT

The July 2021 disclosures of the Pegasus Project showed that military-grade spyware made by the firm NSO Group had been used against more than three hundred Indian mobile numbers. Those numbers belong to journalists, opposition politicians, constitutional functionaries, and activists. Unlike telephone tapping Pegasus takes full control of the target device, pulls data that is already stored and secretly turns on the camera and microphone. Pegasus becomes a tool for hidden watching. This paper argues that this activity is completely outside India's surveillance laws and therefore is unauthorized access under Section 66 of the Information Technology Act 2000, regardless of who used it. By looking at the Supreme Court decision in Manohar Lal Sharma v Union of India, the paper shows how the scandal reveals problems with Articles 14, 19(1)(a), 21, 32 and 226. It places India's reaction in context and points out the gaps in law – especially the lack of a rule that covers state hacking and the broad national-security exemption in the Digital Personal Data Protection Act 2023, which are still open. The paper ends by saying that the Pegasus scandal is not about one piece of technology; it is a test of whether executive power in India is truly, not just apparently, limited by the Constitution.

Keywords: Pegasus spyware, NSO Group, to privacy Article 21 mass surveillance, K.S. Puttaswamy, Manohar Lal Sharma, Information Technology Act 2000 chilling effect, proportionality.

I. INTRODUCTION

- Surveillance has always been an instrument of statecraft, but the nature of that instrument has changed fundamentally in the digital era. Where traditional surveillance required physical proximity, targeted one person at a time, and left detectable traces,

ISSN: 2582-6433

modern spyware operates remotely, at scale, and, crucially, invisibly. Pegasus, developed by the Israeli firm NSO Group Technologies, represents the most sophisticated iteration of this shift: a surveillance platform capable of converting an ordinary smartphone into a total monitoring device without the owner's knowledge, consent, or any visible trace of compromise.

- The name is drawn, deliberately, from Greek mythology, the winged horse that could travel unseen wherever no mortal could follow. The metaphor captures the technology's essential character: it enters a device silently, disguised as something innocuous, and grants its operator what amounts to a god's-eye view of the target's life. NSO Group has consistently maintained that Pegasus is licensed exclusively to vetted government agencies for counterterrorism and serious crime investigation, with each foreign sale requiring approval of the Israeli Ministry of Defense. Independent forensic investigation, however, has repeatedly documented its use against journalists, human rights defenders, political opponents and even heads of state, a gap between stated purpose and documented use that lies at the heart of the global controversy surrounding the company.
- In India, the controversy crystallised in July 2021 when the Pegasus Project, a collaborative investigation coordinated by Forbidden Stories and involving over eighty journalists across seventeen media organisations in ten countries, revealed that more than three hundred Indian mobile numbers appeared on a leaked list of surveillance targets. *The Wire* served as the Indian partner publication.[1] The list included the Leader of the Opposition, a sitting Union Cabinet Minister, an Election Commissioner, a Supreme Court staff member who had accused the then Chief Justice of India of sexual harassment, and the founding editor of the very publication that broke the story.
- This paper proceeds in three broad movements. It first examines the technical architecture of Pegasus and why that architecture places it beyond the reach of India's interception statutes. It then analyses the constitutional violations the scandal discloses, before turning to the Supreme Court's response in *Manohar Lal Sharma* and the legislative gaps that remain despite that intervention.

[1] The Wire, 'Project Pegasus' (India investigation series, July 2021).

ISSN: 2582-6433

II. THE ARCHITECTURE OF PEGASUS: WHY IT IS NOT "INTERCEPTION"

Understanding why Pegasus escapes India's existing surveillance law requires understanding what it technically does, because the entire statutory scheme of the *Indian Telegraph Act, 1885* and the *Information Technology Act 2000,* is built around the concept of *interception: the* capture of a communication as it passes between two points on a network.[2] Pegasus does not intercept communication in this sense. It occupies the device itself.

A. Evolution of Infection Vectors

- Pegasus's infection methods have evolved across three broad generations. The first generation (2016) relied on spear-phishing: a malicious link sent by SMS or email which, once clicked, exploited vulnerabilities in the browser or operating system. This method required user interaction and was, comparatively, detectable by a technically alert target. The second generation (2019) dispensed with this requirement altogether, exploiting a buffer-overflow vulnerability in WhatsApp's video-call function so that an incoming call, even one never answered, was sufficient to infect the device, with the call record automatically deleted to erase any trace.[3]
- The third generation, styled FORCEDENTRY (2019–2021), exploited Apple's iMessage through a malformed file disguised as an image, requiring no interaction whatsoever; Apple patched the underlying vulnerability in iOS 14.8 after disclosure by Amnesty International.[4] A fourth method requires no digital network interaction at all: installation via a wireless transceiver placed in physical proximity to the target device, demonstrating that even air-gapping a device provides no complete protection against state-level capability.
- This progression carries a specific legal significance. Where infection requires no user interaction whatsoever, the state cannot argue that the victim failed to take reasonable precautions; responsibility for the intrusion rests entirely with the deploying agency. Compounding this, NSO Group maintains multiple infection vectors simultaneously, so that patching one vulnerability, WhatsApp's, or Apple's, does not neutralise the threat, since an alternative vector from the arsenal can simply be deployed instead.

[2] Indian Telegraph Act 1885, s 5(2); Information Technology Act 2000, s 69.
[3] This attack formed the basis of WhatsApp's civil suit against NSO Group in the United States: see discussion in Part II(C) below.
[4] Amnesty International, Forensic Methodology Report: How to Catch NSO Group's Pegasus (Amnesty International Security Lab, 18 July 2021).

ISSN: 2582-6433

B. The Payload and the PATN

- Once installed, Pegasus's payload provides what can only be described as total device occupation: real-time interception of communications across every major platform, including end-to-end encrypted applications such as Signal, before encryption is even applied; covert, indicator-free activation of the microphone and camera; continuous GPS tracking; and wholesale extraction of stored photographs, passwords, banking credentials and browsing history. Data is transmitted to the operator through the Pegasus Anonymizing Transmission Network (PATN), a command-and-control infrastructure comprising up to five hundred domain names across multiple jurisdictions, engineered with randomised subdomains and non-standard ports specifically to defeat conventional security scanning.
- The spyware is programmed to self-destruct if it fails to contact its PATN server for sixty consecutive days, ensuring that in the ordinary course no forensic trace of its presence survives, which is precisely why the Supreme Court-appointed technical committee, discussed in Part VI below, was unable conclusively to confirm Pegasus's presence on several compromised devices it examined.
- The consequence, in strict legal terms, is that none of this conduct is interception. Reading data at rest, activating a microphone, and photographing a target through a device's own camera are not communications passing between two points; they are unauthorized access to, and manipulation of, a computer resource within the meaning of section 43 of the Information Technology Act 2000, and therefore an offence under section 66.[5] No provision of the IT Act or the Telegraph Act exempts a government agency from this characterization, and the Internet Freedom Foundation has stated the position categorically: no power to hack the phones of Indian citizens exists under Indian law.

C. The Hummingbird Litigation and the December 2024 Judgment

- The clearest judicial confirmation of this characterization comes not from an Indian court but from the United States. WhatsApp (Meta) alleged in federal litigation that NSO Group had reverse-engineered WhatsApp's proprietary source code to build three custom attack vectors, codenamed 'Heaven', 'Eden' and 'Erised', marketed together as the 'Hummingbird' hacking suite. In December 2024, a US federal court held that this

[5] Information Technology Act 2000, ss 43, 66.

ISSN: 2582-6433

conduct violated the *Computer Fraud and Abuse Act 1986*.[6]

- The judgment is significant for Indian law because it confirms, in a considered judicial forum, that Pegasus deployment is criminal hacking irrespective of whether the deploying party is a sovereign government. There is no principled basis on which the same conduct, directed at Indian citizens, could be treated as anything other than an offence under section 66 of the IT Act 2000.

III. THE PEGASUS PROJECT: EXPOSURE AND INDIAN TARGETS

- The scandal did not emerge through parliamentary inquiry, governmental disclosure, or an internal whistleblower. It emerged from a leaked database of approximately fifty thousand phone numbers that NSO Group's government clients had allegedly identified as surveillance targets, investigated through a rigorous two-stage verification methodology: forensic examination of sixty-seven suspected devices by Amnesty International's Security Lab, of which twenty-three were confirmed infected and fourteen showed signs of attempted penetration, with all findings independently peer-reviewed by the Citizen Lab at the University of Toronto.[7]
- It was this dual verification, independent forensic analysis confirmed by independent peer review, that led the Supreme Court to treat the investigation's findings as credible enough to warrant judicial examination. The presence of a number on the leaked database did not, by itself, prove infection; it established only that the number had been designated a target.
- But the identity of those targeted is constitutionally significant. Rahul Gandhi, then Leader of the Opposition, had two phones reportedly targeted, later stating publicly that 'all my phones are tapped'. Ashwini Vaishnaw, the Union Cabinet Minister for Electronics and IT, was targeted less than three weeks before assuming that very office. Siddharth Varadarajan, founder and editor of *The Wire*, was targeted in circumstances strongly suggestive of an attempt to identify journalistic sources. A Supreme Court staff member who had filed a sexual harassment complaint against the then Chief Justice of India appeared on the list, as did the Election Commissioner and the student activist Umar Khalid, added over a year before his arrest under the Unlawful Activities

[6] Judgment of the US District Court for the Northern District of California in WhatsApp Inc v NSO Group Technologies Ltd (December 2024), finding liability under the Computer Fraud and Abuse Act 1986 (US).
[7] Amnesty International (n 8); see also Citizen Lab, University of Toronto, independent peer-review of Amnesty International Security Lab forensic findings (2021).

ISSN: 2582-6433

(Prevention) Act.

- The most troubling dimension of the scandal is its alleged intersection with the criminal justice system in the Bhima Koregaon case, where lawyers, academics and tribal-rights activists face prosecution on terrorism charges arising from violence near the Bhima Koregaon war memorial in January 2018. Arsenal Consulting, an independent US-based digital forensics firm, found that fabricated incriminating files had been remotely planted on the computers of at least two accused before being 'discovered' and used to justify arrest and prolonged detention.[8]
- Stan Swamy, an eighty-three-year-old Jesuit priest and tribal rights activist whose number appeared on the Pegasus target list, was arrested under the same statute in October 2020 on the basis of evidence whose integrity is now credibly in question, and died in judicial custody in July 2021 while awaiting bail on medical grounds. Taken together, the surveillance and evidence-planting revelations transform Pegasus from a privacy controversy into a potential instrument of wrongful, and in this instance fatal, deprivation of liberty.

IV. THE ABSENCE OF STATUTORY AUTHORISATION

- The foundational legal proposition in any assessment of Pegasus is that no law in India authorises its deployment against Indian citizens. This is not a procedural gap; it is a constitutional void. The Union Government, when confronted with the allegations, pointed to two existing statutes as potential justification, section 5(2) of the *Indian Telegraph Act 1885* and section 69 of the *Information Technology Act 2000,* but neither can bear the weight placed on it.
- Section 5(2) of the Telegraph Act authorises interception of telephone calls and messages on grounds of sovereignty, security of the state, public order or prevention of crime, subject to prior written authorisation from the Union or State Home Secretary, a maximum duration of sixty days extendable to one hundred and eighty, and review by a Ministerial Review Committee. Section 69 of the IT Act, similarly, authorises interception, monitoring and decryption of information transmitted through computer resources, governed by the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.[9] Both provisions share a common

[8] Findings of Arsenal Consulting, independent forensic analysis of digital devices of accused persons in the Bhima Koregaon case, cited in Indian press reporting, 2021.
[9] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information)

ISSN: 2582-6433

limitation: they authorise access to communications in transmission. Neither authorises accessing data at rest, activating a microphone or camera, or extracting content that has already been received and stored, none of which is, in ordinary legal usage, interception at all.

- Section 66 of the IT Act 2000, by contrast, criminalises precisely this conduct: any person who dishonestly or fraudulently commits an act referred to in section 43, including unauthorised access to, or modification of, computer data, is punishable with imprisonment of up to three years, a fine of up to five lakh rupees, or both. Critically, there is no exemption in section 66, or anywhere else in the Act, for government agencies. A state agency that hacks into a citizen's phone commits, on the plain text of the statute, the same offence as a private individual who does so.

V. CONSTITUTIONAL VIOLATIONS: ARTICLES 14, 19, 21, 32 AND 226

A. Article 21, The Right to Privacy and the Puttaswamy Test

The right to privacy was unanimously recognised as a fundamental right under Article 21 by a nine-judge bench of the Supreme Court in *K.S. Puttaswamy v Union of India*,[10] which held that privacy is 'a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21'. The judgment laid down a three-fold test that any state action invading privacy must satisfy: legality, requiring an authorising law; legitimate aim, requiring a valid state objective; and proportionality, requiring a rational nexus between the objective pursued and the means employed.

Pegasus fails all three limbs simultaneously. It fails legality because, as demonstrated in Part IV, no statute authorises hacking. It fails legitimate aim because the deployment of state-exclusive surveillance technology against political opponents, journalists and constitutional functionaries cannot be characterised as pursuing a legitimate security objective. And it fails proportionality decisively: even assuming a genuine security concern, the interception powers already available under section 5(2) of the Telegraph Act would be entirely sufficient to monitor a specific threat, whereas Pegasus provides indiscriminate, total access to an individual's stored data, camera and microphone, a degree of intrusion wholly disproportionate to any conceivable targeted objective. This is not a marginal constitutional failure but a complete one.

Rules 2009.

[10] (2017) 10 SCC 1.

ISSN: 2582-6433

Two earlier decisions anticipated this framework. In *Kharak Singh v State of Uttar Pradesh*,[11] the Court held that continuous and pervasive police surveillance, including domiciliary visits, was incompatible with the personal liberty guaranteed by Article 21, the earliest recognition that pervasive state watching is itself a constitutional harm, independent of any communication actually intercepted. In *Govind v State of Madhya Pradesh*, [12]the Court recognised privacy as a penumbral right implicit in Article 21, while acknowledging that reasonable, defined and proportionate restrictions could be justified, a qualification that Pegasus, being neither defined in scope nor proportionate in application, does not satisfy. Guidelines for lawful telephone interception were subsequently laid down in *People's Union for Civil Liberties v Union of India*,[13] which held that even conventional phone tapping is a serious invasion of the right to hold conversations in private under Article 21. Pegasus is categorically more invasive than anything considered in that case, yet was deployed without even the minimal safeguards PUCL required for ordinary interception.

B. Article 19(1)(a), Press Freedom and the Chilling Effect

Freedom of the press is implicit within Article 19(1)(a)'s guarantee of speech and expression, a proposition affirmed in *Maneka Gandhi v Union of India*,[14] where the Court held that democracy is premised on free debate and open discussion, of which the press is an essential vehicle. Surveillance of journalists produces what is termed the chilling effect, self-censorship arising not from actual prosecution but from the mere awareness of being watched, which causes journalists to avoid controversial subjects and, most damagingly, to refuse contact with sensitive sources. In *Anuradha Bhasin v Union of India*,[15] the Court affirmed that there is no justification for allowing a 'Sword of Damocles to hang over the press indefinitely'. Pegasus is precisely such a sword: invisible, total and, absent detection, permanent. Because a journalist's sources will come forward only if confident that their identity can be protected, and because Pegasus exposes every contact and message on a compromised device, the targeting of Siddharth Varadarajan strikes directly at source protection and, through it, at the possibility of accountability journalism itself.

[11] AIR 1963 SC 1295.
[12] (1975) 2 SCC 148.
[13] (1997) 1 SCC 301.
[14] (1978) 1 SCC 248.
[15] (2020) 3 SCC 637.

ISSN: 2582-6433

C. Article 14, Arbitrariness in Selection of Targets

Article 14 guarantees equality before the law and has been interpreted to prohibit state action that is manifestly arbitrary, irrational or capricious without reasonable basis. The deployment of Pegasus against the Leader of the Opposition, a political strategist working for opposition campaigns, a critical newspaper's editor, and an octogenarian tribal-rights priest is difficult to reconcile with any rational security classification. No coherent basis links these individuals as simultaneous threats to national security sufficient to justify deployment of a military-grade intelligence weapon against each of them, rendering the pattern of targeting prima facie arbitrary and discriminatory.

D. Articles 32 and 226, The Silent Destruction of Constitutional Remedy

The most structurally significant, and least discussed, constitutional harm concerns Articles 32 and 226, which guarantee every citizen the right to approach the Supreme Court and the High Courts for enforcement of fundamental rights, a right the Supreme Court has called 'the soul of the Constitution'. The precondition for exercising this right is knowledge that a violation has occurred. Pegasus is engineered specifically to defeat that precondition: its invisibility during operation, its self-destruction after sixty days of inactivity, and its erasure of digital traces are all designed to ensure the target never learns of the intrusion. A right that cannot be known to have been violated cannot, in practice, be enforced, leaving Articles 32 and 226 intact on paper while rendered largely inert in application to this category of harm.

VI. THE SUPREME COURT'S RESPONSE: MANOHAR LAL SHARMA v UNION OF INDIA

- Following the July 2021 revelations, multiple petitions were filed before the Supreme Court under Article 32, the principal petition filed by Advocate Manohar Lal Sharma giving the litigation its name, with further petitions by senior journalists N. Ram and Shashi Kumar, Communist Party of India (Marxist) Member of Parliament John Brittas, and various civil society organisations.
- The petitioners framed the government's position as a binary from which there was no acceptable third option: either the government had itself deployed Pegasus against its own citizens, incurring criminal and constitutional liability, or it had failed to protect Indian citizens from unlawful surveillance by a foreign tool, incurring liability for dereliction of its Article 21 duty. They further argued, relying on *Ram Jethmalani v Union*

ISSN: 2582-6433

of India,[16] that the government is constitutionally barred from adopting an adversarial posture when fundamental rights are at stake and is instead duty-bound to provide full disclosure to the Court. Finally, they invoked the natural justice maxim *nemo judex in causa sua,* no person may be a judge in their own cause, to argue that a government-constituted committee could not credibly investigate the government's own conduct.

- The government, in response, characterised the allegations as 'conjectures and surmises', proposed that a government-constituted committee would suffice, and declined to confirm or deny purchase or deployment of Pegasus on grounds of national security, filing only a 'limited affidavit' to that effect.
- The bench comprising Chief Justice N.V. Ramana, Justice Surya Kant and Justice Hima Kohli delivered its order on 27 October 2021,[17] rejecting the government's position on every ground advanced. The Court held that 'the State does not get a free pass every time the spectre of national security is raised', and that no omnibus prohibition on judicial review can be claimed merely by invoking that phrase. It found the limited affidavit constitutionally insufficient, holding, citing *Ram Jethmalani* directly, that the government was duty-bound under Article 21 to provide full and frank disclosure rather than adopt an adversarial stance.
- It held that a government-constituted probe committee would violate the principle that justice must not only be done but must be seen to be done, applying *nemo judex in causa sua* directly to bar such an arrangement. And it affirmed, in terms tracking *Puttaswamy* and *Anuradha Bhasin*, that citizens enjoy a reasonable expectation of privacy under Article 21 and that surveillance of journalists produces a chilling effect on Article 19(1)(a) freedoms.
- Exercising its power under Article 32, the Court constituted an independent technical committee under the judicial supervision of retired Justice R.V. Raveendran, supported by three technical experts drawn from the National Forensic Sciences University, Amrita Vishwa Vidyapeetham University and the Indian Institute of Technology Bombay. On 25 August 2022, outgoing Chief Justice Ramana reported that the committee had examined twenty-nine phones and found malware on five, but, precisely because of Pegasus's self-destruction mechanism, could not conclusively confirm the malware's identity as Pegasus.
- The most consequential finding of the entire exercise was procedural rather than

[16] (2011) 8 SCC 1.
[17] Manohar Lal Sharma v Union of India 2021 SCC OnLine SC 985.

ISSN: 2582-6433

technical: the Union Government refused to provide any information to the committee, confirming neither purchase nor deployment, which meant the committee could examine device-level forensic evidence but could never investigate the underlying deployment decision. As of these notes, the case remains relisted for hearing, the committee's full report remains unpublished, no official has been held accountable, and no legislation has been enacted to close the gap the scandal exposed.

VII. A COMPARATIVE PERSPECTIVE

- The contrast between India's institutional response and that of comparable democracies is instructive. France launched three separate judicial inquiries into the targeting of French citizens and officials, including President Emmanuel Macron, whose number appeared on the target list. The European Parliament constituted a dedicated Special Committee on the use of Pegasus and equivalent spyware (the PEGA Committee), producing detailed cross-jurisdictional findings and legislative recommendations.[18]
- Mexico's national anti-corruption investigator and Supreme Court both took public cognisance of surveillance against civil society and lawyers. Even Israel, the country in which NSO Group is headquartered and whose Ministry of Defence must approve every export sale, established an internal commission to examine the adequacy of its own export-control regime.
- he United States Department of Commerce placed NSO Group on its Entity List, restricting its access to US technology supply chains on the ground of 'malicious cyber activities', and, as discussed above, a US federal court found the company liable under the Computer Fraud and Abuse Act 1986.
- Against this backdrop, India's response, a refusal to confirm or deny purchase, a limited affidavit, and non-cooperation with its own Supreme Court's technical committee, stands out not for the absence of allegations, which every jurisdiction faced, but for the near-total absence of institutional follow-through.

  The comparison suggests that the difference lies less in the severity of the underlying facts than in the willingness of the executive to submit to independent scrutiny once those facts came to light.

[18] European Parliament, Report of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee, 2023).

ISSN: 2582-6433

VIII. LEGISLATIVE GAPS AND RECOMMENDATIONS

- Several structural deficiencies in Indian law remain unaddressed by the Pegasus litigation. First, India has no legislation specifically governing state hacking, unlike jurisdictions such as the United Kingdom, whose *Investigatory Powers Act 2016* expressly regulates 'equipment interference' by intelligence agencies, or Germany, whose federal intelligence statute addresses similar capabilities with defined authorisation and oversight requirements.
- Second, the *Digital Personal Data Protection Act 2023*, India's principal data protection statute, contains a sweeping national security exemption that removes state surveillance from its scope altogether, meaning the gap Pegasus exposed is not closed by the very law enacted after the scandal.[19]
- Third, India's surveillance authorisation remains executive rather than judicial: both section 5(2) of the Telegraph Act and section 69 of the IT Act vest approval in the Home Secretary, the same executive branch that benefits from the intelligence gathered, creating a structural conflict of interest that judicial pre-authorisation, familiar in many mature democracies, is designed to avoid.
- Fourth, Indian law imposes no obligation to notify a surveillance subject even after the fact, foreclosing the delayed-but-real opportunity for redress that notification requirements in other systems provide.
- Addressing these gaps would require, at minimum: a standalone statute defining and regulating the circumstances, if any, in which state hacking tools may lawfully be deployed; substitution of executive authorisation with judicial pre-authorisation for any surveillance measure that goes beyond conventional interception; a statutory notification requirement, delayed where necessary to protect an ongoing investigation but not indefinitely withheld; and removal, or at minimum narrowing, of the blanket national security exemption in the Digital Personal Data Protection Act 2023 so that it does not operate as a total carve-out for the very category of state conduct most in need of oversight. Justice Raveendran's own recommendations to the Supreme Court, a dedicated Special Investigation Agency for cybercrime and a citizen grievance mechanism for suspected unlawful surveillance, remain a useful, and as yet unimplemented, starting point.

[19] Digital Personal Data Protection Act 2023, s 17(2)(a) (exemption for processing in the interests of the sovereignty and integrity of India, security of the state, and related grounds).

ISSN: 2582-6433

IX. CONCLUSION

The Pegasus scandal is, at one level, a story about a single piece of software. At a deeper level, it is a test of whether India's constitutional guarantees constrain executive power even when no statute expressly requires it to submit to that constraint, and even when the violation is engineered specifically to remain undetected. The Supreme Court's intervention in *Manohar Lal Sharma* affirmed, correctly and unambiguously, that national security is not a talismanic phrase capable of extinguishing judicial review, that privacy under Article 21 is not subordinate to executive convenience, and that surveillance of the press cannot be tolerated indefinitely under Article 19(1)(a). Yet the Union Government's refusal to confirm or deny even the fact of purchase, sustained through every stage of the litigation, including before the Court's own technical committee, demonstrates that a constitutional guarantee, however clearly stated, is only as strong as the good faith of the institution asked to honour it.

Daniel Solove has argued persuasively that the framing of privacy and security as opposing values is a false dilemma: privacy can be fully protected without sacrificing legitimate security interests, provided surveillance operates within a framework of oversight, proportionality and accountability.[20] On every element of that framework, judicial authorisation, defined scope, accountability for use, and a meaningful mechanism of challenge, Pegasus fails completely. As the underlying technology grows only more powerful and more accessible, the legislative, institutional and judicial choices India makes in the aftermath of this scandal will determine whether constitutional democracy, and not merely constitutional text, survives the digital transformation of the state's surveillance capacity.

BIBLIOGRAPHY TABLE OF CASES

S. No.	Case Name	Citation
1	*Kharak Singh v State of Uttar Pradesh*	AIR 1963 SC 1295
2	*Govind v State of Madhya Pradesh*	(1975) 2 SCC 148
3	*Maneka Gandhi v Union of India*	(1978) 1 SCC 248
4	*People's Union for Civil Liberties v Union of India*	(1997) 1 SCC 301
5	*Ram Jethmalani v Union of India*	(2011) 8 SCC 1
6	*K.S. Puttaswamy v Union of India*	(2017) 10 SCC 1

[20] Daniel J Solove, Nothing to Hide: The False Trade-off between Privacy and Security (Yale University Press 2011).

ISSN: 2582-6433

7	*Anuradha Bhasin v Union of India*	(2020) 3 SCC 637
8	*Manohar Lal Sharma v Union of India*	2021 SCC OnLine SC 985
9	*WhatsApp Inc v NSO Group Technologies Ltd*	US District Court, Northern District of California, judgment of December 2024

TABLE OF STATUTES AND LEGISLATIVE INSTRUMENTS

S. No.	Instrument	Relevant Provision(s)
1	Indian Telegraph Act 1885	s 5(2)
2	Information Technology Act 2000	ss 43, 66, 69
3	Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009	—
4	Digital Personal Data Protection Act 2023	s 17(2)(a)
5	Computer Fraud and Abuse Act 1986 (US)	—
6	Investigatory Powers Act 2016 (UK)	(comparative reference)

BOOKS

- Solove D J, *Nothing to Hide: The False Trade-off between Privacy and Security* (Yale University Press 2011)

REPORTS

- Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus* (Amnesty International Security Lab, 18 July 2021)
- Citizen Lab, University of Toronto, *Independent Peer Review of Amnesty International Security Lab Forensic Findings* (2021)
- European Parliament, *Report of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware* (PEGA Committee, 2023)
- Arsenal Consulting, *Forensic Analysis of Digital Devices of Accused Persons in the Bhima Koregaon Case* (2021)

NEWS AND JOURNALISTIC SOURCES

- The Wire, 'Project Pegasus' (India investigation series, July 2021)