Centre for Knowledge Sovereignty ®

Grand Guruz 2025

Table of Contents

Grand Guruz - Mentorship for Nation Building

Centre for Knowledge Sovereignty®

Concept Note

Context and Strategic Need

India is steadily shaping its identity as a digital-first economy and a global knowledge leader. Yet, as Technology, National Security, and Governance grow increasingly complex, the need for a new generation of Policy Thinkers and Researchers has never been more urgent.

While our universities provide a strong academic foundation, there remains a clear gap between what is taught in classrooms and the practical realities of policymaking. Students rarely get the opportunity to engage directly with experts who have navigated the challenges of Digital Sovereignty, Cybersecurity, Defence, or Regulatory frameworks. This gap leaves a vacuum at a time when India requires well-prepared minds to craft policies that safeguard its Sovereign interests.

Recognizing this need, the Centre for Knowledge Sovereignty (CKS) has conceptualized Grand Guruz : a mentorship-driven research initiative that bridges this gap. It offers a structured platform where seasoned policy veterans engage with bright postgraduate students, ensuring knowledge is not only generated but also transmitted through meaningful dialogue and mentorship.

Program Overview

At its core, Grand Guruz is a mentorship and research program designed to strengthen India's intellectual ecosystem. It facilitates a rare dialogue between two generations: Senior Mentors who bring decades of strategic experience, and young scholars who represent the energy and curiosity of India's future.

The program is built around three pillars:

- Mentorship: Direct, guided engagement with experts.
- Research: Production of original, actionable policy outputs.
- Capacity Building: Equipping students with the tools of policy design, strategic thinking, and effective communication.

Through this model, Grand Guruz aspires to create a cadre of Sovereign-minded professionals who can contribute meaningfully to India's journey as a secure, inclusive, and innovation-led nation.

Objectives

The initiative is guided by four core objectives:

- Mentorship for Impact – Enable students to learn directly from policy leaders who have shaped India's strategic narrative.
- Strategic Research – Encourage the creation of high-quality, policy-relevant research outputs.
- Capacity Building – Strengthen critical skills in research methodology, analysis, and communication.
- Fostering Sovereign Thought Leadership – Cultivate young minds committed to advancing India's national interest in the digital era.

Structure and Modality

The program follows a clear, outcome-oriented structure:

- Participants: Postgraduate students carefully chosen from premier institutions.
- Mentorship Model: Each student is paired with a 'Grand Guru' - a senior expert from

domains such as Cybersecurity, Governance, Defence, Technology, and Law.

- Engagement: A 4–6 week cycle with weekly sessions, mid-term reviews, and a final assessment.
- Deliverables: Each mentee produces an original research paper or policy brief, presents it before an expert panel, and may see it disseminated through CKS and its partners.

Pilot Phase (June–July 2025)

The first edition of Grand Guruz was launched with three postgraduate scholars from OP Jindal Global University, each paired with distinguished mentors of national stature:

- Lt. Gen. Vinod G. Khandare, PVSM, AVSM, SM (Retd.) – Fmr Principal Advisor, Ministry of Defence, Covernment of India, For Military Advisor NSCS, Fmr DG Defence Intelligence Agency
- Lt. Gen. Sanjay Kulkarni, PVSM, AVSM, SC, SM, VSM (Retd.) – Fmr DG Infantry and Siachen Pioneer
- Shri Agendra Kumar – Managing Director, Esri India
- Dr. G. Shreekumar Menon, IRS (Rtd.) Ph.D (Narcotics) – Former Director General NACEN/NACIN

Key activities included one-on-one mentorship sessions, structured reviews, and the development of policy-oriented research papers on themes such as data governance, digital sovereignty, and digital public infrastructure.

To acknowledge their academic effort, each student received an honorarium upon completing their paper and presentation. Beyond the financial reward, students walked away with something far more valuable: direct insights from national leaders and a deeper understanding of India's policy ecosystem.

Strategic Roadmap

Building on the success of the pilot, CKS envisions Grand Guruz as a scalable program with national relevance. The roadmap includes:

- Cohort Expansion – Growing to 10–15 students per cycle with participation from multiple institutions.
- Thematic Clusters – Focused research on AI governance, digital competition, cybersecurity, information warfare, and data localization.
- Annual Symposium – A "Grand Guruz Research Colloquium" where students present findings before ministries, think tanks, and industry leaders.
- Alumni Network – Creating a community of Grand Guruz alumni for long-term mentorship and collaboration.

Strategic Relevance

The Grand Guruz initiative is closely aligned with India's national priorities, including Digital India, the National Cybersecurity Strategy, the DPDP Act, Atmanirbhar Bharat, Viksit Bharat 2047, and the Digital Public Infrastructure Blueprint.

By nurturing young researchers and fostering intergenerational knowledge exchange, Grand Guruz is not just a program - it is a movement to strengthen India's knowledge sovereignty. It ensures that the wisdom of experience meets the curiosity of youth, producing policy leaders capable of navigating the complexities of a digital century.

In the words of

Shri Vinit Goenka

Secretary, Centre for Knowledge Sovereignty

"Mentorship is not merely the transfer of knowledge, it is the shaping of vision and the cultivation of purpose."

At the Centre for Knowledge Sovereignty, we hold a firm belief that the strength of a nation lies not only in its infrastructure or institutions but also in the intellectual capital of its people. Knowledge, when guided with wisdom and purpose, has the power to transform individuals and, through them, societies. This is the guiding principle behind the Grand Guruz Program, an initiative that exemplifies our commitment to nurturing future leaders in Technology, Policy, and Governance.

Mentorship, in its truest sense, is about building character as much as competence. It is about enabling young minds to think beyond the immediate, to question assumptions, and to develop perspectives that are both innovative and rooted in ethical responsibility. The Grand Guruz Program is not designed merely as an academic exercise. Rather, it is a platform where seasoned mentors engage directly with mentees, challenging them to explore complex policy issues, encouraging critical inquiry, and instilling a deeper appreciation of the responsibilities that come with knowledge.

India today stands at a historic juncture. The convergence of Data, Digital Infrastructure, and National Interest presents both unparalleled opportunities and significant challenges. The way we navigate this convergence will determine the trajectory of our nation in the decades ahead. In such a context, the role of young thinkers becomes indispensable. They must not only master the tools of technology and governance but also understand the larger implications for sovereignty, security, and societal well-being.

The Grand Guruz Program seeks to prepare them for precisely this role. By fostering dialogue between experienced mentors and committed mentees, we are creating a fertile space for intellectual growth that transcends textbooks and classrooms. It is in these conversations, sometimes challenging, sometimes inspirational, that mentees begin to connect the dots between theory and practice, between personal ambition and national responsibility.

I am particularly heartened to see how this year’s mentees have embraced the complexity of their tasks. The research papers they have produced are not only rigorous in analysis but also forward-looking in their vision. They reflect an awareness of global trends, an understanding of India’s unique position, and a commitment to crafting solutions that balance innovation with regulation and national interest. This is no small achievement, and it speaks to the potential that guided mentorship can unlock.

However, one program alone cannot suffice. If India is to truly harness its demographic dividend and secure its place as a leader in the digital century, initiatives such as the Grand Guruz Program must be scaled and replicated across institutions and disciplines. We need a steady pipeline of informed, ethical, and visionary individuals who can shape narratives, design frameworks, and safeguard National Sovereignty.

Let us, therefore, see the Grand Guruz Program not as an isolated initiative, but as the spark that lights many more journeys of learning, leadership, and service to the nation. It is not the infrastructure we build or the technologies we adopt that will define India’s future, it is the people we nurture, the values we inculcate, and the vision we shape.

From the Desk of

Prof. Meenakshi Tomar

Vice-Dean, Office of Career Services
O.P. Jindal Global University

It gives me immense pleasure to witness the success of the Grand Guruz Program organized by the Centre for Knowledge Sovereignty (CKS). The initiative has created a meaningful space for mentorship, dialogue, and knowledge-sharing.

For our students, this program has been particularly enriching. The opportunity to learn directly from accomplished mentors, to engage with practical insights, and to reflect upon their own aspirations has added immense value to their academic journey. Experiences such as these help students bridge the gap between classroom learning and real-world practice, preparing them to step confidently into their future roles as responsible professionals and changemakers.

At O.P. Jindal Global University, we remain committed to fostering environment where students can interact with thought leaders, develop critical perspectives, and strengthen their ability to contribute meaningfully to society. The Grand Guruz Program resonates strongly with this vision, and we are proud to have been part of it.

I extend my heartfelt congratulations to the entire CKS team, the mentors, and most importantly, the students, whose enthusiasm, commitment, and active participation brought this initiative to life. I am confident that the learnings from this program will leave a lasting impact on them and will inspire many more such collaborations in the future.

Guiding Thoughts

by Esteemed Guruz of the Program

Next ▶

Mentorship is the Cornerstone of Progress, Innovation & Leadership

Lt. Gen. Sanjay Kulkarni, PVSM, AVSM, SC, SM, VSM (Retd.)

Fmr Director General Infantry and Siachen Pioneer

As I look upon my experience as a mentor for the Grand Guruz Program , guiding the talented individuals, I am filled with a deep sense of pride, gratitude, and reflection. This journey has been profoundly enriching, marked by moments of learning, growth, and transformation for both the mentees and myself.

Mentorship is the cornerstone of progress, innovation, and leadership. The Grand Guruz program exemplifies this spirit by bridging the gap between experience and aspiration. By pairing accomplished Guruz with aspiring students, it fosters a culture of guidance, inspiration, and mutual enrichment. I have come to realize that mentorship is not merely about sharing knowledge, it is about creating spaces where young minds can explore their passions, overcome challenges, and pursue their aspirations with confidence.

One of the most rewarding aspects of this journey has been the opportunity to give back to the learning community and positively impact the next generation of leaders. Witnessing our interns grow and flourish, personally and professionally, has been truly fulfilling. As I reflect, I am reminded that mentorship creates a legacy that transcends generations. The lessons shared and experiences exchanged will remain with these young leaders long after their internship concludes. I have no doubt they will go on to leave their own mark on society, and I feel honoured to have played a role in their journey.

I extend my heartfelt gratitude to each of our interns for placing their trust in us. Their enthusiasm and dedication have made this experience truly memorable. Looking ahead, I am excited to witness the impact our mentees will make in their respective fields, carrying forward the lessons they have learned to create meaningful change.

Together, let us continue to empower the next generation of leaders. Through the Grand Guruz initiative, we can ignite young minds, cultivate leadership, and inspire purpose, shaping a future where India’s demographic advantage translates into progress, prosperity, and national strength.

The Relevance of Technology for Nation

Lt. Gen. Vinod Khandare, PVSM, AVSM, SM (Retd.)
Fmr Principal Advisor, Ministry of Defence, GOI
Fmr Military Advisor NSCS
Fmr Director General Defence Intelligence Agency

The relevance of technology in current-day life for individuals and nations is extremely important. In my opinion, its applications are already in use, both in the civil and National Security domains. What needs to be proliferated now are the knowledge, skills and wisdom to understand these technologies, their multiple applications, and the strategic leverages that accrue once we master them. The stakeholders in this journey are all citizens, who must contribute to ensuring that the nation grows strong in all fields of comprehensive national power. It is a bounden duty of every citizen to contribute selflessly to ensure Comprehensive National Security. We must contribute to the National Vision of VIKSIT BHARAT 2047. A developed nation needs to keep itself secure, therefore it is imperative to be SURAKSHIT BHARAT alongside the growth vision, goals and trajectory.

Towards achieving these goals, the Grand Guruz Program of CKS was a grand success. It was a privilege to be one of the Grand Guruz, and in this capacity I had the opportunity to mentor P.V. Vineet in his important research work on "State Exemptions and Surveillance Overreach: Challenges and Reform Pathways under India's Digital Personal Data Protection Act." His perseverance and focus reflect the seriousness with which the younger generation is engaging in critical national debates.

It is also most opportune to mention the vision and perseverance of Shri Vinit Goenka in conceptualising this program and activating it with the help of his excellent team at CKS. The beneficiaries of this unique program would do well to continue with their pursuit of rigorous research and apply their theoretical knowledge to Indian conditions and challenges. Customised solutions for our national and regional contexts will be most easily accepted, despite the global dominance by the Super Powers and the developed world. We need to grow our human capital through knowledge search, skilling, and hunger to ascend to leading positions globally.

I wish all the successful participants a bright future and I thank the organisers for their painstaking efforts taken for a national cause.

Jai Hind !!!!!

Youth Needs to be Guided for Success and Expertise in Life

Dr. G. Shreekumar Menon, IRS (Rtd.) Ph.D (Narcotics)

Former Director General National Academy of Customs, Indirect Taxes and Narcotics/NACEN

Grand Guruz concept is a unique project initiated by the Centre for Knowledge Security (CKS) as to why youth needs to be guided to follow a particular path for success and expertise in life. It is argued that lack of role modelling and mentoring projects are possible reasons behind youth disempowerment. This exploratory project by CKS was designed to provide effective mentoring that can lead to greater career success, and increased opportunities. It's however important to remember that mentoring is not a magic wand that automatically confers success. Effective mentoring takes effort, and creating successful mentoring relationships requires specific skills, sensibilities, and structure from both the mentor and the mentee.

I am thankful to CKS for providing me a coveted opportunity to take on the role of a mentor, in a unique legal study, that studied the reasons for investigatory lapses in narcotics related case proceedings, resulting in acquittal of offenders. Good mentors will be excited to share their knowledge and be willing to explore the possibility that the mentee may have answers that skipped from the mentor's attention.

Officials at CKS took great pains to design the alliance and discuss the structure of the relationship. Special attention was stressed on:

1. Confidentiality: What's shareable and what isn't?
2. Focus: What are the parameters of the project? What's in and out of bounds?
3. Feedback: What are the expectations around giving and receiving feedback?
4. Goals and accountability: What would mentor and mentee want from this experience?

In narcotics cases the workload is often mountainous, it takes a team to get everything done in a manner that meets and exceeds judiciary's expectations. The more senior lawyers on the team count on juniors to help pay attention to the minute details. The present limited study has reflected on the need for collaboration between legal authorities, policymakers, and civil society to address drug abuse cases, emphasizing the importance of timely access to justice, as delays can be a social cost unaffordable for any society. The issue of pending cases in India is a nationwide problem, exacerbated by overburdened courts, inordinate delays in the legal process, and unsatisfactory case management, especially those related to drug trafficking. Easy acquittals relying on tardy investigations, inadequate expertise in appreciating the legal requirements spelt out in the NDPS Act 1985, and the jurisdiction of Special Courts, are issues needing serious attention. Young lawyers and students of law need dedication, flexibility, and, importantly, a steadfast desire to continually grow to stand out in a field as competitive as narcotics related litigation. It is hoped that this CKS initiative will be the first of a series in mentoring budding lawyers and grooming them for a global career.

The Landscape of Geospatial Policy in India is Rapidly Envolving

Shri Agendra Kumar

Managing Director

ESRI India

Mentoring an undergraduate student delving into the intricate world of Indian geospatial policies has been an intellectually rewarding and personally enriching experience. The landscape of geospatial policy in India is rapidly evolving, marked by government initiatives to liberalize data access, while simultaneously grappling with concerns around privacy, security, and sovereignty. Guiding a student through this complex terrain required a balance of theoretical grounding and practical perspective.

The journey began with introducing the student to the historical context of geospatial data governance in India, the legacy of restrictive mapping laws and the shift towards open data with the 2021 guidelines. Our discussions frequently revolved around not just the promise of democratized geospatial information for innovation and economic growth, but also the potential pitfalls: Regulatory Ambiguity, fear of Data misuse, and Government controls.

One of the primary challenges was helping the student navigate the patchwork of legislation and policy frameworks, distinguishing between what is legally permissible and what is technically feasible. It became clear that there was a pressing need for clarity and capacity-building, both among policymakers and end-users. Throughout, I encouraged the student to critically assess policy documents of India and a few other countries, fostering an attitude of healthy skepticism and an appreciation for the nuanced impacts, positive and negative, of policy shifts on governance, commerce, and society.

Overall, mentoring in this field meant not only sharing academic insights but also instilling a sense of ethical responsibility. Watching the student develop analytical independence and an informed perspective on India's geospatial future was the most gratifying part of this mentoring experience.

From The Secretariat

Next ▶

Mentorship Creates a Legacy that Transcends Generations

Dr. Vijay Rai
Distinguished Fellow
Centre for Knowledge Sovereignty

As I look back on my experience as a mentor for the Grand Guruz Program , guiding the talented individuals who interned with us, I am filled with a deep sense of pride, gratitude, and reflection. This journey has been profoundly enriching, marked by moments of learning, growth, and transformation for both the interns and myself.

Mentorship is the cornerstone of progress, innovation, and leadership. The Grand Guruz program exemplifies this spirit by bridging the gap between experience and aspiration. By pairing accomplished Guruz with aspiring students, it fosters a culture of guidance, inspiration, and mutual enrichment. I have come to realize that mentorship is not merely about sharing knowledge, it is about creating spaces where young minds can explore their passions, overcome challenges, and pursue their aspirations with confidence.

One of the most rewarding aspects of this journey has been the opportunity to give back to the learning community and positively impact the next generation of leaders. Witnessing our interns grow and flourish, personally and professionally, has been truly fulfilling. As I reflect, I am reminded that mentorship creates a legacy that transcends generations. The lessons shared and experiences exchanged will remain with these young leaders long after their internship concludes. I have no doubt they will go on to leave their own mark on society, and I feel honoured to have played a role in their journey.

I extend my heartfelt gratitude to each of our interns for placing their trust in us. Their enthusiasm and dedication have made this experience truly memorable. Looking ahead, I am excited to witness the impact our interns will make in their respective fields, carrying forward the lessons they have learned to create meaningful change.

Together, let us continue to empower the next generation of leaders. Through the Grand Guruz initiative, we can ignite young minds, cultivate leadership, and inspire purpose, shaping a future where India’s demographic advantage translates into progress, prosperity, and national strength.

Grand Guruz is an Investment in the Future of India’s Knowledge Ecosystem

Kriti Sinha

Research Associate
Centre for knowledge sovereignty

At its core, leadership is not measured by individual success but by the ability to create pathways for others to grow. The Grand Guruz Program, conceptualized and nurtured under the Centre for Knowledge Sovereignty (CKS), embodies this philosophy. It has provided a unique platform where experience meets curiosity, and wisdom meets fresh perspectives.

As being associated with CKS Core team, I view this program as more than an academic initiative, it is an investment in the future of India’s knowledge ecosystem. By bringing together seasoned mentors, our “Grand Guruz”, with young, dynamic mentees, we are building a bridge that connects generations of thinkers, policymakers, and innovators. The learnings imparted are not just technical or theoretical; they are lessons in vision, resilience, and responsibility.

This program has reaffirmed my belief that mentorship is the most sustainable form of nation-building. The exchange of ideas, the rigor of research, and the spirit of inquiry that I have witnessed among the mentees are testimony to the immense potential that lies within our youth. Equally inspiring has been the commitment of our mentors, who have guided with patience, insight, and generosity.

The Grand Guruz Program, is an enduring model that must continue to expand, evolve, and inspire. It has set a benchmark for how academia, mentorship, and national interest can converge meaningfully.

I take immense pride in being associated with this initiative and look forward to seeing our mentees carry forward the torch of knowledge, integrity, and innovation into the larger world.

Space Where Ideas Involve Through Dialogue, Discipline & Direction

Shubham Pandey

Coordinator, Grand Guruz Program
Centre for knowledge sovereignty

Coordinating the Grand Guruz Program has been a journey of both learning and Personal Growth for me. This initiative was not just about connecting students with experts, it was about cultivating a space where ideas evolve through dialogue, discipline, and direction.

From our inaugural meetings to the final research submissions, I witnessed the mentees transform their curiosity into clarity. Each interaction with the mentors, our Grand Guruz, brought forth not just guidance but also the wisdom that comes from real-world experience. It reaffirmed my belief that the right mentorship can shift mindsets and accelerate purpose-driven work.

This program has shown us that when young minds are nurtured with attention and strategic guidance, they don’t just follow the discourse, they help shape it. I believe Grand Guruz is just the beginning. With each edition, we have the potential to build a stronger ecosystem of youth-driven, policy-relevant research aligned with national priorities.

I am deeply grateful to CKS and our mentors for trusting me with this role, and to the mentees for giving their best. Together, we’ve built something worth scaling.

Research Papers

Next ▶

Disclaimer : This research paper is the sole work of the student (mentee) and has been prepared exclusively for academic purpose. The views and opinions expressed are those of the author alone and do not necessarily reflect those of CKS or O.P Jindal Global University. CKS takes no responsibility for any errors, omissions, accuracy of the information presented, or any consequences arising from its use.

P V Vineet

Research Paper 1

Title:-

State Exemptions and Surveillance Overreach : Challenges and Reform Pathways Under India's Digital Personal Data Protection Act.

1. Introduction

In today's digital age, the ability to process, access, and control individual data is an integral part of state and corporate power dynamics. Data is not a marginal by-product of digital exchange; it is an integral part of social infrastructure with implications from access to services to the surveillance of political dissent. Against this backdrop, the legal underpinning of data protection is critical as the guardian of fundamental rights, demarcating the boundary between governmental interest and individual privacy. India's *first serious attempt at regulating the space is the Digital Personal Data Protection Act of 2023* (DPDP Act). Whilst the Act is a long-sought step forward in data governance, its exemption provisions—Sections 7(c), 17(2), and 17(3)—are main perils to constitutional rights and democratic accountability standards.

Section 7(c) authorises the state to process personal data without consent for the "performance by the State or any of its instrumentalities of any function under any law," or "in the interest of sovereignty and integrity of India or security of the State" (DPDP Act, 2023). Section 17(2) also authorizes the central government to exempt any state instrumentality from compliance with the law in pursuit of "public order," "friendly relations with foreign States," and other generally articulated purposes. Apart from all this, Section 17(3) also allows for exemptions for private players or groups of data fiduciaries, and hence expands the scope of state-like powers to the domain of private surveillance vendors and data analytics firms. Taken together, these provisions create a robust regime of discretion that allows for the possibility of mass surveillance subject to minimal legal or institutional control.

This problem goes beyond theory. Recent historical experience has shown how surveillance techniques can operate in legally ambiguous environments, normally justified by poorly defined notions such as "public order" or "national security."

The Pegasus spyware case revealed that dozens of journalists, political figures, and activists were surveilled using a military-grade cyberweapon typically licensed only to governments (The Wire, 2022). Yet the government neither confirmed nor denied the existence of such surveillance nor subjected its practices to judicial or parliamentary oversight. Similarly, the Tamil Nadu Police data breach in 2024 exposed how biometric data of protestors and criminal suspects was collected and stored without consent, and then compromised through a facial recognition portal with lax security protocols (Varutra, 2024). These, and similar cases illustrate how the vague wording of statutory exemptions translate to practical, systemic vulnerabilities in citizens' rights to privacy and transparency.

Globally, democracies have developed legal doctrines to handle similar tensions between state security and individual liberties. The European Union's *General Data Protection Regulation* (GDPR) permits exemptions for state functions, but only under the strict conditions of proportionality, necessity, and judicial oversight (European Commission, 2024). For example, GDPR's Article 23 requires that such exemptions must be clearly articulated in domestic law, necessary in a democratic society, and subject to safeguards such as access to remedies and oversight by independent authorities. Likewise, in Israel, surveillance measures taken by intelligence and law enforcement agencies must be authorised through judicial warrants, with limited allowances for exigent circumstances subject to post-facto review (Carnegie Endowment, 2023). But, India's DPDP Act provides no requirement for a warrant, no necessity clause, no ex-ante review, and no obligation to inform affected individuals.

This raises not only legal and normative concerns but also institutional design challenges. In the absence of transparent audit mechanisms or judicial gatekeeping, exemptions risk becoming the norm rather than the exception. By not defining key terms such as “security of the State” or “public order,” the law places excessive interpretive power in the hands of the executive. This has implications beyond surveillance, potentially undermining the right to information (RTI), the freedom of expression, and the rights of protestors and marginalised communities, who are often the first to bear the brunt of disproportionate state scrutiny (Hindustan Times, 2022; TechPolicy.Press, 2024).

Moreover, the lack of a transparency portal or quarterly disclosure mechanism regarding the number of surveillance requests under Section 7(c) represents a significant accountability gap. Countries like Singapore, Canada, and Brazil have institutionalised such mechanisms to ensure a balance between state access to data and citizens' rights to know how their data is being used (ITS Rio, 2024). In India, however, ministries and law enforcement agencies rarely publish any data regarding data access or processing, especially when done under national security pretexts. This opacity not only undermines legal accountability but corrodes public trust in governance, especially in an environment already marked by widespread digital illiteracy and power asymmetries.

The objective of this paper is therefore twofold: to investigate how broad state exemptions under Sections 7(c), 17(2), and 17(3) of the DPDP Act have enabled instances of surveillance overreach, and to evaluate whether these legal provisions meet the standards of necessity, proportionality, and transparency that underpin a democratic society. Using a case study approach, the paper examines three emblematic instances of surveillance: the Pegasus spyware operation, the Tamil Nadu police facial recognition breach, and the digital surveillance during the 2024 farmers’ protest, to trace how the legal structure of exemptions interacts with institutional behaviour and real-world consequences.

By combining statutory analysis with empirical documentation, this paper aims to provide policy recommendations that can help align India’s data protection regime with both constitutional norms and global best practices. The stakes are high: in a society where digital infrastructures increasingly mediate citizenship, governance, and resistance, the question of who can access data, and under what conditions; is no less than a question of power.

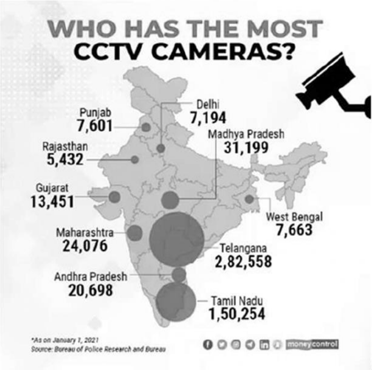


Image: Moneycontrol: State-wise distribution of CCTV cameras, with Telangana and Tamil Nadu as leading surveillance states.

2. Background

The evolution of data protection jurisprudence in India reflects a convergence of constitutional interpretation, legislative enactment, and administrative praxis. With the enactment of the *Digital Personal Data Protection Act, 2023* (DPDP Act), the Indian legal system has attempted to codify a framework for the governance of personal data that simultaneously upholds individual autonomy and facilitates the lawful exercise of state functions. The Act draws its constitutional lineage from the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), wherein the Supreme Court of India unanimously affirmed the right to privacy as a fundamental right under Article 21 of the Constitution. However, the recognition of privacy was not unconditional. The judgment envisaged that any curtailment of the right to privacy must satisfy the test of legality, necessity, and proportionality, thereby laying down a tripartite standard for evaluating restrictions on informational privacy.

In this legal context, the DPDP Act represents an attempt by the legislature to articulate the parameters within which personal data may be processed, accessed, and retained by both public and private entities. The Act is organised around the principle of fiduciary responsibility, classifying data processors as "Data Fiduciaries" and data subjects as "Data Principals." This fiduciary framing imposes obligations on data handlers to act in a manner consistent with the best interests of the data principal, subject to reasonable exceptions authorised by law. Sections 4 through 11 of the Act outline the grounds for lawful processing, with consent as the default modality. Nevertheless, the statute provides several carve-outs wherein data may be processed without the express consent of the data principal. Among the most consequential of these are the exemptions granted to the State under Sections 7(c), 17(2), and 17(3), which merit a nuanced examination.

Section 7 of the DPDP Act delineates "legitimate uses" under which personal data may be processed in the absence of consent. Clause (c) of this section permits data processing "for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State" (DPDP Act, 2023, §7(c)). This statutory language enables the State to engage in non-consensual processing for the fulfilment of statutory functions or to advance objectives connected with the national interest. Notably, the provision does not prescribe any threshold of necessity or proportionality, nor does it condition such processing upon prior judicial authorisation. The legislative text also does not enumerate an exhaustive list of circumstances under which the terms "security of the State" or "sovereignty" may be invoked, thereby delegating interpretative discretion to the executive branch.

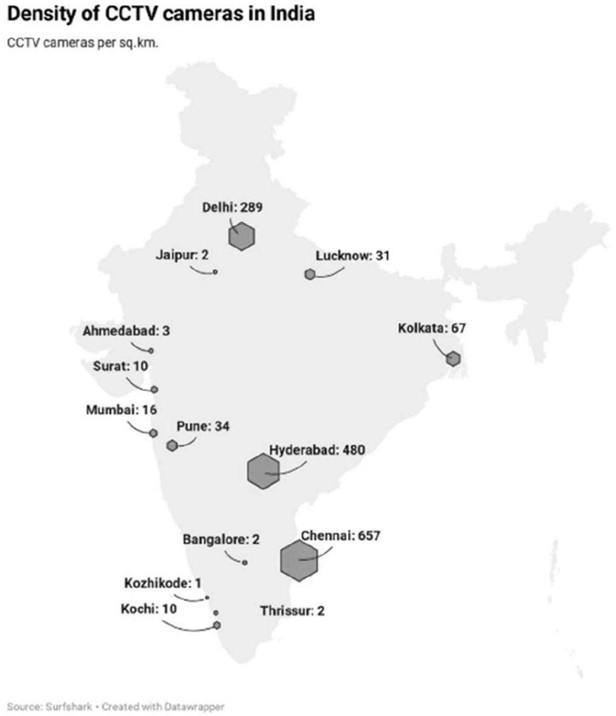
Section 17 of the DPDP Act introduces further exemptions under the heading of “exemptions for certain processing.” Subsection (2)(a) permits the Central Government, by notification, to exempt any instrumentality of the State from the application of the Act in its entirety or in part if such exemption is deemed necessary in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or for preventing incitement to the commission of any cognisable offence (DPDP Act, 2023, §17(2)(a)). This provision authorises a form of statutory derogation, permitting specific state agencies to operate outside the purview of the data protection obligations otherwise imposed by the Act. While this may be seen as a mechanism to preserve the operational flexibility of the sovereign, particularly in sensitive domains such as intelligence and defence, it does not currently stipulate a mechanism for ex ante scrutiny or independent oversight of the exercise of such discretion.

Subsection (3) of Section 17 extends the exemption regime beyond the domain of state instrumentalities to private data fiduciaries. It empowers the Central Government to exempt any class of data fiduciaries from the application of any provision of the Act, having regard to factors such as the volume and nature of personal data processed, the risk to the rights of data principals, and the impact on state functions. This formulation permits functional exemptions for private actors who may be involved in the provision of surveillance technologies, telecommunications infrastructure, or strategic services that intersect with public functions. However, the statutory language does not prescribe the specific procedural safeguards that must accompany the issuance of such exemption notifications, nor does it condition them upon an objective assessment of necessity or proportionality by an independent body.

The exemption clauses in the DPDP Act are not anomalous in global data protection regimes. Article 23 of the European Union's *General Data Protection Regulation* (GDPR) similarly permits Member States to restrict the scope of data subject rights and data controller obligations for reasons of national security, defence, public security, or the prevention and investigation of criminal offences. However, the GDPR stipulates that such restrictions must be provided for by law, respect the essence of the fundamental rights and freedoms of individuals, and be necessary and proportionate in a democratic society (European Commission, 2024). Furthermore, European jurisprudence has routinely emphasised the necessity of judicial oversight and the availability of effective remedies to ensure that such exemptions do not become instruments of arbitrary power. A comparative analysis, therefore, invites consideration of how India's evolving data protection landscape may integrate similar principles while respecting its constitutional framework and administrative imperatives.

It is also pertinent to observe that the operationalisation of data protection norms in India intersects with pre-existing statutory frameworks such as the *Information Technology Act, 2000*, and sectoral regimes governing telecommunications, health, and financial data. The DPDP Act represents a transversal statute intended to harmonise disparate data regimes under a singular architecture. Nevertheless, its interaction with national security legislation, including the *Unlawful Activities (Prevention) Act*, the *Telegraph Act*, and various executive orders, creates a legal ecosystem where multiple authorities may exercise concurrent or overlapping powers relating to data access and processing.

Against this legislative and institutional background, it becomes imperative to examine how the provisions under Sections 7(c), 17(2), and 17(3) have functioned in practice, particularly in relation to public interest surveillance. This paper, therefore, turns to specific case studies that have attracted public and judicial attention in recent years. By analysing these instances, the paper seeks to illuminate the manner in which statutory exemptions are interpreted and applied, the procedural safeguards currently in place, and the implications for data principals whose rights may be affected by such processing. In doing so, the study contributes to the broader discourse on how India may reconcile national security prerogatives with the constitutional values of accountability, transparency, and the rule of law.



Density of CCTV cameras in India

CCTV cameras per sq.km.

Source: Surfshark • Created with Datawrapper

Image: Surfshark: Global ranking of CCTV camera density per square kilometre: Chennai tops global surveillance cities.

3. Research Question

How do state surveillance exemptions under India's DPDP Act compare to global standards, and what legal reforms are necessary to align with democratic oversight principles?

4. Methodology

This policy paper adopts a hybrid methodology that combines doctrinal legal analysis, comparative constitutional and statutory study, and case-based empirical inquiry. The objective is to evaluate the adequacy of the exemption clauses under Sections 7(c), 17(2), and 17(3) of the *Digital Personal Data Protection Act, 2023* (DPDP Act), particularly in relation to surveillance oversight and privacy protection.

The doctrinal component involves a close textual and purposive interpretation of the DPDP Act, especially its provisions on legitimate state use, exemptions, and data fiduciary obligations. This reading is situated within the Indian constitutional framework, drawing on the privacy standards articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which sets out the tripartite test of legality, necessity, and proportionality.

The comparative legal analysis examines statutory surveillance and data protection frameworks from four jurisdictions: Singapore (Personal Data Protection Act, 2012), Israel (Wiretap Law, 1979; Protection of Privacy Law, 1981), the United Kingdom (Investigatory Powers Act, 2016; Data Protection Act, 2018), and the United States (Foreign Intelligence Surveillance Act, 1978; USA FREEDOM Act, 2015). These are selected for their relevance in balancing national security imperatives with privacy safeguards and judicial oversight.

The empirical component employs a case study approach, examining three recent Indian incidents: the Pegasus spyware episode, the Tamil Nadu Police data breach, and the 2024 farmers' protest surveillance. Each case is analysed through the lens of legal justification, institutional oversight, and rights impact.

Together, this triangulated method provides a multi-layered understanding of surveillance practices under the DPDP Act and offers grounded recommendations for reform.

5. Timeline

The timeline below outlines the sequence of critical legal, technological, and administrative events that form the evidentiary and analytical basis of this policy paper. These events provide insight into how state exemptions under the *Digital Personal Data Protection Act, 2023* (DPDP Act) interact with surveillance practices and regulatory gaps in India.

2017 – The Supreme Court of India, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, declares the right to privacy a fundamental right under Article 21. The judgment establishes the tripartite test of legality, necessity, and proportionality for state interference with privacy.

2021 – The *Pegasus Project*, coordinated by global media outlets, reveals that Pegasus spyware was allegedly deployed against Indian journalists, political opposition figures, and civil society actors. While the government neither confirmed nor denied its use, the matter sparked public debate on surveillance oversight.

2022 – Reports emerge of increased RTI application denials on national security grounds, citing Section 8(1)(a) of the RTI Act. Rejection rates rise by over 80% in some ministries (Hindustan Times, 2022), indicating growing opacity around surveillance-related disclosures.

2023 – The *Digital Personal Data Protection Act* is enacted, codifying wide-ranging state exemptions under Sections 7(c), 17(2), and 17(3).

2024 – The Tamil Nadu Police Facial Recognition Portal is breached, leaking over 50,000 biometric profiles. Surveillance of protestors during the farmers' movement also raises concerns regarding drone and facial recognition use under loosely interpreted public order grounds.

This timeline frames the case studies and forms the empirical core for policy evaluation.

6. Discussion

Case Study 1: Pegasus Spyware and Non-Transparent State Surveillance (2021)

The Pegasus spyware revelations of 2021 represent a defining episode in the discourse on state surveillance, data protection, and informational privacy in India. As part of a global investigative collaboration led by Forbidden Stories and Amnesty International, it was revealed that Pegasus—a highly sophisticated surveillance software developed by Israel's NSO Group and sold exclusively to government clients—was used to target over 300 Indian phone numbers, including those belonging to journalists, opposition politicians, constitutional authorities, academics, and human rights activists (The Wire, 2022).

Forensic analysis conducted by Amnesty's Security Lab confirmed the presence of Pegasus infections on several devices, establishing a credible evidentiary trail that implicated state actors. Despite the extensive documentation and global outcry, the Government of India issued no formal acknowledgement of procurement or deployment. Instead, it invoked grounds of "national security" and "public interest" to resist both judicial intervention and parliamentary inquiry (Drishti IAS, 2023). The Supreme Court eventually constituted a technical committee to examine the allegations, which found instances of malware use but did not establish conclusive state involvement due to lack of cooperation from government agencies (SC Observer, 2023).

In the context of the *Digital Personal Data Protection Act, 2023*, this incident illuminates the practical risks of broad state exemptions. Under Section 7(c) of the DPDP Act, state agencies are permitted to process personal data without consent for functions related to "sovereignty," "security of the State," and "public order." The Pegasus surveillance campaign, though predating the Act, would likely fall within the interpretive scope of this provision were it invoked post-2023. Crucially, the Act does not mandate prior judicial approval, independent authorisation, or even post-facto reporting when such surveillance is undertaken. The enabling language allows for covert data interception without a proportionality test or public transparency mechanism.

Furthermore, under Section 17(3), the Central Government may exempt specific classes of data fiduciaries; including potential vendors or surveillance enablers, from compliance with data protection provisions. The Pegasus case exemplifies how such provisions might shield private contractors operating in conjunction with the State from legal liability or scrutiny. The absence of a robust regulatory mechanism to audit or verify such exemptions significantly diminishes the potential for institutional accountability.

From a constitutional perspective, the operation of such surveillance in secrecy and without oversight is difficult to reconcile with the tripartite test laid down in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). In that decision, the Court mandated that any intrusion into the right to privacy must satisfy legality (existence of law), necessity (legitimate state aim), and proportionality (least intrusive means). The Pegasus revelations raise concerns particularly around the proportionality and procedural fairness components of this test. The scale, secrecy, and selective targeting of individuals strongly suggest that even if national security were a valid justification, the means adopted may not have met the threshold of democratic acceptability.

The Pegasus case demonstrates the potential for surveillance to occur under opaque conditions when statutory exemptions lack adequate procedural safeguards. It raises critical questions regarding the balance between executive discretion and constitutional rights in India's data protection regime. The case underscores the need for reforms to ensure judicial oversight, vendor accountability, and transparency in state surveillance activities conducted under the DPDP Act.

Case Study 2: Tamil Nadu Police Facial Recognition Breach (2024)

In March 2024, a major data breach incident involving the Tamil Nadu Police's Facial Recognition System (FRS) raised significant concerns regarding the security and legality of biometric data processing under the framework of the *Digital Personal Data Protection Act, 2023*. A hacker using the pseudonym "Valerie" gained unauthorised access to a police-maintained portal hosting facial recognition data, exposing over 50,000 biometric records. These included facial scans, FIR-related metadata, and details of individuals under investigation or associated with protests (Varutra, 2024).

The data breach revealed systemic issues in both data storage practices and the legal basis for biometric data collection. The portal lacked basic encryption protocols and access controls, and no audit trail was available to determine how the data was accessed, or by whom. The incident occurred during a period of heightened police surveillance in Chennai, where biometric data was collected at large-scale public gatherings, including protest sites and public transit hubs.

Under Section 7(c) of the *Digital Personal Data Protection Act, 2023*, state instrumentalities may process personal data without obtaining the consent of the data principal if such processing is undertaken “for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State.” In this case, law enforcement authorities justified the use of facial recognition technology and the collection of biometric data under the grounds of maintaining public order and preventing incitement to the commission of cognisable offences.

However, the provision does not prescribe any criteria for assessing the proportionality of the data collection, nor does it require a Data Protection Impact Assessment (DPIA) or prior judicial authorisation. The language of Section 7(c) does not include procedural prerequisites or reporting obligations, which in effect permits non-consensual biometric data collection without structured oversight. Furthermore, the failure to secure the stored data represents a contravention of Section 8(5) of the DPDP Act, which states that “the Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.” The breach illustrates that the absence of codified compliance monitoring and enforcement mechanisms undermines the purpose of the obligation.

In addition, Section 17(2)(a) empowers the Central Government to exempt any instrumentality of the State from compliance with the provisions of the Act “in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognisable offence.” This discretionary exemption, if exercised, could potentially remove liability from the concerned law enforcement agencies despite the breach. The provision does not currently mandate a notification to be published with detailed justification or include temporal or scope-based limits.

From a constitutional perspective, the legality of non-consensual biometric surveillance, particularly in peaceful public settings, engages Article 21 of the Constitution, which guarantees the right to life and personal liberty. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court cautioned against disproportionate surveillance measures and emphasised the importance of both necessity and proportionality in any state action affecting privacy. The Tamil Nadu incident raises the question of whether facial recognition surveillance of protestors or commuters, in the absence of imminent threat or individualised suspicion, satisfies the proportionality test.

The breach also draws attention to the limitations of India’s current institutional framework in enforcing data security obligations. Unlike the European Union’s *General Data Protection Regulation* (GDPR), which requires DPIAs for high-risk processing activities and mandates that supervisory authorities be informed of breaches within seventy-two hours, the DPDP Act does not operationalise these thresholds in the context of state agencies. The lack of publicly accessible breach notifications or transparency portals further exacerbates institutional opacity.

In conclusion, the Tamil Nadu Police facial recognition breach exemplifies the risks associated with wide exemptions granted to state agencies under the DPDP Act. It highlights the need for mandatory security audits, judicial preconditions for high-risk surveillance, and a procedural mechanism for invoking exemptions under Sections 7(c) and 17(2). The incident underscores that in the absence of judicial review, enforceable DPIAs, and breach reporting obligations, the processing of biometric data by law enforcement bodies may not adequately protect the rights of data principals as envisioned by the Act or the Constitution.

Case Study 3: Surveillance During the 2024 Farmers' Protest

The 2024 farmers' protest, organised in response to policy dissatisfaction regarding minimum support prices and agricultural subsidies, witnessed the deployment of multiple state surveillance technologies, raising critical concerns about lawful data processing, proportionality, and the limits of exemption provisions under the *Digital Personal Data Protection Act, 2023*. Various reports confirmed that law enforcement agencies employed aerial drones, automated facial recognition systems (AFRS), and call data record (CDR) analysis to monitor protestors' movements, affiliations, and communications (TechPolicy.Press, 2024). These actions were carried out without any publicly available judicial warrant or parliamentary oversight, and in the absence of a declared state of emergency or exceptional law invoked under the *Criminal Procedure Code*.

The legal justification offered by officials for the use of such surveillance infrastructure relied on the need to maintain "public order" and prevent incitement to cognisable offences. This rationale aligns with the permissible grounds under Section 7(c) of the *Digital Personal Data Protection Act, 2023*, which allows the State or its instrumentalities to process personal data without the consent of the data principal "for the performance... of any function under any law... or in the interest of sovereignty and integrity of India or security of the State." The expansive construction of this clause permits a broad interpretation of what constitutes a legitimate state function. However, it omits procedural safeguards such as judicial authorisation, data minimisation principles, or real-time oversight, which would be essential to ensuring the legality of mass surveillance activities in a democratic society.

The incident also invokes the operation of Section 17(2)(a), which allows the Central Government to exempt state instrumentalities from the application of the Act in furtherance of public order or other enumerated interests. While such a provision may serve the objective of administrative expediency in exigent situations, its discretionary nature, coupled with the lack of mandatory disclosure or temporal limits, raises questions about its application to peacetime assemblies and non-violent protests. In this particular instance, the surveillance encompassed individuals not accused of any offence, which may fall short of the constitutional standards articulated by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where it was held that privacy restrictions must be necessary in a democratic society, proportionate to the aim pursued, and backed by a law with adequate procedural safeguards.

It is noteworthy that the technologies deployed involved the use of real-time facial recognition feeds matched against legacy criminal databases, thereby exposing individuals to potential false positives and stigma. Furthermore, the collection of metadata through mobile triangulation and CDR analysis enabled pattern recognition that could reveal not only individual participation but also the structure of mobilisation networks. This implicates not merely privacy but also the right to assembly under Article 19(1)(b) and the freedom of association under Article 19(1)(c) of the Constitution. Surveillance practices that have the effect of deterring lawful assembly and discouraging civic participation must be examined through a lens of heightened scrutiny.

From a comparative perspective, under the GDPR and the jurisprudence of the European Court of Human Rights, such mass surveillance operations targeting peaceful protestors would be subject to independent oversight and prior judicial review. High-risk processing activities involving special categories of personal data—such as biometric identifiers, require the performance of a Data Protection Impact Assessment (DPIA) and must demonstrate a compelling public interest proportional to the intrusion. The DPDP Act, while incorporating broad obligations under Section 8 on data protection duties, does not explicitly operationalise

DPIAs or impose them as a precondition for surveillance undertaken by state authorities under Section 7(c).

Moreover, the absence of publicly accessible reporting mechanisms for data access or surveillance metrics, either at the ministerial or departmental level, means that affected individuals cannot reasonably assess whether they have been subjected to surveillance or seek remedies under applicable law. This results in an asymmetry of power that is structurally embedded in the exemption framework.

In conclusion, the 2024 farmers' protest surveillance episode illustrates the expansive application of state exemptions under the DPDP Act without a commensurate institutional structure for oversight, transparency, or remedy. It reveals the pressing need to introduce mandatory DPIAs for high-risk processing, judicial authorisation for mass surveillance, and public dashboards disclosing the volume and legal basis of data processing activities related to public order. Without such procedural reforms, the broad discretion afforded by Sections 7(c) and 17(2) may disproportionately affect constitutionally protected freedoms in the absence of individualised suspicion or lawful derogation procedures.

Comparative Jurisprudence:

Singapore's Model of Data Protection and Surveillance Oversight

Singapore, which attained independence in 1965—nearly two decades after India—has evolved into a model for digital governance and regulatory clarity, particularly in the domain of personal data protection. Despite being a highly centralised and security-conscious state, Singapore has demonstrated a structured approach to balancing state surveillance powers with individual rights. The country's progress in enacting well-defined data protection statutes, ensuring regular audits, and embedding accountability mechanisms stands in sharp contrast to the ambiguity that characterises the exemption clauses in India's *Digital Personal Data Protection Act, 2023* (DPDP Act).

At the heart of Singapore's data protection framework is the Personal Data Protection Act, 2012 (PDPA), which came into force in phases beginning in 2013. The PDPA governs the collection, use, disclosure, and care of personal data by private organisations and, in modified form, by public agencies. While Singapore allows certain national security and public interest exemptions, these are narrowly tailored and accompanied by reporting obligations and independent oversight. Public sector agencies are governed by the Government Instruction Manual on ICT & Data, which sets out cybersecurity and data protection requirements. Unlike India's broad Section 7(c), Singapore's exemption mechanisms are purpose-limited, subject to ministerial review, and bounded by subsidiary legislation.

A cornerstone of Singapore's model is its data breach notification regime, which became mandatory with the 2020 amendments to the PDPA. Organisations must notify the Personal Data Protection Commission (PDPC) and affected individuals within 72 hours of becoming aware of a data breach that is likely to cause significant harm or affect more than 500 individuals. This transparency mandate plays a pivotal role in ensuring public accountability and pre-emptive containment of harms, features absent in the current Indian framework.

Singapore also mandates Data Protection Impact Assessments (DPIAs) for high-risk projects, particularly those involving facial recognition systems, location tracking, or biometric authentication. The Model AI Governance Framework, published by the Infocomm Media

Development Authority and the PDPC, also encourages accountability in algorithmic surveillance and automated decision-making—an area in which India's DPDP Act remains silent.

An illustrative example where Singapore's framework averted a major surveillance concern is the TraceTogether contact tracing app during the COVID-19 pandemic. Although initially promoted as privacy-preserving, the app's data was later accessed by police under the Criminal Procedure Code for a serious criminal investigation. This sparked public backlash. In response, the government amended legislation to restrict TraceTogether data access strictly to investigations for serious offences, thus realigning executive action with public expectations and privacy assurances. The incident demonstrates both the operational flexibility and responsiveness of the legal framework, including the willingness to legislate corrective safeguards swiftly.

Another example is the SingHealth cyberattack (2018), where personal data of 1.5 million patients was exfiltrated in one of the worst breaches in Singapore's history. Although the attack targeted state medical records, the incident triggered extensive audits, mandatory remedial training for IT administrators, and enhanced breach response standards. The PDPC's investigation and public release of findings, including specific accountability of senior personnel, reflected a rule-based enforcement culture.

Singapore's legal regime succeeds in balancing national security prerogatives with individual rights through statutory specificity, independent regulatory architecture, and procedural mandates such as DPIAs and breach disclosures. The State's authority is not absolute but institutionally bounded through periodic review and layered accountability. These features mitigate the potential for systemic overreach while maintaining operational efficiency. India's DPDP Act, particularly its provisions under Sections 7(c), 17(2), and 17(3), could benefit from adopting similar institutionalised checks—especially in mandating reporting obligations, refining exemption scopes, and embedding pre-emptive review mechanisms for high-risk data processing.

Israel's Surveillance Oversight and Data Protection Regime

Israel presents a compelling example of a jurisdiction that combines robust national security architecture with statutory mechanisms designed to preserve the rule of law and constitutional safeguards in the realm of surveillance and data protection. As a state with persistent security concerns and a highly developed intelligence apparatus, Israel has nonetheless instituted meaningful procedural controls, particularly through judicial oversight, sector-specific regulation, and institutional accountability. These mechanisms are essential in constraining executive discretion and preserving citizens' informational autonomy.

Israel does not have a singular, omnibus data protection statute equivalent to the European Union's *General Data Protection Regulation* (GDPR) or Singapore's *Personal Data Protection Act* (PDPA). However, it maintains a structured legal framework under the Protection of Privacy Law, 1981 (PPL), supplemented by sectoral guidelines issued by the Israeli Privacy Protection Authority (PPA). The PPL defines "databases" and regulates their use, requiring registration, adherence to data minimisation principles, and limitations on the use of sensitive data. Importantly, it provides a foundational right to privacy, which was elevated to constitutional status through the Basic Law: Human Dignity and Liberty (1992). This legal elevation imposes a proportionality requirement on any legislative or executive action that infringes on privacy rights.

The primary statutory mechanism for surveillance oversight in Israel lies in the Wiretap Law, 1979, which governs the interception of communications by law enforcement and security agencies. This statute mandates that wiretap orders must be issued by a judge and may only be granted upon a substantiated request demonstrating necessity and specific public interest. The order must also be time-bound, with strict limits on renewal. Surveillance for purposes of state security is subject to authorisation by the Minister of Defence or the Prime Minister, but even in such cases, there exists a supervisory role played by the Attorney General and the Knesset Subcommittee for Intelligence Affairs.

In contrast to India's *Digital Personal Data Protection Act, 2023*, which permits broad exemptions under Section 7(c) without mandatory judicial scrutiny, Israel's surveillance regime embeds judicial authorisation as a prerequisite for any targeted interception. Furthermore, state security-related surveillance is subject to periodic reporting to parliamentary committees, thereby ensuring both political and institutional oversight.

A salient example of Israel's approach to balancing public health interests and privacy arose during the COVID-19 pandemic, when the Shin Bet (Israel Security Agency) was temporarily authorised to track infected individuals' mobile phone data to assist in contact tracing. This measure was taken under the Shin Bet Law, 2002, and was implemented only after Knesset approval and under the supervision of the Attorney General. However, following a series of petitions, the Israeli Supreme Court ruled in 2020 that such surveillance must meet the test of proportionality and could not be continued without a primary legislation explicitly authorising it. In its judgment, the Court reiterated that even in exceptional circumstances, the rights to dignity and privacy under the Basic Law could not be suspended without lawful, proportionate justification subject to legislative scrutiny.

This judicial intervention illustrates how constitutional and statutory principles operate together to prevent surveillance overreach. The requirement that state surveillance measures be "anchored in primary legislation" with defined purposes and oversight obligations serves as a structural constraint on executive power. It ensures that derogations from privacy rights are not carried out through ad hoc executive orders but must comply with rule-of-law principles.

In addition, Israel's Privacy Protection Regulations (Data Security), 2017 mandate rigorous cybersecurity practices and breach notification procedures for data controllers. While these rules do not apply in full to state security bodies, they form part of the regulatory ethos that governs the handling of personal data and set a baseline expectation for institutional data responsibility. Regulatory guidance issued by the PPA encourages data controllers to conduct risk assessments, employ encryption, and establish incident response mechanisms, particularly when dealing with biometric or geolocation data.

Israel's data protection and surveillance oversight model is distinguished by its reliance on judicial authorisation, sectoral legislation, and the constitutional embedding of the right to privacy. The system reflects a commitment to procedural regularity, proportionality, and democratic accountability, even in the face of persistent national security threats. These mechanisms create a calibrated balance between state imperatives and individual rights, which may offer a valuable template for reforming India's data protection regime. In particular, India could consider introducing mandatory judicial review for surveillance conducted under Section 7(c) of the DPDP Act and limiting executive discretion through statutory specificity and reporting requirements modelled on Israel's parliamentary and judicial supervisory arrangements.

The United States and Surveillance Oversight in a Federal Framework

The United States maintains one of the most complex and layered legal architectures for surveillance and data protection, reflecting the federal character of its legal system and the competing imperatives of national security, civil liberties, and technological innovation. While the United States does not possess a singular, comprehensive federal data protection statute akin to the European Union's *General Data Protection Regulation* (GDPR) or Singapore's *Personal Data Protection Act* (PDPA), it operates through a constellation of sector-specific statutes and constitutional doctrines. This decentralised approach is complemented by robust institutional oversight mechanisms, particularly in the context of state surveillance.

At the federal level, one of the most significant legislative instruments governing electronic surveillance is the Foreign Intelligence Surveillance Act, 1978 (FISA). Enacted in the aftermath of the Watergate scandal and revelations about intelligence overreach by the Church Committee, FISA establishes a legal framework for the surveillance of foreign powers and agents of foreign powers within the United States. A key feature of FISA is the requirement that all targeted electronic surveillance conducted for foreign intelligence purposes be authorised by the Foreign Intelligence Surveillance Court (FISC), a special Article III court that operates in camera and ex parte.

Under FISA Section 702, the United States government is permitted to collect the electronic communications of non-U.S. persons located outside the country, subject to procedures approved by the FISC. However, subsequent judicial interpretations and disclosures, particularly following the revelations by Edward Snowden in 2013, exposed the incidental collection of U.S. persons' communications through programs such as PRISM and UPSTREAM. This led to the enactment of the USA FREEDOM Act, 2015, which introduced significant reforms, including the termination of the bulk metadata collection program previously operated under Section 215 of the USA PATRIOT Act and the creation of a panel of amici curiae to assist the FISC in cases presenting novel legal questions.

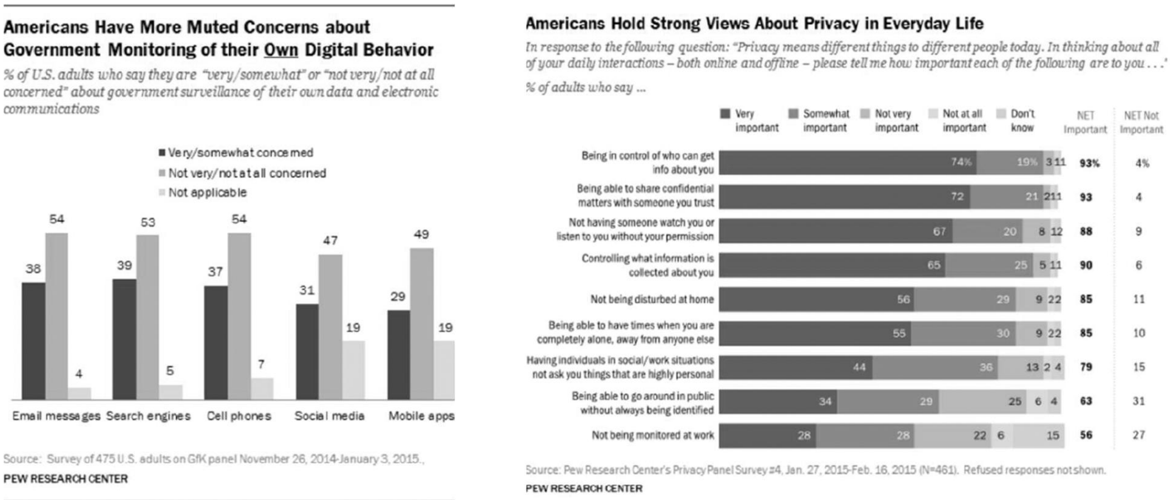
Importantly, the U.S. surveillance regime operates under constitutional constraints articulated primarily through the Fourth Amendment, which guards against unreasonable searches and seizures and requires probable cause for the issuance of warrants. In domestic law enforcement contexts, courts have consistently required warrants for the interception of communications, reinforced through the Electronic Communications Privacy Act, 1986 (ECPA) and its subcomponents—the Wiretap Act, the Stored Communications Act, and the Pen Register Act. These statutes regulate when and how government entities may access stored or real-time electronic communications, imposing procedural requirements and judicial supervision.

In terms of data breach management and transparency, the United States has adopted a decentralised but proactive posture. Forty-eight states, along with the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, have enacted laws requiring private or governmental entities to notify individuals of security breaches involving personally identifiable information. At the federal level, certain industries such as healthcare (under HIPAA) and finance (under GLBA) are subject to specific privacy and breach notification obligations.

A pivotal example of the functioning of institutional oversight in surveillance contexts can be found in the Snowden disclosures (2013). The leaks revealed the expansive scope of NSA's surveillance programs under both domestic and foreign intelligence authorities. The resulting public and legislative pressure led to judicial reviews, congressional hearings, and the eventual passage of the USA FREEDOM Act. Notably, the reforms were driven by civil society advocacy, media transparency, and congressional oversight, demonstrating the systemic capacity for institutional correction.

Another significant instance occurred in 2020, when the FISA Court of Review and the Department of Justice Office of the Inspector General (OIG) identified errors in FBI applications submitted to the FISC for surveillance of a U.S. citizen during the 2016 presidential campaign. The case led to procedural tightening, mandatory audits, and a formal apology from the FISA Court regarding insufficient diligence. These developments affirm that judicial supervision under FISA, though largely opaque, is not immune from accountability mechanisms.

While the U.S. model does permit a significant degree of executive latitude in the surveillance domain, particularly concerning foreign intelligence, it embeds robust judicial review and legislative scrutiny. The existence of independent inspectors general, adversarial review in select FISC proceedings, and periodic statutory sunset clauses collectively serve to limit excessive or prolonged surveillance authority.



Americans Have More Muted Concerns about Government Monitoring of their Own Digital Behavior

% of U.S. adults who say they are "very/somewhat" or "not very/not at all concerned" about government surveillance of their own data and electronic communications

Source: Survey of 475 U.S. adults on GfK panel November 26, 2014-January 3, 2015.,

PEW RESEARCH CENTER

Americans Hold Strong Views About Privacy in Everyday Life

In response to the following question: "Privacy means different things to different people today. In thinking about all of your daily interactions – both online and offline – please tell me how important each of the following are to you . . .'

% of adults who say ...

■ Very important
■ Somewhat important
■ Not very important
■ Not at all important
■ Don't know
NET Important
NET Not Important
Being in control of who can get info about you
74%
19%
3
1
1
93%
4%
Being able to share confidential matters with someone you trust
72
21
2
1
1
93
4
Not having someone watch you or listen to you without your permission
67
20
8
1
2
88
9
Controlling what information is collected about you
65
25
5
1
1
90
6
Not being disturbed at home
56
29
9
2
2
85
11
Being able to have times when you are completely alone, away from anyone else
55
30
9
2
2
85
10
Having individuals in social/work situations not ask you things that are highly personal
44
36
13
2
4
79
15
Being able to go around in public without always being identified
34
29
25
6
4
63
31
Not being monitored at work
28
28
22
6
15
56
27

Source: Pew Research Center's Privacy Panel Survey #4, Jan. 27, 2015-Feb. 16, 2015 (N=461). Refused responses not shown.

PEW RESEARCH CENTER

Image: Pew Research Center

In the Indian context, the absence of such institutional checks within the *Digital Personal Data Protection Act, 2023*—notably the lack of a dedicated data protection tribunal, independent oversight board, or warrant-based surveillance preconditions—stands in contrast to the multiple layers of accountability present in the U.S. model. Even in a national security-heavy framework, procedural due process and judicial participation remain indispensable to upholding democratic legitimacy.

While the United States does not operate under a unified data protection regime, its surveillance and information privacy jurisprudence reflects a dynamic interplay between statutory specificity, constitutional interpretation, and institutional oversight. India's DPDP Act could benefit significantly from emulating key safeguards found in U.S. law, such as pre-surveillance judicial authorisation, transparency in exceptional data access, and statutorily mandated audits of surveillance activity. These would ensure that national security objectives are pursued within a legal framework that respects both transparency and fundamental rights.

The United Kingdom's Surveillance Oversight and Data Protection Regime

The United Kingdom provides a comprehensive and mature model for regulating state surveillance and personal data processing through an integrated legal and institutional framework. Following its exit from the European Union, the United Kingdom retained many principles of the *General Data Protection Regulation (GDPR)* through its domesticated form known as the UK GDPR, read in conjunction with the Data Protection Act 2018 (DPA 2018). In addition to regulating private and public-sector data processing, the United Kingdom maintains a distinct statutory framework for surveillance conducted by intelligence and law enforcement agencies under the Investigatory Powers Act 2016 (IPA 2016). The UK's approach is characterised by statutory specificity, multi-tiered oversight, judicial authorisation, and public reporting obligations.

The Data Protection Act 2018, which operates alongside the UK GDPR, provides general obligations for lawful data processing, including transparency, purpose limitation, and data minimisation. Part 3 of the DPA 2018 specifically governs processing by law enforcement agencies and provides exemptions where necessary for the prevention, investigation, detection, or prosecution of criminal offences. However, these exemptions are narrow and require that the processing be both necessary and proportionate. Importantly, the law obliges data controllers in the law enforcement context to maintain detailed logs, conduct Data Protection Impact Assessments (DPIAs) for high-risk processing, and cooperate with the Information Commissioner's Office (ICO), the independent regulatory authority.

State surveillance is governed under a separate and highly structured statute, the Investigatory Powers Act 2016, also referred to as the "Snooper's Charter." This legislation consolidated and updated existing powers for bulk data collection, interception of communications, equipment interference (hacking), and targeted surveillance. Critically, the IPA 2016 introduced a unique double-lock system, whereby any warrant for intrusive surveillance must be approved both by a Secretary of State and subsequently by a Judicial Commissioner. The Judicial Commissioners are part of the Investigatory Powers Commissioner's Office (IPCO), an independent oversight body tasked with reviewing the lawfulness of surveillance operations and conducting inspections of public authorities.

For example, under Section 20 of the IPA, warrants for the interception of communications must be limited to what is necessary for national security, serious crime prevention, or safeguarding economic well-being. The scope of collection must be specific, and bulk powers can only be authorised in limited, predefined circumstances. Moreover, the Act mandates that the use of each surveillance capability: whether for bulk acquisition of internet connection records or equipment interference, be reported, audited, and reviewed.

A relevant instance demonstrating the application of this regime was the legal challenge brought by Liberty v. Secretary of State for the Home Department (2019). The High Court ruled that aspects of the IPA, particularly the bulk data retention powers, were inconsistent with fundamental rights under the European Convention on Human Rights (ECHR). The decision compelled the government to revise internal protocols to ensure compliance with Article 8 (Right to Privacy) and Article 10 (Freedom of Expression). The case highlighted that while the IPA grants significant investigatory powers, their exercise is not immune from judicial scrutiny or fundamental rights challenges.

Another example of the law functioning as intended is the annual IPCO report process, which includes disclosures of non-compliance, such as when local law enforcement agencies inadvertently exceeded authorised surveillance parameters. In such cases, the IPCO publicly records the breach, identifies the institutional lapse, and mandates remedial measures. These transparency measures strengthen public trust and institutional accountability.

The United Kingdom's legal model is notable for its strict procedural layering. High-risk processing requires DPIAs; all surveillance authorisations are documented and justified; oversight is both judicial and parliamentary; and the public has access to redress mechanisms. Additionally, the law mandates periodic reviews by the Investigatory Powers Tribunal, an independent judicial body where individuals may challenge unlawful surveillance.

In contrast, India's *Digital Personal Data Protection Act, 2023* permits extensive exemptions under Sections 7(c), 17(2), and 17(3) without requiring prior judicial approval or ex-post facto review by an independent commissioner or tribunal. Furthermore, India currently lacks a statutory obligation for the publication of surveillance audits or the maintenance of DPIAs for high-risk public interest data processing, such as those involving facial recognition or call metadata analysis.

In conclusion, the United Kingdom demonstrates how state surveillance can be lawfully conducted through a transparent and proportionate framework supported by institutional checks. The incorporation of judicial scrutiny, mandatory DPIAs, detailed recordkeeping, and an empowered data protection authority ensures that the exercise of investigatory powers remains consistent with democratic principles and the rule of law. These structural features provide critical reference points for India as it seeks to operationalise its data protection regime under the DPDP Act. Specifically, the establishment of an independent oversight commission and mandatory judicial review for surveillance activities would substantially enhance legal certainty and safeguard constitutional rights.

7. Recommendations

In light of the legal analysis and empirical case studies discussed, the following recommendations are proposed to enhance procedural safeguards, institutional accountability, and proportionality within the framework of the *Digital Personal Data Protection Act, 2023* (DPDP Act), particularly regarding Sections 7(c), 17(2), and 17(3).

1. Introduce Statutory Specificity to Section 7(c)

The term "security of the State" should be defined through a closed list of legitimate aims, including terrorism prevention, espionage, or grave threats to public safety. This would align with the principle of legality as interpreted in *Justice K.S. Puttaswamy v. Union of India* and reflect international practices such as the Investigatory Powers Act 2016 (UK) and the GDPR's Article 23.

2. Mandate Judicial Authorisation for Surveillance

Any surveillance or data access carried out under Section 7(c) must be subject to prior judicial approval or post-facto review within a fixed time frame, as practiced in Israel under the Wiretap Law (1979) and in the UK's double-lock system. Judicial scrutiny serves as a critical check on executive discretion.

3. Repeal or Amend Section 17(3)

The power to exempt private entities, including data fiduciaries, from obligations under the Act should be repealed or made subject to parliamentary notification and independent audit by a regulatory authority.

4. Establish a Data Surveillance Review Board (DSRB)

An independent oversight body comprising legal and technical experts should be tasked with reviewing all exemption notifications and high-risk processing activities. This board must publish quarterly reports.

5. Mandate Data Protection Impact Assessments (DPIAs)

For high-risk activities such as facial recognition, biometric processing, or metadata collection, DPIAs should be made mandatory and submitted to the proposed Data Protection Board or the DSRB for prior review.

8. Conclusion

The *Digital Personal Data Protection Act, 2023* (DPDP Act) represents a significant legislative milestone in India's journey toward regulating the complex interplay between personal data, state function, and individual rights. Enacted in response to the Supreme Court's landmark recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Act seeks to create a comprehensive framework for data governance. Yet, the provisions under Sections 7(c), 17(2), and 17(3) expose a critical tension between the State's interest in national security and the individual's right to informational self-determination.

This policy paper has undertaken a doctrinal and empirical inquiry into how these exemption clauses, in their current form, may enable unchecked surveillance. Through detailed analysis of three contemporary case studies, Pegasus spyware deployment, the Tamil Nadu Police facial recognition breach, and the surveillance during the 2024 farmers' protest, it becomes evident that the current legal framework allows for wide interpretive latitude without commensurate procedural safeguards. The absence of judicial preconditions, lack of independent oversight, and minimal public disclosure obligations have collectively contributed to an ecosystem where surveillance can occur without demonstrable accountability or necessity assessments.

India's current regime stands in marked contrast with international practices. In Singapore, statutory definitions are embedded within the *Personal Data Protection Act* and supplemented with breach notification mandates and Data Protection Impact Assessments (DPIAs). Israel relies on its *Wiretap Law* and judicial warrant system, with its constitutional Basic Law reinforcing proportionality and legal clarity. The United States, through instruments like FISA and the USA FREEDOM Act, incorporates judicial oversight and legislative review even within a national security-heavy environment. The United Kingdom's Investigatory Powers Act introduces a double-lock mechanism requiring both executive and judicial approval, alongside an independent oversight body, IPCO.

These jurisdictions demonstrate that national security imperatives need not stand in opposition to democratic transparency and procedural fairness. Rather, security and privacy can coexist when executive power is subjected to clear statutory limitations, judicial review, and regular audit mechanisms. Such models have proven responsive even in crisis contexts, whether through Singapore's legislative amendments following the use of TraceTogether data or Israel's Supreme Court intervention in Shin Bet's contact-tracing program.

India's approach, however, risks normalising exceptionalism. The open-textured nature of terms like "public order," "sovereignty," and "security of the State," combined with executive discretion in exempting state or private entities from compliance, creates significant scope for arbitrariness. These provisions, if left unmodified, may fall short of the legality, necessity, and proportionality standards laid down in Indian constitutional jurisprudence and reflected in comparative practice.

Furthermore, the lack of an institutionalised mechanism to monitor or review the invocation of exemptions creates a democratic accountability vacuum. Without judicial gatekeeping or an independent Data Surveillance Review Board, the legality of surveillance operations remains difficult to challenge. Citizens lack not only the knowledge of when their data is processed but also the procedural tools to contest such processing under the law. This undermines the very objective of the DPDP Act, which is to build a data protection framework based on trust, transparency, and the rights of the data principal.

As India becomes increasingly data-intensive and digitally dependent, the stakes of surveillance governance grow exponentially. Whether through state-facilitated biometric authentication, predictive policing, or public health monitoring, the state's ability to process personal data is expanding across domains. This expansion must be matched by robust legal safeguards to ensure that personal data is not merely a tool of governance but also a site of rights-based protection.

This policy paper, therefore, concludes that while the DPDP Act provides a much-needed regulatory foundation, its exemption clauses require urgent recalibration. Judicial preconditions, precise statutory thresholds, independent oversight, and transparency mandates must be integrated into the law's architecture. The future of data governance in India depends not just on enabling the state to act, but on ensuring that such action is constitutional, proportionate, and subject to democratic scrutiny.

Only through such reform can India align its data protection regime with global standards while fulfilling its constitutional promise of dignity, liberty, and accountability in the digital age.

9. References

1. Carnegie Endowment for International Peace. (2023). *Understanding India's new data protection law*. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law
2. Central Information Commission. (2008). *Annual report 2007–08*. https://cic.gov.in
3. Drishti IAS. (2023). *Pegasus case and surveillance concerns*. https://www.drishtiias.com/daily-news-analysis/pegasus-case
4. European Commission. (2024). *GDPR enforcement guidelines*. https://ec.europa.eu
5. Frontline. (2024). *Data breach exposes 50,000 biometric records in Tamil Nadu*. [Reported coverage; source name retained as "Frontline" due to non-specific link]
6. Hindustan Times. (2022, March 5). *83% increase in rejection of RTI applications on national security grounds*. https://www.hindustantimes.com/india-news/83-increase-in-rejection-of-rti-applications-on-national-security-grounds-data-101646469748249.html
7. Information Commissioner's Office (ICO). (2019). *Guide to the Investigatory Powers Act*. https://ico.org.uk/for-organisations/investigatory-powers
8. ITS Rio. (2024). *Surveillance oversight in Brazil: Enforcement report 2023*. https://itsrio.org
9. Judgment: Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

10. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*. https://www.meity.gov.in
11. PRS India. (2025). *Analysis of state surveillance under DPDP Act*. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
12. SC Observer. (2023). *Pegasus spyware probe case background*. https://www.scobserver.in/cases/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-case-background
13. TechPolicy.Press. (2024). *India clamps down on dissent with drones and facial recognition during farmer protests*. https://techpolicy.press/india-clamps-down-on-dissent-with-drones
14. The Wire. (2022, November 4). *Pegasus 2.0: New targets in India*. https://www.thewire.in
15. UK Government. (2016). *Investigatory Powers Act 2016*. https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
16. Varutra. (2024). *Tamil Nadu Police data breach: Information available for sale on the dark web*. https://www.varutra.com/ctp/threatpost/postDetails/Tamil-Nadu-Police-Data-Breach:-Information-Available-for-Sale-on-Dark-Web/a3paTG42UUp6azZ5RkRzU3J0SjN5Zz09

Akash Namboodiripad

Research Paper 2

Title:-
A Critical Analysis of Reasons for NDPS Acquittals in Hyderabad between January 2024 and March 2025

Abstract

This paper analyses reasons for NDPS Act acquittals in Hyderabad (2024-2025) through judgment analysis and stakeholder interviews. Key findings reveal that inadmissible evidence and procedural lapses contribute to over 90% of acquittals. A major factor is the inadmissibility of confessional statements made to police or NDPS officers, as established by the Supreme Court in Tofan Singh v. State of T.N. Delays in inventory certification and issues with mediator credibility also significantly weaken prosecution cases. The study highlights systemic investigative and procedural inadequacies at the grassroots level. Recommendations include enhancing capacity-building for state police and addressing judicial pendency to improve conviction rates.

Introduction

The Narcotics Drugs and Psychotropic Substances Act (NDPS) Act of 1985 was constituted in view of Article 47 of the Indian Constitution which mandates that the *'State shall endeavour to bring about prohibition of the consumption except for medicinal purposes of intoxicating drinks and of drugs which are injurious to health'* and the existence of three global conventions on drugs –

- The Single Convention on Narcotics Drugs 1961
- The Convention on Psychotropic Substances 1971
- The UN Convention against Illicit Traffic in Narcotics Drugs and Psychotropic Substances 1988

The NDPS Act is stated to prohibit, except for medical or scientific purposes, the manufacture, production, trade, use, etc. of narcotic drugs and psychotropic substances.[1] The Act replaced earlier laws such as the Dangerous Drugs Act and Opium Acts, with the intention to divulge the power of enforcement to a larger network of state and central agencies, especially in Section 9 and 10 of the NDPS Act where the functions are detailed. It effectively established statutory authorities such as the Narcotics Commissioner (Sec 5) who leads the Central Bureau Narcotics and the Narcotics Control Bureau (through a notification under Sec 4 NDPS). The NCB coordinates action across Central and State functionaries under the Ministry of Home Affairs (MHA). Section 10 elaborates on the power of the state government to permit, control and regulate the proliferation, possession, cultivation and manufacture of narcotic drugs and psychotropic drugs. It is within this federal framework of decentralisation and clear division of

[1] Government of India, *National Policy on Narcotic Drugs and Psychotropic Substances*, n.d.

powers that India constitutes its drug policy. A recent development in this framework includes the operationalisation of the NCORD (National Narcotics Coordination Portal).

India's geographical position is sandwiched between the world's two largest drug dens - the Golden Triangle and the Golden Crescent. This results in an unprecedented amount of illicit supply chain incentives for illegal actors making India a market and transit point for the proliferation of drugs and narcotics across global markets, especially due to its large coastline. Add to this the domestic illicit cultivation, manufacture and possession of illegal substances and it makes for an ever-changing and adaptive drug crime ecosystem.

Policy Relevance

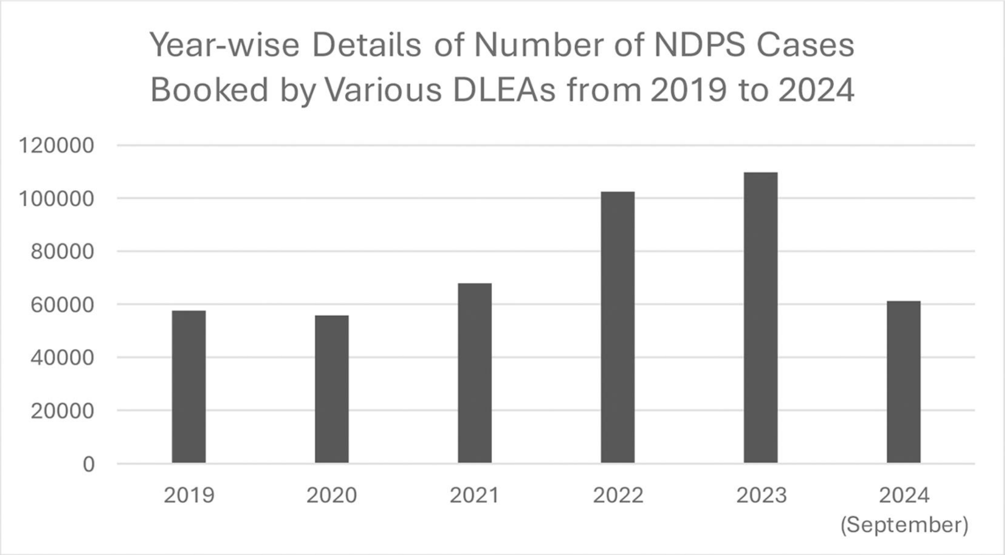


Fig 1: Year-wise Details of Number of Narcotic Drugs and Psychotropic Substances (NDPS) Cases Booked by Various Drug Law Enforcement Agencies (DLEAs) from 2019 to September 2024[2]

[2] RAJYA SABHA SESSION - 266 UNSTARRED QUESTION No 1081. ANSWERED ON, 4TH DECEMBER 2024. Source - Narcotics Control Bureau (NCB) database. Data of 2024 (September) are Provisional Figure. Data for 2024 (Upto 30th September).

According to data from answers made in Rajya Sabha session 267, in the year 2024, a total of **89913** cases were registered under NDPS throughout the country out of which only **110** were convicted.[3] The total value of drugs found in the same year stand at $1.07 Billion, according to estimates provided by various security agencies.[4] In 2022, Rajya Sabha Question No. 839, the second question posed for the Minister of Home Affairs to state "the reasons for low conviction rate and whether Government is planning any particular measure to make the law more effective and increase conviction rate, if so, details thereof;".[5] The answer given is the following:

> *"The Government through Narcotics Control Bureau (NCB) organises training program to upgrade the skills of the public prosecutors and Drug Law Enforcement Officers to ensure better conviction rate. NCB has initiated quarterly training program for Special Public Prosecutors and two training programs have already been conducted."*

Telangana State operates a four tier system of drug enforcement through the following agencies:

- Prohibition & Excise department
- Telangana State Anti-Narcotics Bureau (TSANB)
- Telangana State Police
- Drug Control Administration (DCA)

Additionally the Hyderabad City Police also operates Hyderabad Narcotics Enforcement Wing (H-NEW) and Narcotics Investigation Supervision Wing (NISW). Hyderabad City Police Jurisdiction is spread over an area of 3600 km^2 with an approximate population of 9.7 million . It operates 71 Law & Order Police Stations, 07 Women Police Stations, 31 Traffic Police Stations, separate wings viz., City Security Wing , Special Branch, Task Force, Detective

[3] 1. "State/UT-Wise Number of Narcotic Drugs and Psychotropic Substances (NDPS) Cases Registered and Number of Conviction during 2022-24," Open Government Data Platform India, May 30, 2025, News Desk, "Telangana Sees 29 Pc Increase in NDPS Violations in 2024, Says Report," *The Siasat Daily* (blog), December 29, 2024, https://www.siasat.com/telangana-sees-29-pc-increase-in-ndps-violations-in-2024-says-report-3156049/.. RAJYA SABHA SESSION - 267 UNSTARRED QUESTION No. 1508 ANSWERED ON, 12TH MARCH 2025. Source - Narcotics Control Bureau (NCB).

[4] 1. Murali Krishnan, How India became a methamphetamine, cocaine hub, June 1, 2025, https://www.dw.com/en/how-india-became-a-methamphetamine-and-cocaine-hub/a-71210919.

[5] "GOVERNMENT OF INDIA MINISTRY OF HOME AFFAIRS RAJYA SABHA UNSTARRED QUESTION NO. 839." 2022. Press release. December 15, 2022. Accessed June 17, 2025. https://www.mha.gov.in/MHA1/Par2017/pdfs/par2022-pdfs/RS-14122022/839.pdf.

Department, Cyber Crime, Narcotics Enforcement Wing, City Armed Reserve, IT Cell working under Commissioner of Police.[6]

YEAR	NO. OF CASES	ACCUSED ARRESTED	NO. PERSONS PD ACT IMPOSED	TOTAL WORTH/RS. DRUGS SEIZED
2021	1346	3180	152	48.45 Cr.
2022	1278	3096	225	28.26 Cr.
2023	1450	2892	32	94.38 Cr.

Table 1 : Case Statistics of Telangana State (TGANB)[7]

The above statistic provided by the Telangana State Anti-Narcotics Bureau (TGANB) point to an upward trend in the number of cases registered. The state has registered a total of 2387 NDPS cases off which only 4 were convicted in 2024 according to data mentioned in session 267. This is almost a 60.74% increase from the number of cases registered in 2023. The State of Telangana, according to a news report, has seen a 29% increase in NDPS violations in 2024 due to which the Prohibition and Excise department conducted Operation Dhoolpet, under which 317 individuals were arrested[8]. Growing urbanisation and service sector growth in Hyderabad have contributed to an increasingly sophisticated criminal proliferation of narcotics and psychotropic substances. In Hyderabad, NDPS (Narcotic Drugs and Psychotropic Substances) Act cases are primarily tried in the City Civil Court Complex. Specifically, the Special Court for CBI Cases, Hyderabad handles cases related to the NDPS Act, as part of the CBI court complex. Additionally, the Criminal Court Complex within the City Civil Court complex also handles NDPS cases.

Experts have identified low conviction rates and delay in punishments as legal hurdles in the war on drugs in Punjab.[9] Low conviction rates therefore lay the breeding ground for both

[6] "About Us." n.d. Hyderabadpolice.Gov.In. Accessed June 18, 2025. https://www.hyderabadpolice.gov.in/about.html.

[7] "Telangana State -," October 9, 2023, https://tganb.tspolice.gov.in/telangana-state/.

[8] 1. News Desk, "Telangana Sees 29 Pc Increase in NDPS Violations in 2024, Says Report," The Siasat daily, December 29, 2024, https://www.siasat.com/telangana-sees-29-pc-increase-in-ndps-violations-in-2024-says-report-3156049/#:~:text=Hyderabad%3A%20Telangana%20witnessed%20an%20increase,compared%20to%201%2C134%20in%202023.

[9] 1. R K Arora and Vinay Kaura, "War on Drugs: Challenges for the Punjab Government," ORF, May 9, 2017, https://www.orfonline.org/research/war-drugs-challenges-punjab-government.

demand and supply of illegal substances. This issue posits a significant hurdle within the legal and policing system in India as a whole.

Some of the most cited reasons for acquittals are:

1. Discrepancy in the Test Identification Parade
   A Test Identification Parade **(TIP)** is a legal procedure under Sec 54 of the BNSS used during criminal investigations in India (and many other common law countries) where a witness or victim is asked to identify the accused from a line-up of people. *(BNSS Sec 54)*
   If the parade is delayed, improperly conducted, or the witness is 'tipped off' beforehand, courts may find the identification unreliable—leading to benefit of doubt to the accused. TIP is only corroborative, not substantive evidence.

2. Preparation of inventory
   Upon seizure of drugs the relevant agency is required to seize all goods present at the site of seizure (not just the narcotic substance). Incomplete or poorly documented inventory raises suspicion of tampering or fabrication, weakening the prosecution's case *(NDPS Act Sec 52A)*.

3. Inadmissible evidence
   Statements given before an NDPS or Police officer require corroborative evidence making statements inadmissible as evidence in a court of law unless substantiated. Under Indian law, especially in NDPS cases, confessional statements made to police or NDPS officers are not admissible unless supported by independent corroborative evidence. The NDPS Act provides for a reverse burden of proof, but the prosecution must first establish a *prima facie* case**.** If the prosecution relies solely on such statements without independent proof, courts may discard such evidence, causing acquittal *(NDPS Act Sec 25 and 53A) (Indian Evidence Act, Section 25)*.

4. Procedural lapses
   Procedural lapses is the broad miscellaneous category consisting of lapses made after inventory certification, apart from those specifically addressed through other categories. It includes standard procedure mandates that if an accused is to be searched, they should be **informed** i.e. explicitly made to understand of their right to be searched before a magistrate or gazetted officer. Procedure also mandates that seizures made under *NDPS Sec 42(2)* says if an officer records information in writing under sub-section (1) or records grounds for their belief under its proviso (for sunset to sunrise entry/search), they must send a copy of this record to their immediate official superior within seventy-two hours.
   Non-compliance with this mandatory requirement can make the entire recovery (of drugs) illegal, thus failing the prosecution *(NDPS Act Sec 50)(NDPS Act Sec 42)*.

5. Not produced before a gazetted officer or magistrate (Section 50 violation)

   NDPS law requires that before search/seizure is undertaken, the accused must be offered the choice to have the search conducted in the presence of a gazetted officer or magistrate *(NDPS Act Sec 50)*. Failure to give this opportunity invalidates the search process—making the evidence collected inadmissible.

6. Illegal Searches

   Searches conducted without valid authorization or warrant, or without following proper procedure (such as the presence of a lady officer), are deemed illegal. Evidence collected from such illegal searches is liable to be excluded, which seriously damages the prosecution's case. *(NDPS Act, Sec 41, 42 & 43 – conditions for search and seizure)*

7. Delay in sending samples to forensic labs

   As per procedure, seized substances must be promptly sent to a Forensic Science Laboratory (FSL) for analysis after approval by the Magistrate. Delays raise doubts about whether the sample was tampered with or substituted, leading to acquittal *(NDPS Act, Sec 52A)*

8. Labs make inconclusive forensic reports

   Forensic reports that fail to clearly identify the seized substance as a narcotic drug or psychotropic substance that collapsed the prosecution's case. Courts require conclusive evidence—an ambiguous or unclear report creates reasonable doubt (*NDPS Act, Sections 52A, 53)*

9. Fabricated investigations

   When inconsistencies or contradictions appear in prosecution evidence, courts may infer possibility of planted or fabricated evidence. This violates the **presumption of innocence** guaranteed under law, forcing courts to acquit the accused to prevent miscarriage of justice *(Indian Constitution, Article 21)*.

10. Witness turning hostile

    Witnesses who retract their earlier statements or deny knowledge of the incident while testifying in court severely weaken the prosecution. Without witness support, crucial links in the chain of evidence break—leading to failure to prove guilt beyond reasonable doubt (*Indian Evidence Act, Sec 154)*

Case Classification

Drug Trafficking	Drug Abuses	Possession
Cultivation	Smuggling	Peddling

Objective

Undertake a critical analysis of reasons cited for acquittals of NDPS Cases in Hyderabad between 2024 to March 31st, 2025

- Derive a qualitative understanding of issues affecting NDPS acquittals
- Triangulate with available judgement reports

Research Question

What are the primary procedural, evidentiary, and systemic factors contributing to NDPS case acquittals in Hyderabad courts, and how do these patterns relate to the broader state and national context?

Methodology

The research for the paper would involve mixed-methods research. It will involve a mix of interviews, secondary data analysis and relevant case studies.

The research has been conducted taking into account respondent anonymity to ensure candid insights. By protecting their identities, the research aims to encourage participant stakeholders to share their experiences and observations. The purpose of the questionnaire is to gather stakeholder and field level insights on procedural and policy perspectives on NDPS acquittals. The questionnaire has been posed to a total of 4 prominent stakeholders within the enforcement system of Hyderabad. Testimonies can be collected through stakeholders such as lawyers, law firms that specialise in NDPS cases, police officers, NCB officers etc. A bilingual (English-Hindi) semi-structured questionnaire was designed to assess procedural and evidentiary practices in NDPS cases. The survey included 11 open-ended questions, covering areas such as seizure protocols, forensic delays, confessional reliance, and witness testimony. The questionnaire was shared with select legal and enforcement professionals in Hyderabad. The following questions were posed:

English: In your experience, how frequently do procedural issues or challenges arise in the conduct of Test Identification Parades (TIP) in NDPS cases?
Hindi: आपके अनुभव में, एनडीपीएस मामलों में पहचान परेड (TIP) के दौरान प्रक्रिया से जुड़ी कुछ चुनौतियाँ या दिक्कतें कितनी बार आती हैं?

English: To what extent is the list of seized items (including narcotic and non-narcotic substances) typically reviewed or verified at the time of seizure?
Hindi: जब सामान जब्त किया जाता है (ड्रग्स और अन्य चीज़ें), तो उस सूची की जांच या पुष्टि आमतौर पर किस स्तर पर होती है?

English: In your opinion, how commonly do NDPS cases in Hyderabad rely on confessional statements as primary evidence?
Hindi: आपके अनुसार, हैदराबाद में एनडीपीएस मामलों में कबूलनामे को मुख्य सबूत के रूप में कितनी बार इस्तेमाल किया जाता है?

English: Based on your observation, how consistently are procedural safeguards such as informing the accused about the option of search before a magistrate or gazetted officer followed during investigations?
Hindi: आपके अवलोकन के अनुसार, क्या जांच के दौरान यह प्रक्रिया नियमित रूप से अपनाई जाती है कि आरोपी को मजिस्ट्रेट या गैज़ेटेड अफसर के सामने तलाशी के विकल्प की जानकारी दी जाए (धारा 50 NDPS)?

English: How common is it, in your experience, for the accused to not be offered the option of being searched before a magistrate or senior officer?
Hindi: आपके अनुभव में, क्या ऐसा अक्सर होता है कि आरोपी को मजिस्ट्रेट या वरिष्ठ अधिकारी के सामने तलाशी का विकल्प नहीं दिया जाता?

English: From your perspective, how frequently do inter-departmental searches face procedural gaps (e.g., lack of proper documentation or required personnel like a lady officer)?
Hindi: आपके विचार में, विभिन्न एजेंसियों द्वारा की गई तलाशियों में नियमों या प्रक्रिया से जुड़ी कुछ कमियाँ (जैसे दस्तावेज़ों की अनुपस्थिति या महिला अधिकारी की गैर-मौजूदगी) कितनी बार देखी जाती हैं?

English: How timely, in your view, are seized samples typically sent to forensic science laboratories (FSL)?
Hindi: आपके अनुसार, जब्त किए गए सैंपल आमतौर पर फॉरेंसिक लैब (FSL) को कितनी जल्दी भेजे जाते हैं?

English: How often, based on your observation, do forensic reports clearly establish the nature of the seized substance?
Hindi: आपके अवलोकन के अनुसार, फॉरेंसिक रिपोर्ट कितनी बार जब्त पदार्थ की प्रकृति को स्पष्ट रूप से दर्शाती है?

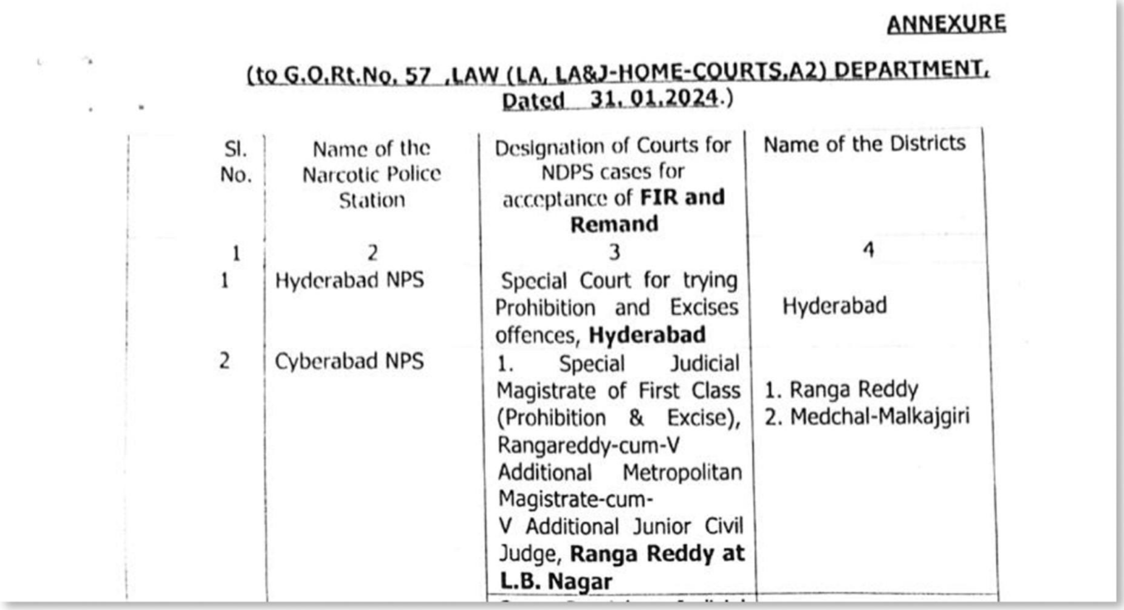
English: In your experience, how often do questions arise regarding the credibility or consistency of evidence presented in NDPS cases?
Hindi: आपके अनुभव में, एनडीपीएस मामलों में प्रस्तुत सबूतों की विश्वसनीयता या संगतता को लेकर कितनी बार प्रश्न उठते हैं?

English: How frequently do witnesses change their statements or differ from initial records during NDPS trials? In your opinion, what factors contribute to this?
Hindi: एनडीपीएस मामलों की सुनवाई के दौरान गवाहों के बयान बदलने की घटनाएं कितनी सामान्य हैं? आपके अनुसार, इसके क्या प्रमुख कारण होते हैं?

(For example: Fear of retaliation / Lack of protection / Police pressure / Forgetting / Other)

English: In your view, what changes or improvements in investigation, procedure, or legal provisions could help enhance conviction rates in NDPS cases across India?
Hindi: आपके विचार में, भारत में एनडीपीएस मामलों में सज़ा की दर बढ़ाने के लिए जांच, प्रक्रिया या क़ानूनी प्रावधानों में किन बदलावों या सुधारों की आवश्यकता है?

Data sources include Government reports, fieldwork, academic papers, testimonials. Judgement reports are taken of cases that have been disposed and judgements delivered between the dates of January 2024 and March 2025 from online resources under E-Court Services, Govt of India.



ANNEXURE

(to G.O.Rt.No. 57 ,LAW (LA, LA&J-HOME-COURTS,A2) DEPARTMENT, Dated 31. 01.2024.)

Sl. No.	Name of the Narcotic Police Station	Designation of Courts for NDPS cases for acceptance of **FIR and Remand**	Name of the Districts
1	2	3	4
1	Hyderabad NPS	Special Court for trying Prohibition and Excises offences, **Hyderabad**	Hyderabad
2	Cyberabad NPS	1. Special Judicial Magistrate of First Class (Prohibition & Excise), Rangareddy-cum-V Additional Metropolitan Magistrate-cum-V Additional Junior Civil Judge, **Ranga Reddy at L.B. Nagar**	1. Ranga Reddy 2. Medchal-Malkajgiri

Fig 2: GOVERNMENT OF TEIANGANA ABSTRACT : Special Courts - Designation of the six (6) Excise Courts of Special Judicial Magistrate of First Class with territorial jurisdiction for accepting FIRs and Reirands from Narcotic Police Stations of Hyderabad, Cyberabad, Rachakonda and Warangal, registered under the Narcotic Drugs and Psychotropic Substances Act, 1985 (Central Act, 61 of 1985)- Orders-Issued.[10]

The Special Court for trying Prohibition and Excise offenses in Hyderabad is located at the Commissioner of Prohibition and Excise Department building.

Locations visited

- Metropolitan Criminal Court, Nampally
- TGANB Office
- NCB Zonal Office

Additional testimonies can be collected through stakeholders such as lawyers, law firms that specialise in NDPS cases, police officers.

[10] 1. R Thirupathi, "GOVT OF TELANGANA ABSTRACT," Telangana Anti-narcotics Bureau (TGANB), January 31, 2024, http://tganb.tspolice.gov.in/wp-content/uploads/2024/02/49-Legal-TSNAB-2024-57-Court-Order.pdf.

Findings

Respondent Number	Designation
1	Defence Lawyer
2	Defence Lawyer
3	Assistant to Public Prosecutor
4	TGANB Official

Table 2: Stakeholder Designations and Respondent Anonymization

All respondents stated that TIP is generally not conducted in NDPS cases. Respondent 4 also mentioned that a procedure mirroring TIP can be a template for further strengthening prosecution. Respondent 1 and 2 suggested that there existed significant variation in the inventory practices between different agencies such as the NCB or the Prohibition and Excise Department.

Respondent 4 stated that confessional statements made by Prosecution Witnesses or the Investigating Officers were highly scrutinised and held in "serious doubt" during court proceedings. The onus of proving corroborative evidence lies on the investigative agencies and that "any witness provided is ensured to be from different govt offices and not from the same".

Respondent 3 states that lapses in procedure were considered a void of awareness among agencies the more state centric they are in their training and jurisdiction. This includes the accused being given the option of being searched in front of a gazetted officer or magistrate. Respondent 4 pointed that in majority of cases, accused are searched in front of a gazetted officer rather than a magistrate.

Respondent 1 and 2 said that defence lawyers are easily about to create leverage by pointing to discrepancies made in the illegality of searches made. Respondent 4 said that enforcement agencies often lay out respective procedural templates that may vary in the details but are more or less based on NDPS guidelines in its basic framework.

Respondent 3, who was associated with the office of the public prosecutor, pointed to the delay in sending contraband samples to forensic labs as the largest contributor to acquittals. Respondents 1 and 2 said that Telangana had some of the best forensic capabilities in the country and therefore the chances of missing the nature of the seized substances were low. Respondent 3 further stated that the reason for the delay in sending FSL samples can be attributed to the delayed approval or certification of inventory of samples by the magistrate from the *Maalkhana* (designated storage) to be sent to the relevant labs. All respondents pointed to defence insinuations combined with corroborative evidence of fabricated investigations being a prominent reason for prosecution weakening which leads to increased chances of acquittal. Respondent 1 and 2 said that prosecution witnesses, especially those with "dubious backgrounds" are subject to increased scrutiny. Only defence witnesses are therefore "more likely" to change their statements during proceedings relative to those presented by prosecution.

To understand the procedural and evidentiary issues contributing to NDPS cases, a total of 10 cases from within the Hyderabad Criminal Courts Complex were sourced from E-Court Services, which is a publicly available service and is under the maintenance of the National Informatics Centre, Ministry of Electronics and Information Technology, Government of India. The cases taken are those whose judgements were delivered between January 2024 and March 2025. The following is the list of cases:

- *PS Mahankali Vs Gadepaka Mahesh @ Saidulu @ Sai Mahesh Reddy*
- *PS Narayanaguda Vs A3 Padagala Pranav*
- *PS Sultan Bazar Vs A4 Bontha Parmesh*
- *RPS Secunderabad Vs A1 Sheikh Wasim*
- *PS Panchagutta Vs A2 Yogeshwar Goud*
- *PS Hussaini Alam Vs Tokala Kumara Swamy*
- *PS Bowenpally Vs A2 Erva Bhavani Prasad @ Bittu*
- *PS Musheerabad Vs A1 Bhushipaka Ganesh @ Ganda*
- *PS Shahinayat Gunj Vs A2 Darshan*
- *PS Bahadarpura Vs Guguloth Noor @ Shaikh Noor*

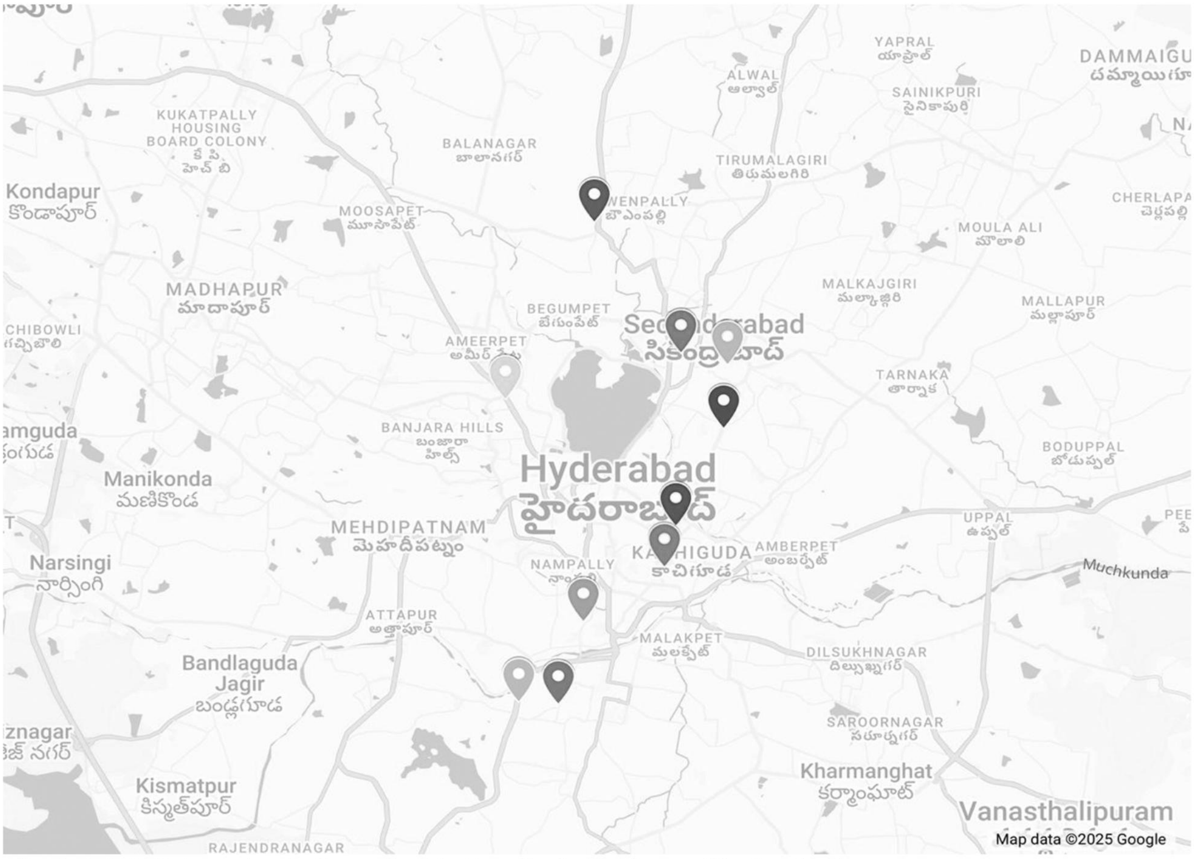


Fig 3: NDPS Acquittal Cases by Police Jurisdiction – Hyderabad

It is found that 100% of the cases are of drug possession while 20% of it is of drug abuse and drug trafficking each. None of the cases involve peddling, smuggling or cultivation.

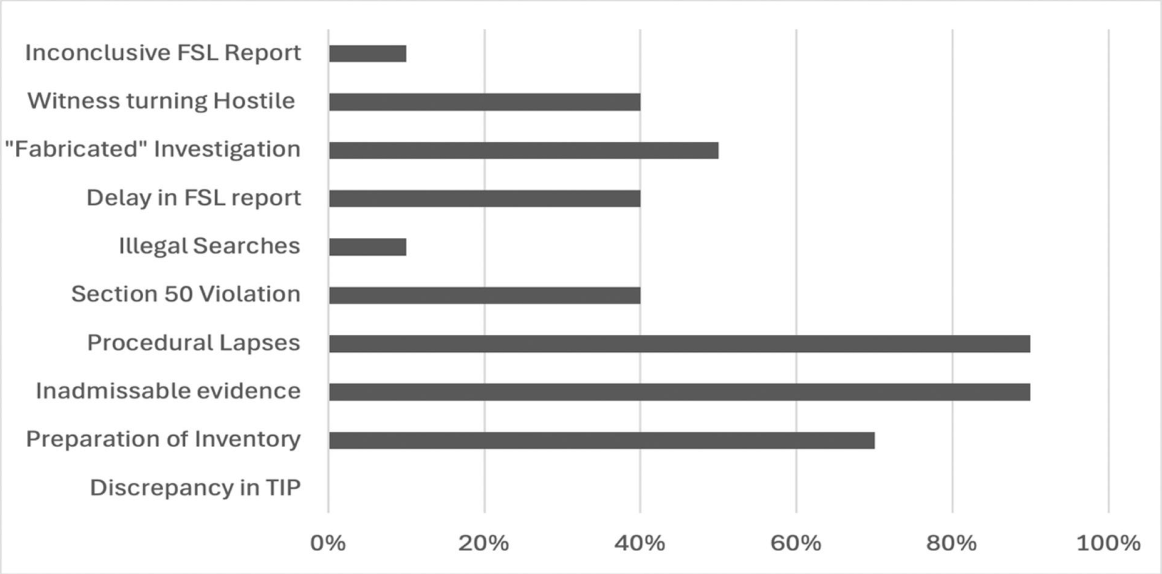


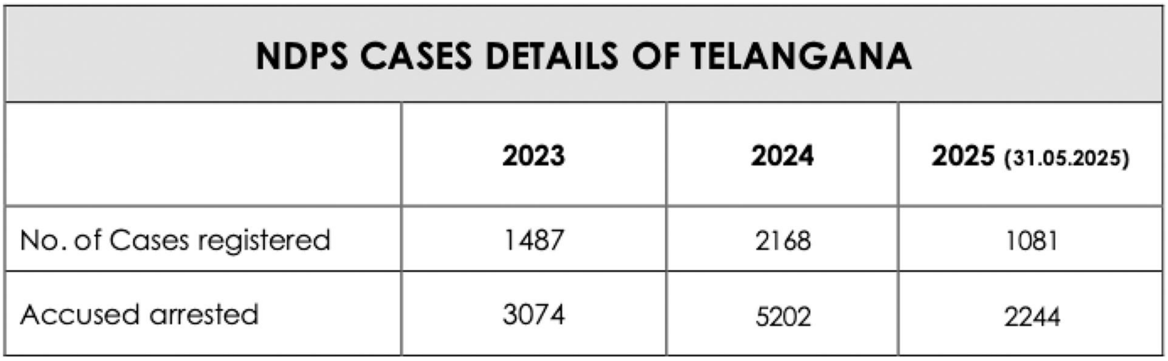
Fig 4: Percentage Distribution of Reasons Cited for Acquittal in NDPS Cases (n = 10)

Reasons Contributing to Acquittal	Percentage	Count
Discrepancy in TIP	0%	0
Preparation of Inventory	70%	7
Inadmissible evidence	90%	9
Procedural Lapses	90%	9
Section 50 Violation[11]	40%	4
Illegal Searches	10%	1
Delay in FSL report	40%	4
"Fabricated" Investigation	50%	5
Witness turning Hostile	40%	4

Table 3: Frequency and Percentage of Legal and Procedural Grounds for Acquittal in Analysed NDPS Judgments

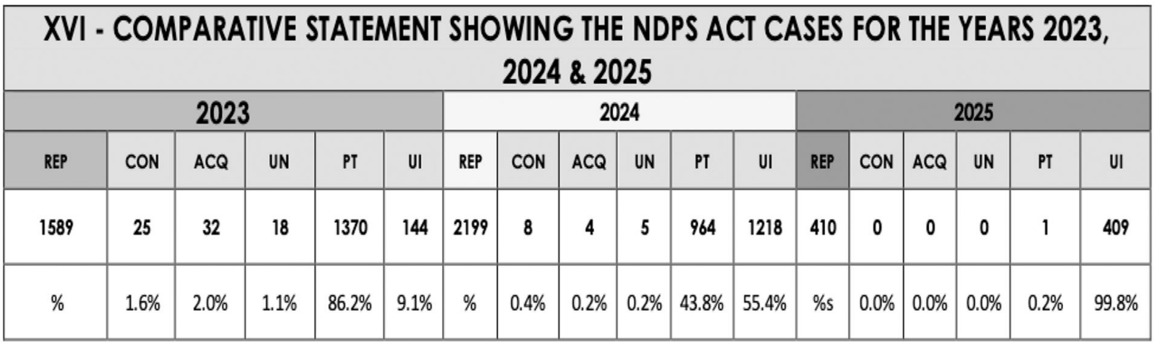
Out of all the cases taken, 90% cases reported inadmissible evidence and procedural lapses as key factors contributing to the weakening of prosecution's case and therefore leading to acquittal. 70% of cases reported preparation of inventory as being a reason cited for eventual acquittal. 40% of cases reported not being produced before a gazetted officer or magistrate and delay in sending samples to forensic labs as leading to case acquittals. Similarly 40% cases have also reported witnesses turning categorically hostile. Only 10% of cases reported searches made as being categorically "illegal" in nature. Similarly only 10% of cases reported forensic labs making inconclusive reports as contributing to acquittal. In 50% of cases, the honourable benches have insinuated or cited "fabrication" of evidence as an aspect that weakened the prosecution. 0% cases suggested an discrepancy in Test Information Parade as a factor that contributed to acquittal.

[11] Not produced before gazette officer of magistrate: Section 50 of the NDPS act stipulates that when an officer authorised under Section 42 is about to search a person, they **shall**, if the person so requires, take them without unnecessary delay to the nearest Gazetted Officer of specified departments or to the nearest Magistrate



NDPS CASES DETAILS OF TELANGANA			
	2023	2024	2025 (31.05.2025)
No. of Cases registered	1487	2168	1081
Accused arrested	3074	5202	2244

Fig 5: NDPS Case Details of Telangana. Source: TGANB



XVI - COMPARATIVE STATEMENT SHOWING THE NDPS ACT CASES FOR THE YEARS 2023, 2024 & 2025

2023						2024						2025					
REP	CON	ACQ	UN	PT	UI	REP	CON	ACQ	UN	PT	UI	REP	CON	ACQ	UN	PT	UI
1589	25	32	18	1370	144	2199	8	4	5	964	1218	410	0	0	0	1	409
%	1.6%	2.0%	1.1%	86.2%	9.1%	%	0.4%	0.2%	0.2%	43.8%	55.4%	%s	0.0%	0.0%	0.0%	0.2%	99.8%

Fig 6: Year-wise Comparison of NDPS Act Cases by Stage of Disposition and Outcome (2023–March 2025)[12] Source: TGANB

Discussion

The overall scenario present a very interesting take on the drug enforcement scenario in Hyderabad. Discrepancy in TIP is not clearly cited as a reason for acquittal in any of the cases taken. The closest violation is mentioned in *PS Hussaini Alam Vs Tokala Kumara Swamy* where the police failed to collect the registration certificate of the seized car, making its ownership by any of the accused difficult to determine. Additionally this absence is further corroborated by all respondents stating that TIP is not conducted in NDPS cases.

In the context of Preparation of Inventory, in *PS Hussaini Alam Vs Tokala Kumara Swamy* there is delay of more than a month t in magistrate certification of inventory. The court noted that this mandatory provision of Section 52-A of NDPS Act should be allowed "as soon as may be". Additionally the date of samples drawn for the FSL report predated this certification. The photographs taken during the Magistrate's verification showed that the seized property did not contain any panch slips or identity slips, nor did they show the date or signatures of mediators, raising "a serious doubt about the seized property". In *PS Panchagutta Vs A2 Yogeshwar Goud*,

[12] REP – Reported Cases, CON – Convictions, ACQ – Acquittals, UN – Untraced Cases, PT – Pending Trial, UI – Under Investigation

a delay of 50 days in the application magistrate certification of inventory was seen. A similar lack of panch slips with the seized samples and photographs was seen as well. In *PS Bahadarpura Vs Guguloth Noor @ Shaikh Noor* the court noted that the process of inventory certification was initiated after two weeks of drawing and sending the samples for analysis. In *PS Shahinayat Gunj Vs A2 Darshan* the delay for inventory certification was of four months where samples were drawn prior to the certification. A similar lack of assigned panch slips to seized items and photographs was seen as well. In *RPS Secunderabad Vs A1 Sheikh Wasim*, the requisition for inventory certification was filed sixteen months after after the seizure. In *PS Musheerabad Vs A1 Bhushipaka Ganesh @ Ganda* the delay is of 5 months. However in *PS Mahankali Vs Gadepaka Mahesh @ Saidulu @ Sai Mahesh Reddy* the delay in certification was not seen. Only a lack of panch slip on seized contraband was seen. In *PS Sultan Bazar Vs A4 Bontha Parmesh* the prosecution "failed to bring evidence as to the inventory of the contraband seized, photographs taken and drawn the representative samples in the presence of Magistrate by filing requisition before him soon after the seizure". The court cited *Yousuf @ Asif vs State (Crl.Appeal No.3191/2023)*[13]*,* which held that without proper inventory certification by the Magistrate, the seized contraband and samples "would not be a valid piece of primary evidence in the trial," thus vitiating the trial and weakening prosecutions case.

Almost all cases showed varying degrees of inadmissible evidence presented in court. In *PS Hussaini Alam Vs Tokala,* the confessional statements of A1 to A4 were found to be inadmissible. The court cited T*ofan Singh Vs. State of T.N. (2021) 4 SCC 1*[14] as precedent for stating that confessional statements made under *Section 67* of the NDPS Act were inadmissible in the trial of an offence. *Section 67* of the NDPS Act grants officers authorised by the Central or State Government the power to call for information, require the production of documents or things, and examine any person acquainted with the facts and circumstances during an inquiry into a contravention of the Act. In *PS Mahankali Vs Gadepaka Mahesh @ Saidulu @ Sai Mahesh Reddy*, the complainant (P.W.5) recorded the confession of the accused. The judgment highlighted that this occurred prior to the Gazetted Officer arriving. While not explicitly citing *Tofan Singh*, this practice is generally considered a basis for inadmissibility of such confessions. In *PS Narayanaguda Vs A3 Padagala Pranav* the prosecution's case against A3 was largely based on the confessions of A1 and A2 to the police, where A2 stated that A3 was a customer. The judgment therefore further implies that such police confessions are not sufficient to establish guilt although it does not mention the evidence as inadmissible. A similar

[13] Mohit Khandelwal & Associates. "Yusuf @ Asif v. State, Criminal Appeal No.3191/2023," April 26, 2025. https://mkajaipur.com/yusuf-asif-v-state-criminal-appeal-no-3191-2023/#:~:text=Yusuf%20%40%20Asif%20v.-,State%2C%20Criminal%20Appeal%20No.3191%2F2023&text=The%20Intelligence%20Officer%20of%20Narcotics,kept%20in%20two%20jute%20bags.

[14] LawBhoomi. "Toofan Singh Vs State of Tamil Nadu." LawBhoomi, April 16, 2025. https://lawbhoomi.com/toofan-singh-vs-state-of-tamil-nadu/#:~:text=Toofan%20Singh%20vs%20State%20of%20Tamil%20Nadu%20Judgement,-In%20a%20significant&text=The%20Court%20held%20that%20confessions,21%20of%20the%20Indian%20Constitution.

pattern is seen in all other cases where the statements recorded in confession to the police are held inadmissible and T*ofan Singh Vs. State of T.N. (2021) 4 SCC 1* is cited.

Procedural lapses is the broad miscellaneous category consisting of lapses made after inventory certification, apart from those specifically addressed through other categories. In *PS Hussaini Alam Vs Tokala*, the Gazetted Officer belonged to the same police department as that of the complainant and investigating officer. The mediators taken were not inhabitants local to the location of search and seizure. The failure to secure local inhabitants as mediators meant that mandatory procedures under Sections 100 and 165 of the Criminal Procedure Code (Cr.P.C.), which are applicable to NDPS Act cases as per *State of Punjab Vs. Balbir Singh (1994) 3 SCC 299*[15], were not followed. One of the mediators even admitted to acting as mediator to 10 other police cases, throwing doubt on his independence. Therefore the court found their statements “unworthy of credence”. Additionally a joint notice under *Section 50* of the NDPS Act was issued to all accused upon seizure. The court, citing *State of Rajasthan Vs. Parmanand (2014) 5 SCC 345*[16], ruled that the right to be searched before a Gazetted Officer or Magistrate must be communicated "clear, unambiguous and individual," and a joint communication "may create confusion" and "dilute the right". In *PS Mahankali Vs Gadepaka Mahesh @ Saidulu @ Sai Mahesh Reddy* the police searched the accused and seized Ganja *before* the arrival of the Gazetted Officer. Additionally the court found the presence of mediators at the time of confession and seizure "doubtful" and the report informing superior officers under Section 42(1) of NDPS Act lacked the date and time of receipt, raising doubt about immediate intimation. In *PS Narayanaguda Vs A3 Padagala Pranav* prosecution witnesses 1 to 4 failed to produce evidence that A3 purchased drugs from A1 and the search was also found to be conducted before the Gazetted officer’s effective presence. The mediators role was also found to be limited. In *PS Sultan Bazar Vs A4 Bontha Parmesh* prosecution failed to produce an FSL report for specific samples during proceedings as to the determination of the drug seized, which relied only a witness testimony. Acquittal of co-accused (A1 – A3 and A5 – A9) also weakened prosecution’s case. The biggest reasons seen overall are that of the Gazetted Officer being from the same department and the mediators being non-locals or “doubtful” interest.

None except for one of the cases were deemed to be categorically “illegal”. In *PS Panchagutta Vs A2 Yogeshwar Goud,* the searches were implied to be illegal due to the mediators turning hostile and admitting that their signatures were obtained in the police station rather than at the scene as legally mandated. In *PS Mahankali Vs Gadepaka Mahesh @ Saidulu @ Sai Mahesh Reddy* the contraband was seized on site before the arrival of the Gazetted Officer therefore

[15] Anand, AS. “SC State of Punjab Vs Baldev Singh on 21 July, 1999.” Press release, July 21, 1999. Accessed July 24, 2025. https://jajharkhand.in/wp/wp-content/judicial_updates_files/10_Narcotic_Drugs/01_search_of_a_person_of_an_enclosed_place_in_a_public_place/State_Of_Punjab_vs_Baldev_Singh_on_21_July,_1999.PDF.

[16] Supreme Court of India, J., Ranjana Prakash Desai, and Madan B. Lokur. “State of Rajasthan Vs Parmanand and Anr.” Legal case. *Supreme Court of India*, February 28, 2014. https://narcoticsindia.nic.in/Judgments/State_Of_Rajasthan_vs_Parmanand_And_Anr_on_28_February_2014.pdf.

rendering the search categorically illegal. The remaining cases are just procedurally flawed in its search execution and does not mention the legal status of the searching process itself.

With regards to the delays in sending samples to forensic labs the cases derive a mix of plain delays sending samples to the forensic labs and the sending of samples prior to inventory certification by the magistrate. The biggest delay seen between seizure to the sending of samples seen is that of approximately 2 months in *PS Panchagutta Vs A2 Yogeshwar Goud. Section 52-A* mandates the promptness with which contraband must be presented in court and be certified for sending samples to forensics. Although it does not specify any specific time frame the NDPS Act and its varied judicial interpretations emphasixe that the process must occur "soon after" or "as soon as may be". Delays of even a few weeks can undermine the prosecution's case by casting doubt on the integrity of the seized evidence.

An inconclusive FSL report is not explicitly mentioned but in *PS Sultan Bazar Vs A4 Bontha Parmesh* the lack of any evidence of samples taken or of an FSL report resulted in the weakening of prosecution's case thus making the FSL process "inconclusive". All remaining cases reported conclusive forensic reports of contraband ranging from *Ganja* to *Methamphetamine*.

Five cases have clearly stated in their judgements that "alleged seized property was also been tampered with" and that the evidence "does not inspire much confidence". The causes for such pronouncements have been the various procedural and legal lapses made during seizure and investigation such as delays in certification and issues with the bias of mediators. While an NDPS charge is considered severe for the accused, the agencies investigating are subject to intense scrutiny in building a *prima facie* case. The courts and the larger legal system are keenly aware of evidence fabrication and misuse at the hands of investigative agencies. Therefore any fabrication of evidence under judicial proceedings is subject to prosecution under *Section 229* of the *Bharatiya Nyaya Sanhita (BNS)*[17].

Witnesses turning hostile seem to be a recurring issue. In *PS Panchagutta Vs A2 Yogeshwar Goud* half the prosecutions witnesses and all the mediators turned "completely hostile". In *PS Bowenpally Vs A2 Erva Bhavani Prasad @ Bittu* the occurrence of total hostility was preceded by lack of support for prosecution's case in material aspects..

The absence of acquittal cases involving smuggling, peddling and cultivation suggest that these are all consumer-level cases. Therefore the cases involving them are possibly subject to the different jurisdiction of agencies such as H-NEW, TGANB or NCB which are more adept at handling higher-level offences.

Overall these findings sheds light on a critical issue within India's drug law enforcement: the law is strong on its face, but the NDPS Act suffers from gross investigative and procedural inadequacies at the grassroots level. It is rare for NDPS cases to get convicted in a state such

[17] Law, Apni, and Apni Law. "Section 229 – Bharatiya Nyaya Sanhita (BNS) – Punishment for False Evidence." ApniLaw, March 30, 2025. https://www.apnilaw.com/bare-act/bns/section-229-bharatiya-nyaya-sanhita-bns-punishment-for-false-evidence/.

as Telangana, where in 2024 only 4 per of 2387 NDPS cases resulted in conviction-sets up a system wherein cases are registered, but mere registration without adherence to legal mandates serves to sustain the stranglehold of drug offenses on society essentially through lack of conviction.

Policy Recommendations

- The issue of delays in preparation and certification of inventory by the magistrate points to the larger issue of judicial pendency where the Indian judicial system, as recent as 2023, held more than 50 million cases pending in the judicial pipeline. .[18] As seen in Fig 6, in the year 2024 a total of 2199 cases were reported, where 964 were pending trial i.e. almost 43.8% of total number of cases. The Law Commission of India, in its 1987 report, initially recommended a significant increase in the judicial workforce, proposing a target of 50 judges per million people. This crucial recommendation was subsequently reinforced by the Supreme Court in 2001 and further endorsed by the Parliamentary Standing Committee on Home Affairs in 2002, underscoring a consistent acknowledgment of the need to boost judicial strength to manage the escalating caseload.[19]
- While specialized state agencies such as TGANB may be proficient with NDPS proceedings, state police in general seem to require capacity building and stricter compliance in terms of adhering to procedure, particularly in seizure, search and court proceedings. Telangana State as an entity overall performs significantly better compared to states such as Bihar or Uttar Pradesh and possesses superior forensic paraphernalia/infrastructure. Creating better capacity for handling NDPS court proceedings within the state law and order infrastructure outside of nodal agencies such as NCB and TGANB is the way forward.

Conclusion

The judiciary's strict scrutiny of procedural compliance, especially concerning mandatory safeguards under the NDPS Act , serves as a vital check against potential misuse of power and fabrication of evidence. While this ensures protection of fundamental rights *(Article 21 of the Indian Constitution)*, it also places a significant onus on investigating agencies to build a robust *prima facie* case that can withstand judicial challenge.

[18] Tnn. "Over 5 Crore Court Cases Pending, Government Tells Lok Sabha." *The Times of India*, December 15, 2023. https://timesofindia.indiatimes.com/india/over-5-crore-court-cases-pending-government-tells-lok-sabha/articleshow/106032857.cms#:~:text=Over%205%20crore%20court%20cases,TOI%20GAMES.

[19] Tnn. "Over 5 Crore Court Cases Pending, Government Tells Lok Sabha." *The Times of India*, December 15, 2023. https://timesofindia.indiatimes.com/india/over-5-crore-court-cases-pending-government-tells-lok-sabha/articleshow/106032857.cms#:~:text=Over%205%20crore%20court%20cases,TOI%20GAMES.

From a policy standpoint, the consistent stress on strict procedural compliance by courts such as in the cases of acquittal gives rise to an immediate need for more relevant capacity-building, better operational aspects, and continuous training of state police and other drug law enforcement agencies. Addressing the pendency in courts, as stressed in a long-pending recommendation by the Law Commission of India to increase the strength of judges , may perhaps indirectly relieve some of the worsening delays for crucial stages such as inventory certification while augmenting the strength of the prosecution in NDPS matters.

The focus of the study was to conduct in-depth analyses of the procedural, evidentiary, and systemic reasons that largely contribute to the acquittal of NDPS cases in the courts at Hyderabad, thus throwing light on the scenario of drug law enforcement in the region compared to state and national trends. The study of ten judgments passed by the Hyderabad Criminal Courts Complex acquitting the accused in NDPS cases reveals serious recurring weaknesses on the part of the prosecution to land in convictions; this was corroborated by qualitative insights drawn from stakeholder interviews.

The findings most unequivocally establish that procedural lapses and unlawful evidence presentation apply in more than 90% of the cases considered for acquittal. Notably, the most recurring and serious flaw had been the courts' disapproval of admission into evidence of confessional statements made to the police or NDPS officers, a view buttressed by the Supreme Court in *Tofan Singh v. State of T.N.*

Limitations

- Sample space is restricted to details provided by the Special Court
- Contradiction made by differences in data provided by Govt reports and those provided by independent news agencies
- Difficulty in collecting statements from individuals holding public office
- Case judgements restricted to Hyderabad Criminal Courts Complex. Does not include Telangana State High Court judgements
- Data Sourcing Restricted to Publicly Available E-Court Services

Research Paper 3

Title:-

Unlocking India's Geospatial Potential: Reforming Policy for Innovation, Inclusion, and Sovereignty

Aryan Gupta

Geospatial information- maps, satellite images, and other spatial data is a basic input into modern-day governance, fueling action in areas such as infrastructure planning and delivery, agricultural productivity, disaster preparedness, response, and, importantly, national security. Recognising the changing economic context and developmental objectives of the Indian state, the Government of India initiated policy reforms to deepen the governance architecture for geospatial and drone technology from 2021-2023. The results were the Guidelines for the Acquisition and Production of Geospatial Data (February 2021), the Drone Rules (August 2021, amended in 2023), the National Geospatial Policy (December 2022), and the Indian Space Policy (2023). Altogether, these documents seek to "strengthen the geospatial sector which eventually contributes to national development, economic prosperity and a thriving information economy" and empower India to leverage spatial technologies for innovation and inclusive growth.

India made important advances in the status of the geospatial data regime through these policies. With the aim of liberalising access to geospatial data, inspiring follow-on innovation from the private sector, and increasing national data sovereignty and security. The policy architecture of geospatial data is evolving steadily, and with continued efforts, areas such as regulatory clarity, improved data availability, and stronger engagement models present valuable opportunities for further refinement and growth. Addressing these challenges will ensure that the government's ambitious reforms achieve their full transformative potential. With a focus on global best practices, this policy paper will highlight core challenges and offer specific reforms to promote a nimble, inclusive, and innovation-oriented geospatial system.

This paper examines India's geospatial data framework, highlighting areas where regulatory structures can be streamlined or clarified, and identifies opportunities to better align them with the nation's aspirations for inclusion, innovation, and sovereignty. The paper systematically adopts a comparative approach to identify global best practices by investigating the geospatial policies of frontrunners such as Singapore, the United States, the United Kingdom, the European Union and Australia.

The document provides different and actionable policy proposals to the Government of India with an emphasis on short-term opportunities. Central priorities are opening up geospatial data access and usability, protecting national and individual rights, enabling innovation and start-up efforts, and allowing inclusive participation across all three sectors. This analysis draws upon valid and reliable government sources and policy documents, which adds to its rigour and credibility.

BACKGROUND

National Geospatial Policy (2022). The NGP 2022 is a high-level policy document issued by the Department of Science & Technology. It builds upon the 2021 liberalisation guidelines, which, for the first time, allowed Indian companies (and approved foreign entities) to acquire, process and commercially distribute the data. The NGP 2022 reiterates this trajectory: it is explicitly "citizen-centric" and "aims to promote private sector participation through continued enhancements of Ease of Doing Business in the sector". Its stated vision is "to make India a world leader in the global geospatial space" and to leverage geospatial information for service delivery, economic growth, and national security. Key features of the NGP include:

- Open Data Mandates: The policy declares that Survey of India topographic data and other geospatial data generated with public funds will be treated as "common good" and "made easily available". It explicitly calls for "open standards, open data and open platforms". The intent is to liberalise data sharing and spur innovation by making government-collected data accessible.
- Institutional structure: NGP establishes a Geospatial Data Promotion and Development Committee (GDPDC), and this will act as the peak coordinating body. This Committee (different from prior inter-ministerial committees) will include members from a sectoral, state, and central government, private and academic, and civil society perspective. The committee will make recommendations on rules, standards, and project oversight.
- Geographic Goals: The policy aligns with national goals, which explicitly include support for "Atmanirbhar Bharat" ("self-reliant India") through encouragement for Indian companies to produce their geodata. It embraces the UN's Integrated Geospatial Information Framework (IGIF) for best practices. It commits to "innovation" – enabling startups and bridging the geospatial digital divide. It also calls for strengthening geospatial education, standards development, and subnational (state-level) coordination.

Drone Rules (2021, 2023). The regulation of drones in India is mandated under the Drone Rules, 2021 (MoCA), regulated under the Aircraft Act. The Drone Rules classify unmanned aerial vehicles (UAVs) as "drones" according to their weight and intended use of the drone. Also, the UAVs must have a Unique Identification Number (UIN) to operate legally, and nearly all commercial UAV operations must obtain a UAOP to operate legally.

The rules distinguish red/yellow/green zones (not allowed to fly or limited areas), as well as requiring an operator to get a permit to operate near a facility or sensitive area or airport. Notably, the 2021 rules abolished prior mandatory security clearances (streamlining approvals) and introduced a digital portal ("Digital Sky") for licensing. While India has significantly liberalised its drone ecosystem through the Drone Rules, 2021 and subsequent amendments, certain operational restrictions remain. For instance, Beyond Visual Line of Sight

(BVLOS) flying is still tightly regulated and permitted only under specific trials and approvals. The 2023 amendment further eased access by allowing a wider set of government-issued identity documents for pilot certification, thereby broadening participation. Nonetheless, commercial drone operations often require coordination with multiple agencies such as DGCA and security authorities, which presents opportunities for streamlining to better align with India's innovation and growth aspirations. Remote Sensing Data Policy (RSDP). India's RSDP (2011, DOS/ISRO) tightly controls satellite imagery. The government (through ISRO's NRSC) is the *sole and exclusive owner* of data from Indian satellites, licensing it to users. Any entity wishing to acquire/distribute remote-sensing data (from Indian or foreign satellites) within India must obtain a license from the nodal agency. In practice, this means NRSC operates a de facto monopoly on high-resolution imagery, granting only usage licenses. The RSDP permits the government to withhold or restrict data, citing security or foreign policy. Over time, this restrictive stance has drawn criticism for limiting civilian access and private innovation.

Implementation Status

Many aspects of these policies are in the process of being implemented, reflecting the scale of ambition behind the National Geospatial Policy (NGP). Its goals, such as promoting open data, nurturing a vibrant start-up ecosystem, and introducing geospatial thinking in schools, set a strong foundation for future progress. Initiatives like a national spatial data portal and upgraded Survey of India map products are underway, and further momentum is expected. While the Digital Sky platform continues to evolve and RSDP maintains strict controls on foreign satellite imagery, these challenges present valuable opportunities for refinement. In this context, a critical analysis of existing gaps can play a constructive role in guiding the next phase of policy advancement.

Thematic Pillars of the National Geospatial Policy

The National Geospatial Policy 2022 identifies **14 "fundamental data themes"** (Annexure-II) spanning the full spectrum of mapping and spatial data: 1) Geodetic Reference Frame; 2) Ortho imagery; 3) Functional Areas (Administrative Boundaries); 4) Geographical Names; 5) Elevation and Depth; 6) Water; 7) Transport Networks; 8) Buildings and Settlements; 9) Land Cover and Land Use; 10) Physical Infrastructure; 11) Land Parcels; 12) Addresses; 13) Geology and Soils; and 14) Population Distribution.

In practice, **progress on these themes is uneven**. For example, the Survey of India has expanded its geodetic network – over 1,000 Continuously Operating Reference Stations (CORS) are now online – but the full modernised geodetic frame (with 2025 goals for an updated datum and geoid) is still in progress. High-resolution satellite imagery and elevation data exist (ISRO's Cartosat-1 mission has generated national DEMs and orthoimage strips), but much of this data remains non-public or limited by policy (IN-Space now requires special authorisation for sub-30cm resolution data).

Administrative and address data in India remain fragmented. State land record systems (for example, Karnataka's Bhoomi) and urban cadastral pilots (such as NAKSHA's urban land parcel mapping in many ULBs) are advancing. However, there is not yet a single, fully operational national cadastre or unified address registry covering all regions. Under DILRMP, most village land rights records have been digitised and many cadastral maps are being digitised and geo-referenced, but considerable work remains to integrate all parcels, addresses and ownership information uniformly across the country. Datasets on water, land use, infrastructure, and other sectors are managed across multiple ministries and agencies, and while full integration is a work in progress, there are promising developments underway. For example, the Geological Survey of India is establishing the National Geoscience Data Repository (NGDR), and the NSDI under Department of Science and Technology, is building out the National Data Registry and Clearinghouse for metadata and datasets. Although there is not yet a single, legally mandated unified geospatial data portal that covers all ministries, the National Geospatial Policy 2022 provides a strong framework for coordinated data sharing, interoperability, and eventual centralization.

KEY CHALLENGES

1. Control of Data Access and Limiting Licensing

- The Guidelines for Geospatial Data, in 2021, were aimed at removing old restrictive regimes such as the Remote Sensing Data Policy, but publicly funded datasets are increasingly being opened up; however, legacy frameworks and implementation processes still need to be aligned with the government's new liberalisation efforts. Streamlining these transitions will help fully unlock the intent of recent reforms.
- Even though formal licensing has been simplified, we are impeded by operational challenges like sensitive data types, platform limitations, or the complexity of institutional responsibilities, which still limit creative opportunities and participation.
- The Overly Restrictive Data Licensing, despite NGP 2022's call to treat publicly-funded geodata as a common good, the old RSDP still requires licenses for virtually all remote-sensing data. In practice, a company cannot freely download satellite imagery for innovation; it must apply to the NRSC or an authorised agency. Survey of India topographic maps are generally offered for sale or under licence rather than being entirely free, especially for detailed or vector data products. Some maps and formats, such as Open Series Map PDFs at 1:50,000 scale, are now available for free download. Higher-resolution or full-layer maps, however, often carry licensing fees, while maps with restricted or sensitive content remain under tighter control. These emerging free-access offerings, alongside ongoing efforts to improve availability and transparency, are welcome steps toward more open geospatial data distribution. Maps at 1:50,000 scale have limited use, though they exhibit the intent to make the data available. This approach is gradually shifting towards global trends of openness, but further simplification will help India fully align with

international best practices. The ambiguity between promoting open data and retaining control creates confusion among users.

2. **Bureaucratic Complexity:**

- Too many agencies are regulating geospatial data and drone operations with little oversight during the processes.
- While the Digital Sky platform has introduced structured workflows and set indicative timelines (for example, 60 days for RPTO authorisations and 2 working days for UIN issuance when all documentation is complete), in practice some approvals still experience delays, particularly in cases requiring inter-agency coordination, the submission of complete zonal data, or security clearances. These challenges represent clear areas for streamlining, which the ongoing migration to the eGCA portal aims to address.
- The Bureaucratic Overlap and Complexity occur when Multiple agencies have overlapping authority. For instance, the Ministry of Science (DST) issues geospatial guidelines, DoS/ISRO issues satellite data licenses, DGCA/DGCA issues drone approvals, and the Home Ministry can intervene for security grounds. The NGP's new GDPDC will coordinate policy, but its powers are not clearly defined. On drones, a single flight may need DGCA permission, AAI permission near airports, and Defence clearance near certain facilities. The technology-neutral goals of NGP and drone rules are thus hampered by heavy, multi-layered approvals. Stakeholders acknowledge that 'ease-of-doing-business' has significantly improved with initiatives like the Digital Sky portal. However, refining operational processes and reducing delays would further enhance the effectiveness of these reforms.

3. **Implementation Shortfalls:**

- The National Geospatial Policy (2022) provides a strong foundation, defining standards and interoperability requirements and charting a path toward establishing a national geospatial data portal. Many key infrastructural elements are already underway - for example, the National Data Registry under NSDI, published BIS standards for metadata and data exchange, and open APIs in policy guidelines. While full nationwide integration is still evolving, the momentum is clear, and ongoing development promises increasingly unified and accessible geospatial data infrastructure.
- It is unclear whether start-ups that are working to provide useful applications for entrepreneurs or researchers can obtain datasets to access such basic things as maps of natural resources or property parcel data, and which agency might be able to support them in an application to enable the use and creation of this type of data.
- The National Geospatial Policy 2022 sets a clear vision for the democratization of geospatial data, emphasizing open standards and interoperability. While the National Geospatial Data

Repository (NGDR) is still under development, recent initiatives, such as Maharashtra's plan (**MahaAgri-AI Policy 2025-2029**, the **MahaTech** program, and the **MahaBHUMI** project, to establish a robust geospatial ecosystem, are indeed positive steps. The state is also participating in the national **Operation Dronagiri** pilot project.) to establish a dedicated institution for geospatial technology, demonstrate a commitment to advancing this vision. These efforts signify a positive trajectory toward enhancing data accessibility and integration across states and agencies.

4. **Low Integration Across State and Local Agencies**
   - Most geospatial activity occurs at the subnational level, yet state governments lack mandates and/or support to be in alignment with a national policy. The NGP speaks of sub-national arrangements, but there is no mandate or funding for state geospatial missions. State governments often still restrict data (e.g. state satellite imagery or surveys). In contrast, countries like the US embed local governments in NSDI planning. The absence of a national-local coordination mechanism means data silos persist, and local needs (e.g. vernacular mapping, community planning) are under-supported.

5. **Lack of Inclusion and development of capacity**
   - Policy rhetoric strongly emphasises inclusion, and further dedicated initiatives for women, rural youth, and start-ups can build on this commitment.
   - India’s geospatial data framework, guided by the RSDP and the Digital Personal Data Protection Act, reflects a strong emphasis on national security while gradually opening avenues for innovation. The RSDP mandates authorization for high-resolution satellite data, ensuring sensitive information is protected, while the DPDPA addresses personal digital data, though its applicability to geospatial data is still evolving. Initiatives like the National Geospatial Data Repository (NGDR) under the GDPDC are underway to centralize and democratize access, signaling a positive shift toward greater data availability. At the same time, there remains a need for clearer guidance on data retention, cross-border sharing, and privacy, especially location data, to reduce uncertainty for innovators and citizens. Developing a nuanced framework that encourages open access for non-sensitive geospatial data, while restricting only genuinely sensitive information, can align India with global best practices and accelerate the responsible use of geospatial information.
   - Innovation and Inclusion Not Fully Embedded: The NGP and drone policy laud innovation and inclusive growth. Yet on the ground, few schemes empower underrepresented groups. There is no special program for training women or rural youth in geospatial sciences, even though the policy calls for introducing geospatial thinking from school onwards. Startup incentives (like tax breaks or accelerators) have been announced (e.g. “Mission Dronagiri” centres), but these

remain small-scale. Intellectual property generation and skilling lag. Other countries demonstrate the payoff of inclusion: Singapore's master plan explicitly aims to "benefit more segments of society", and the EU views geodata as an innovation platform for all industries. India's current gap means many potential entrepreneurs or researchers lack the data or training to participate.

- In summary, India's geospatial policy framework reflects a promising vision of liberalization, while balancing the need for oversight and security. This creates an evolving ecosystem that is gradually consolidating the government's commitment to open data and fostering innovation lays a strong foundation, yet entrepreneurs sometimes encounter procedural hurdles and limited access to datasets. Addressing persistent challenges, such as licensing complexities, overlapping institutional responsibilities, and the absence of streamlined data-sharing mechanisms, will be crucial. Successfully resolving these issues will enable India to fully harness its potential and emerge as a global leader in geospatial innovation.

COMPARATIVE ANALYSIS

India's geospatial reforms can be informed by global leaders. The table contrasts India's approach with exemplar practices in Singapore, the USA, the UK, and the EU. In leading jurisdictions, **unified frameworks** and open data are the norm.

For instance, the **USA** enacted the Geospatial Data Act (2018) to codify an NSDI, mandating all federal agencies coordinate under the FGDC and publish geodata (e.g. free Landsat, NOAA data).

The **UK** created a Geospatial Commission (2018) to drive a location data strategy; Ordnance Survey now makes most mapping products free and open.

The EU requires member states to harmonise (standardise) spatial datasets (via the INSPIRE directive) and provides open access for its Copernicus satellite data.

Singapore has OneMap, an integrated base-map system, and offers land-use and environmental layers in one portal.

These systems support private innovation: all of the above countries provide grants, incubators or challenge prizes to encourage geospatial startups and R&D.

By contrast, India's ecosystem is in transition-fragmentation remains, but initiatives like the NGP and GDPDC are promising moves toward harmonisation. Compared to global peers, India is now aligning its frameworks more closely with best practices. The NGP is a move towards harmonisation/concordance; however, to be effective, it has to imitate these best practices from around the globe: create one nodal body coordinating between central and state obligations (like FGDC/NGAC or the UK's Ordnance Survey's effective partnership), adopt open standards, and employ open-source tools.

1. **REPUBLIC OF INDIA**			
Policy Framework & Coordination	**Data Access & Open Data**	**Innovation & Private Sector Support**	**Standards & Open-Source**
Multiple agencies (DST, DoS, DoLR, etc.) share NGP implementation. GDPDC (under DST) oversees coordination, but has limited legal authority to enforce integration. NGP reforms still await legislation for permanence	Recent liberalization under NGP/Guidelines (2021) makes *government-funded* maps and data freely accessible to Indian users . However, no central open-data portal yet (NGP's promised repository is still under development). High-resolution or security-sensitive data remains restricted.	India's National Geospatial Policy 2022 fosters innovation and private sector engagement, with initiatives like Operation Dronagiri. Expanding data access, funding, and streamlined regulations can further strengthen a vibrant geospatial ecosystem.	NGP endorses open standards (OGC, ISO) and IGIF compliance, but adoption is uneven. NIC's BharatMaps uses OGC services . Many agencies are still using proprietary formats, or older standards.

2. **REPUBLIC OF SINGAPORE**			
Policy Framework & Coordination	**Data Access & Open Data**	**Innovation & Private Sector Support**	**Standards & Open-Source**
Whole-of-government model: single	OneMap platform provides open base maps	Active support: govt agencies run hackathons,	Government systems use international standards

government bodies (e.g. Land Transport Authority) manage geospatial policy. Master Plan 2040 uses geoplanning across agencies.	and land-use data; a national data portal (data.gov.sg) publishes agency datasets (open APIs for demographics, transport, etc.). No data localization laws.	sponsor startups (e.g. OnePAHUB incubator). Regulatory sandbox (Monetary Authority) allows data sharing trials. Plentiful tech grants for Smart Nation projects.	(ISO 191xx). Singapore agencies often leverage commercial software but data is shared via standard APIs (REST, WMS). OpenStreetMap has broad usage for last-mile applications.

3. UNITED STATES OF AMERICA			
Policy Framework & Coordination	**Data Access & Open Data**	**Innovation & Private Sector Support**	**Standards & Open-Source**
NSDI approach: FGDC (Federal Geographic Data Committee) coordinates all 50+ agencies under the Geospatial Data Act . National Address Database initiative led by White House.	High emphasis on open data: USGS (Topo, satellite), NOAA (weather, LIDAR), Census, etc. All Federal data inventories are catalogued on data.gov and GeoPlatform. States also run open data portals.	Strong supportive ecosystem: NASA, NSF and NOAA have SBIR/STTR grants to spur geo-startups USGS Crowdsourcing Grants, Esri grants, and DARPA challenges. Tech incubators (e.g. Digital Sandbox) often include GIS.	The US uses OGC/ISO standards across federal data (e.g. FGDC's CSDGM, now ISO 19115 metadata). Open-source GIS (like GDAL, QGIS) are widely used in government and academia. The USGS supports open data science.

4. UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

Policy Framework & Coordination	Data Access & Open Data	Innovation & Private Sector Support	Standards & Open-Source
Unified by national and devolved agencies. The UK Geospatial Commission (hosted in Cabinet Office) works with Ordnance Survey (lead mapping agency) and heads a pan-UK strategy . Regional GIS consortia coordinate with OS (e.g. Scotland's GI strategy).	OS's *OS OpenData* makes topographic maps free. Data.gov.uk includes local and national geodata (e.g. environment, planning data). Many public datasets have permissive licenses. The UK also invests in open-source (standard OGC) solutions for interoperability.	UK offers funding via Innovate UK and Ordnance Survey (Geovation accelerator) for geotech entrepreneurs. R&D tax credits and Catapult centers (e.g. Geospatial Commission-backed urban catapult) bolster innovation.	The UK mandates OGC standards for public geodata (e.g. INSPIRE standards). Open-source platforms (QGIS, PostGIS) are common in local gov. The Ordnance Survey makes APIs available openly and supports organisations developing programs using the data offered through LE1379.

5. <u>EUROPEAN UNION</u>			
Policy Framework & Coordination	**Data Access & Open Data**	**Innovation & Private Sector Support**	**Standards & Open-Source**
The INSPIRE directive requires all member states to have common spatial data infrastructure. The following EU lails provide common data sets (EU uses same data to populate Eco-Status web applications).	Data that is INSPIRE compliant includes thematic maps, land registry excerpts, and is using national geoportals to access (e.g.: data.gouv.fr, data.gov.ie). Copernicus is providing free access to satellite imagery. The	Horizon Europe and national innovation programs fund geospatial R&D (e.g. Galiléo startups). European Space Agency Business Incubation Centres (like London & Denmark) nurture space/GIS startups. The	EU projects require open standards (e.g. INSPIRE schemas). Many EU-funded geo-platforms are open-source (e.g. INSPIRE Geoportal). Member states also contribute to OSGeo initiatives.

Although the EU offers guidance, many local agencies have established additional constraints. For example, in the case of European share data guidelines for drone licenses (EASA, and common data for urban and regional planning).	European Union is promoting open source development in projects that are funded by EU (such as Copernicus Open Hub developed in open source and is using open source tools). GDPR shapes data release policies.	EU Geo-innovation Awards recognize private contributions.	

This comparison shows India's National Geospatial Policy (NGP) 2022 marks a significant step toward liberalizing geospatial data access, yet challenges persist in its implementation. While the policy aims to promote open data and public-private partnerships, the actual private sector involvement remains limited, and the innovation ecosystem is still developing. The government's commitment to fostering start-ups is evident, but concrete incentives are yet to be fully realized. Additionally, administrative complexities, including multiple oversight bodies and unclear data-sharing rules, contrast with the more streamlined frameworks observed in other countries. Addressing these issues will be crucial for India to realize its potential as a global leader in geospatial innovation.

Data Infrastructure & Governance

India possesses significant geospatial assets in different agencies, but they must be better integrated. For example : Indian Railways Integration of RFID and GAGAN for Enhanced Operations.

India Railways has effectively harnessed geospatial technologies to bolster operational efficiency and safety. A notable example is the integration of Radio Frequency Identification (RFID) technology and the GPS Aided Geo Augmented Navigation (GAGAN) system.

RFID Implementation for Asset Tracking

Indian Railways has initiated a comprehensive RFID project aimed at automating the identification and tracking of rolling stock, including wagons, coaches, and locomotives. By 2022, the goal was to equip all rolling stock with RFID tags, enhancing the accuracy and speed of asset tracking across the vast railway network. Trackside RFID readers installed at key locations automatically capture data from passing tagged assets, transmitting this information to central servers for real-time monitoring and management.

GAGAN Integration for Navigation and Safety

To further enhance operational safety, Indian Railways has collaborated with the Indian Space Research Organisation (ISRO) to utilize the GAGAN system. GAGAN, a satellite-based augmentation system, provides precise navigation support by improving the accuracy of GPS signals. This system assists in mapping railway routes, monitoring encroachments, and ensuring safety at unmanned level crossings by providing real-time location data to control centers, even in areas with limited mobile connectivity.

These integrated technologies exemplify how Indian Railways is leveraging geospatial innovations to modernize its operations, enhance safety measures, and improve asset management, thereby contributing to the development of a robust data infrastructure and governance framework.

The RFID project for rolling stock tracking was implemented by the Centre for Railway Information Systems (CRIS) under the Ministry of Railways, with oversight from the Railway Board. Indian Railways collaborated with ISRO to integrate the GAGAN satellite-based navigation system, enhancing operational safety, accurate mapping, and monitoring of assets across the network.

Another example in this domain would be the integration of geospatial data with the OneView Space Management (OVSM) system which is crucial for future planning, particularly in initiatives like the FASTag and GPS-based tolling systems. These systems rely on precise geospatial data to manage and optimize the movement of vehicles on national highways.

Geospatial Integration in OVSM and Tolling Systems

The Ministry of Road Transport and Highways (MoRTH), through the National Highways Authority of India (NHAI) and its subsidiary, Indian Highways Management Company Limited (IHMCL), is spearheading the implementation of a Global Navigation Satellite System (GNSS)-based Electronic Toll Collection (ETC) system. This system utilizes satellite-based tracking to charge tolls based on the distance a vehicle travels on toll roads, aiming to replace the existing FASTag system. The GNSS-based system is designed to operate in a hybrid model alongside FASTag, with both systems functioning simultaneously at selected toll plazas.

A key component of this system is the creation of geo-referenced maps of the highway network, with precision up to the decimeter level. These maps delineate the main carriageway, service roads, and elevated portions, ensuring accurate distance calculation for tolling purposes. The geo-referenced data is essential for the system's operation, enabling real-time tracking and toll calculation based on the vehicle's location.

Oversight and Committee Involvement

The implementation of the GNSS-based tolling system is overseen by the Ministry of Road Transport and Highways (MoRTH), with the National Highways Authority of India (NHAI) and Indian Highways

Management Company Limited (IHMCL) playing pivotal roles. The IT Taskforce report, 2016 , by Ministry of Road Transport and Highways, Government of India has been actively involved in the planning and implementation of the GNSS-based tolling system.

Additionally, a workshop was organized by IHMCL with fintech companies to explore innovative applications of the FASTag system, focusing on aspects such as regulatory compliance, grievance redressal, security, and non-toll applications. This workshop indicates a collaborative approach involving various stakeholders in the development and expansion of the FASTag ecosystem.

The **Survey of India** (SoI) is the official mapping agency (topographic maps, geodetic surveys) under the DST; the 2024 Survey of India (Group 'A') Service Rules update aims to modernise its mandate. The **National Informatics Centre (NIC)** has launched the "Bharat Maps" platform – a multi-layer GIS service with tiled base maps up to 1:4,000 scale, geocoding, and map APIs that central and state e-Gov applications can embed. ISRO's **NRSC** provides satellite imagery and derived maps via its Bhuvan portal (including free DEM downloads).

Other specialised centres (e.g. GSI's Bhukosh geoportal, NSDA's NBDM) maintain siloed datasets , highlighting the fragmented nature of India's Geospatial ecosystem. A new Geospatial Data Promotion and Development Committee (GDPDC) under DST is intended to appoint lead agencies for each theme, but it currently lacks clear authority to mandate data sharing or enforce interoperability across departments.

Urban land records are being digitised: the *NAKSHA* program (under DoLR) is mapping urban parcels and utilities in dozens of cities via drones and GIS. The next step is to harmonise these urban datasets with rural cadasters and Survey of India (SoI) maps, a process that could significantly enhance national spatial accuracy. To improve data usability nationwide, India must advance cross- institutional coordination and adopt open-data standards. For example, linking SoI topo-maps with NIC's BharatMaps reference data and state land portals (Bhoomi, e-Dhara, etc.) could, in principle, enable seamless and interoperable map layers. However, this remains more aspirational than operational, as integration is currently constrained by differences in data formats, licensing regimes, and institutional silos across agencies. Adopting IGIF- inspired architecture and open licenses would help reduce these barriers: many valuable datasets are still "locked" within agencies despite the NGP's stated commitment to democratisation.

The Union Cabinet approved a **National Geospatial Data Repository (NGDR)** in 2024, aiming to serve as a central platform for geospatial data across sectors. Linking states and departments into the NGDR will require coordinated governance and clear standards. To ensure interoperability, datasets (e.g., cadastral maps, address tables) should be published in open, OGC- complaint formats and accessible via standards APIs, enabling seamless integration across platforms. Strengthening governance through formalized NGP reforms, empowering the GDPDC or a similar body to ensure compliance, and implementing a unified geoportal for all ministries and states will create a more coordinated, efficient, and scalable geospatial ecosystem.

In summary, stronger governance can be achieved by formalizing the NGP reforms, empowering the GDPDC or a similar body to ensure compliance, and implementing a unified geoportal that integrates contributions from all ministries and states, paving the way for a more coordinated and efficient geospatial ecosystem.

Private Sector Development

India's private geospatial industry is still nascent and faces multiple hurdles. Though policy now invites private innovation, in practice, the private sector is still at an early stage, but with initiatives like IN-SPACe PPPs and National Geospatial Data Repository, the environment is increasingly favourable for growth. India's geospatial startup ecosystem is rapidly evolving, with many firms initially focusing on GIS applications and analytics. Some of these startups have expanded their offerings, developing advanced satellite imaging, digital mapping, and location-based solutions that serve diverse sectors such as agriculture, mining, and environmental monitoring. These examples demonstrate the potential of India's private sector to drive innovation in geospatial technologies, highlighting the need for policies that further support startups through data access, funding, and streamlined regulations.

Venture capital for deep mapping and EO ventures is scarce. Moreover, private firms often lack timely access to high-quality data (some of which is still government-restricted), curbing the pipeline of product development. Participation in policymaking has been limited, but feedback suggests that regulatory rules are not sufficiently co-developed with the sector.

To stimulate growth in India's geospatial sector, public-private partnerships (PPPs) and targeted incentives can play a constructive role, complementing ongoing efforts under the National Geospatial Policy (NGP). Initiatives such as the IN-SPACe PPP for indigenous Earth Observation satellites and DST's proposal for a PPP-driven National Geospatial Data Repository demonstrate the potential of collaborative models. Building on these, there is scope to explore structured PPP mechanisms that allow startups and SMEs to contribute to tasks such as updating topographic maps or disaster models, while adhering to national standards and procurement norms.

In addition to financial incentives-such as R&D tax credits, duty exemptions for geospatial hardware/software, or accelerated depreciation for capital expenditure-knowledge transfer remains crucial. Collaborative arrangements with institutions like ISRO or NIC, including joint R&D labs and temporary expert exchanges between government and private sector, could enhance technical capacity in a measured and scalable way.

Supporting geospatial startups beyond the seed stage is also important. Government accelerators, including Atal Innovation Mission centres, could incorporate dedicated tracks for geo-tech ventures that link proof-of-concept to product-market readiness, while tracking progress through metrics such as the number of startups incubated, follow-on funding raised, and patents filed.

The broader goal is to evolve from a "startup ecosystem" to a robust geospatial industry ecosystem. This requires ensuring private-sector input in governance, for example through designated seats on NDIA or GDPDC, and introducing competitive innovation grants modelled on NASA SBIR or EU Horizon programs. Ultimately, the success of the National Geo-mission will depend on deliberate incentives, structured partnerships, and a focus on bridging government-held data with innovators, all implemented with an understanding of India's technical and administrative complexities.

The intersection of Emerging Technologies, Privacy, and Security

Geospatial QR Tracking System for Waste Management

Cities are increasingly leveraging emerging technologies-such as geospatial analytics, AI, and IoT-to improve urban service delivery and operational efficiency. Indore, for instance, has demonstrated how technology-enabled systems can enhance waste management, optimize coverage, and provide actionable insights for policymakers. Such examples highlight the potential of integrating innovative digital tools into governance frameworks while maintaining attention to privacy, security, and scalability.

QR Code Tagging of Bins

- Every waste bin across the city is assigned a unique QR code.
- These codes are linked to a centralized geospatial database, recording each bin's exact location using GPS coordinates.
- The data ensures that every bin can be tracked in real time and mapped spatially to monitor coverage and efficiency.

Integration with Collection Vehicles

- Waste collection trucks are equipped with mobile scanning devices or smartphones.
- When a truck collects waste, operators scan the QR code on the bin.
- The scan updates the central system in real time, confirming that the bin has been serviced.

Geospatial Mapping, AI & Analytics

- All scanned data is fed into a GIS-enabled dashboard, showing the precise locations of collected bins, missed pickups, and service gaps.
- AI and machine learning algorithms analyze historical data to optimize collection routes, forecast peak waste generation times, and enhance operational efficiency.
- IoT sensors in select bins monitor fill levels, providing predictive insights for collection planning.

Accountability, Privacy & Performance Monitoring

- Each scan is timestamped and linked to the specific operator, enabling performance monitoring and accountability.
- Privacy measures ensure that data collection is limited to operational purposes, without capturing personal information.
- Citizens can access reports on service coverage, enhancing transparency.

Impact on Urban Sanitation

- This integration of QR codes, geospatial mapping, AI, IoT, and real-time analytics has allowed Indore to maintain systematic waste collection, prevent bin overflow, and ensure timely disposal.
- The city has consistently been ranked as India's cleanest city, demonstrating the transformative potential of emerging geospatial and digital technologies in secure and efficient urban governance.

The above is one of the example of how GIS is integrated with other technologies resulting the best outcome. AI, machine learning, and computer vision approaches are accelerating the impact geospatial applications in ways that are not predictable, even static environment (e.g.: automatic extraction of features layer from imagery, and predictive analysis for land use allocation), etc., real-time routing for traffic). India has already begun exploring these new technologies (e.g., IITs, space agencies applying AI to agriculture, urban planning), but they also introduce very serious privacy and security issues. Geospatial sensors routinely capture personal data: faces, license plates, movement patterns and even biometric identifiers can be recorded in street images and video.

Under India's forthcoming Digital Personal Data Protection Act (2023), such incidental collection of personal data will require consent or justified exemptions. In practice, obtaining consent from every identifiable individual in public is infeasible (e.g. street-view or drone surveys). A technical mitigation is already envisioned: survey cameras must blur or mask faces and number plates at the point of capture. Legally, adopting the "reasonable expectation of privacy" principle (as in many Western jurisdictions) could clarify that truly public imagery may not count as personal data requiring consent. Data security also must adapt: geospatial platforms increasingly rely on potentially vulnerable hardware. For instance, concerns have been raised about foreign-made cameras and drones that transmit data over external networks. India's IN-SPACe now requires foreign satellite imagery to be accessed only via JV or authorised channels.

The same safeguards should apply to imaging devices (such as local storage requirements for CCTV, and certified devices for public-sector uses). In addition, any policy framework need to specifically incorporate ethical standards - for example, articulating principles around privacy as per the UN's Integrated Geospatial Information Framework (IGIF), and taking lessons from international peers on best practices, data protections for biometric data, such as the EU GDPR, or operating principles around surveillance cameras in the United Kingdom.

In conclusion, a future-ready geospatial policy should have established principles around privacy-by-design and security-by-design. This includes public agencies and private firms using strong encryption, access controls, and data minimisation (for example, strip when without significant loss of meaning possible, or use coarse accuracy where fine detail is unnecessary). Public awareness campaigns can also educate citizens about location data rights. By aligning with international norms (GDPR, IEEE ethics standards, IGIF), India can leverage AI/ML in GIS while safeguarding its citizens – an imperative if India is to be trusted as a global leader in geospatial governance.

Aspect	Public Sector Role	Private Sector Role
Investment & Funding	Central/state agencies fund mapping infrastructure (ISRO, SoI budgets; ₹100 Cr Geospatial Mission in 2025).	Private capital for geospatial R&D is limited, though incubators and targeted programs provide some support. Emerging PPPs, such as IN-SPACe's EO initiative, are starting to bridge this gap.
Data Creation & Access	Government produces core data (topo maps, satellite imagery) and runs portals (NIC's BharatMaps , Bhuvan).	Private companies enhance and deliver geospatial services using public data. Innovators also crowdsource (OpenStreetMap).
Innovation Pipeline	Research labs (IIRS, DoS labs) develop new methods; government tech accelerators (DRDO labs, IIT centers) pilot projects.	Startups remain concentrated in niche geospatial services, with few scaling nationally; stronger support is needed from seed through growth stages.
Engagement & Governance	Policy is led by government (DST, DoS, MoRD) with occasional advisory input from industry bodies.	Industry associations (AGI, SFF) lobby for reforms; their participation is growing but still informal. Formal inclusion in decision bodies (GDPDC, parliamentary committees) is limited.

1. **Rethink and accelerate timelines.**

The implementation timelines set out under the National Geospatial Policy (NGP) for several thematic areas, such as NGDR integration and national GIS infrastructure, extend to 2035, which may slow sectoral transformation. To expedite progress, the Government could develop time-framed, outcome-based roadmaps with accelerated milestones-for instance, achieving initial nationwide NGDR integration by 2030 rather than 2035. Accelerated timelines would enable earlier realization of benefits such as improved disaster response, more efficient urban planning, and faster commercialization of geospatial services. These roadmaps should be publicly available, linked to annual targets, monitored by a senior-level oversight body, and complemented with a performance dashboard to track compliance and progress in real time.

2. **Activate thematic workstreams with the lead agency**

India's thematic governance approach spans 14 distinct areas, each led by a designated Ministry or agency, with progress actively monitored by bodies such as GDPDC and DST. To further strengthen coordination and transparency, inter-agency working groups could complement existing monitoring, and selected progress summaries could be periodically shared with relevant stakeholders. Adequate allocation of technical and human resources to each theme will ensure sustained momentum, facilitate cross-sectoral collaboration, and enable more informed policy decisions without duplicating existing reporting mechanisms.

3. **Require the Private Sector to Cooperate in Service Delivery**

Private sector engagement in geospatial service delivery remains underutilized, limiting innovation and competition. Government agencies often provide services that could be competitively procured, which can crowd out private investment. To address this, private-sector participation should be institutionalized through formal mechanisms such as public–private partnerships, competitive tendering, and contractual arrangements for non-sovereign services. Government funding should be focused on core sovereign functions and addressing market failures, while incentivizing innovation and efficiency in areas where the private sector has proven capacity.

The Geospatial Data Promotion and Development Committee (GDPDC) plays a central role in coordinating geospatial initiatives across ministries and promoting sector development in line with the NGP. While GDPDC is already facilitating standards, planning, and cross-ministerial collaboration, continued support for its activities-through stakeholder engagement, knowledge sharing, and capacity-building-can enhance its effectiveness and ensure sustained progress in the geospatial ecosystem.

5. Restructure the Funding Channel and Outcome Measures

Current funding sources are limited in scale and purpose, and do focus on sustaining start-ups over other forms of funding and outcomes. We need a more balanced funding mechanism to encourage and support the innovation ecosystem from start-ups through to scale-ups and then established companies. It is recommended that the funding performances shift from kudos about establishing new start-ups to outcomes of product commercialisation, social impact, and interoperability with government systems. Government procurement norms also need to be adapted to allow scale-ready forms of companies, like SMEs and large companies, to participate meaningfully.

6. Expand Substates, Make-up, and Capacity

The effectiveness of the National Geospatial Policy relies on active subnational participation. Many states are already leveraging geospatial technologies, supported by existing sectoral funding and incentive mechanisms such as DoLR's Naksha program. To strengthen outcomes, the Government could focus on improving coordination across states and ministries, sharing best practices, and aligning incentives to encourage innovation and standardized adoption, without creating additional bureaucratic layers.

7. From Policy to Legislation

The geospatial ecosystem in India operates under policy frameworks, which can sometimes face challenges such as variable enforcement or funding unpredictability. Given the rapid evolution of geospatial technologies, establishing flexible guidelines and consolidated regulatory frameworks-drawing together the NGP, Drone Rules, and Remote Sensing Data Policy-may provide clarity, secure investments, and define roles for government and private actors without the rigidity of formal legislation. This approach balances regulatory certainty with adaptability to technological and market developments.

8. National Geospatial Data Portal

- The Survey of India has initiated efforts to develop a national geospatial portal. Policy focus should be on ensuring interoperability, open access, and alignment with international standards, while integrating datasets across agencies to support planning, research, and innovation.

9. Leveraging Drones to Enhance India's Geospatial Capability

India can leverage its geospatial capability through the advancement of drone technology across a unified Drone–Geospatial Infrastructure Framework, which is an inherent part of the National Geospatial Policy 2022. In addition to regulation, the Draft Civil Drone Bill, 2025 should also allow the DGCA, DST and Survey of India agencies to have real-time access (through cloud-enabled secure protocols) to engage in data sharing. To enhance research and protect citizen privacy and ensure that data usage is ethical, the Drone-Geospatial Innovation Fund and the Data Ethics Framework can serve as two important mechanisms for consideration. At the same time, coordinating units at the state-level can promote drone technology while building out skill development centers to support indigenous manufacturing, capacity building and self-reliance. Collectively, this would help position the drone as a significant feature of India's geospatial ecosystem, with the potential to improve innovation, governance and sustainable national development.

10. Remote Sensing Data Policy (RSDP)

- NRSC's Bhuvan provides 5m-resolution imagery free of charge, while higher-resolution datasets (1m or 30cm) are accessible via In-SPACe registration or commercial providers. Policy emphasis should be on streamlining access procedures, promoting private-sector participation, and maintaining consistency with global standards.

11. Drone Regulations

- Drone Rules 2021 have already simplified approvals for low-risk operations and aerial surveys. Policy recommendations should focus on identifying and addressing residual friction points, facilitating inter-agency coordination, and supporting niche applications in areas such as urban planning, disaster relief, and research.

12. Data Governance Implementation

- Existing guidelines classify sensitive versus non-sensitive geospatial data, which agencies can apply without major difficulties. Policy efforts could focus on harmonizing interpretations across agencies and providing clarity for regulated cross-border data flows where applicable.

13. Support Startups and R&D

- Government grants, tax incentives, incubators, and programs like GDPDC have fostered early-stage geospatial innovation. Policy focus should be on specific gaps, such as enabling scale-up funding, streamlining access to specialized datasets, and strengthening collaboration between academia and industry, while recognizing that the ecosystem is developing organically.

14. Inclusive and strategic drone deployment.

- India has a growing domestic drone manufacturing sector, with a range of products accessible to private companies and NGOs. Policy emphasis should be on promoting equitable access to drone technology for public-interest applications, supporting domestic manufacturing, and aligning adoption with national security considerations.

15. Security & Privacy Frameworks:

- Most government geospatial datasets do not contain personally identifiable information, and data is hosted on approved domestic cloud platforms. Policy attention should be on clearly defining any residual security or ethical issues, ensuring compliance with DPDP Act provisions where relevant, and promoting home-grown solutions for sensitive geospatial infrastructure.

These recommendations aim to further strengthen India’s geospatial ecosystem by supporting innovation, inclusion, and national interests. By promoting open-data norms, regulatory clarity, and targeted capacity-building, India can complement existing policies and ongoing industry-academia collaborations, aligning with international best practices and accelerating the adoption and impact of geospatial technologies.

Conclusion

India is primed for a revolution in geospatial policy. To realise this promise, policy needs to transition from promise to practice. A streamlined, inclusive and innovation-oriented geospatial policy will create a climate of sustainable economic, infrastructural and societal growth across governance, disaster preparedness, or other relevant national resilience models. From a pressing course correction now, India can begin positioning itself as a global leader in the geospatial sphere.

Geospatial information and drone technologies provide India with unprecedented and vast opportunities to attain economic development, governance, and societal benefits. The recent actions taken by the Centre clearly articulate this potential by developing an ambitious vision of innovation, inclusivity, and sovereignty. But policy papers alone will not deliver on these ambitions.

Based on our analysis, we believe that some institutional barriers-such as legacy licensing practices, overlapping regulations, and evolving governance structures-still pose challenges. However, with the momentum already created by the government's liberalisation drive, these issues can be addressed to accelerate the sector's growth.

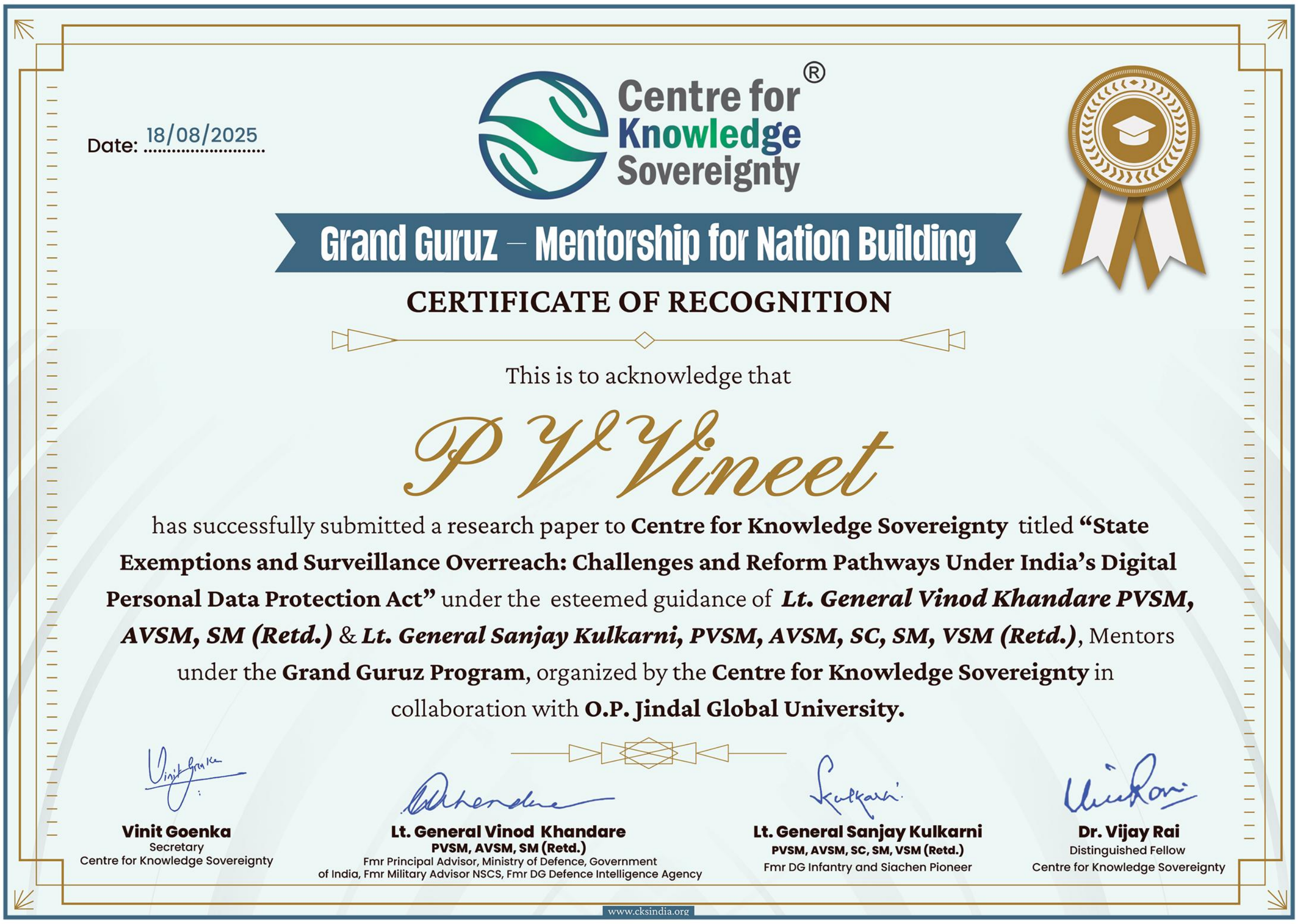
Lastly, it should be possible for India to think more innovatively and copy from the rest of the world to seize the opportunities presented in the space: (1) through openness (i.e., making data openly and broadly available); (2) agree on simplifying a risk-based regulatory framework (i.e., risk low to medium risk activities will have minimal to no regulation) especially in the case of low risk bare-bones models; and (3) aim for institutional arrangements that are seamless across all forms of government, as opposed to traditional top-down hierarchies, and preserve pooled dataset and platform outcomes.

We urge the government to move swiftly on the recommendations outlined above. Establishing an interoperable geospatial data portal, accelerating drone approvals, and nurturing a vibrant Startup ecosystem are not mere administrative measures-they are strategic investments in India's future. Making geospatial data accessible as a public good and creating an enabling environment for its innovative use will unlock significant benefits in disaster management, smart infrastructure, precision agriculture, and many other critical sectors.

Equally important is ensuring that these initiatives are implemented with dual objectives: **Inclusion**, by bringing new communities into the technology ecosystem, and **Sovereignty**, by safeguarding strategic interests while fostering innovation. With the right policy direction, India's geospatial revolution can become a cornerstone of its digital transformation, economic growth, and strategic capabilities in the years ahead.

Certificates of Recognition

Next ▶



Date: 18/08/2025

Centre for Knowledge Sovereignty®

Grand Guruz – Mentorship for Nation Building

CERTIFICATE OF RECOGNITION

This is to acknowledge that

P V Vineet

has successfully submitted a research paper to **Centre for Knowledge Sovereignty** titled **"State Exemptions and Surveillance Overreach: Challenges and Reform Pathways Under India's Digital Personal Data Protection Act"** under the esteemed guidance of ***Lt. General Vinod Khandare PVSM, AVSM, SM (Retd.)*** & ***Lt. General Sanjay Kulkarni, PVSM, AVSM, SC, SM, VSM (Retd.)***, Mentors under the **Grand Guruz Program**, organized by the **Centre for Knowledge Sovereignty** in collaboration with **O.P. Jindal Global University.**

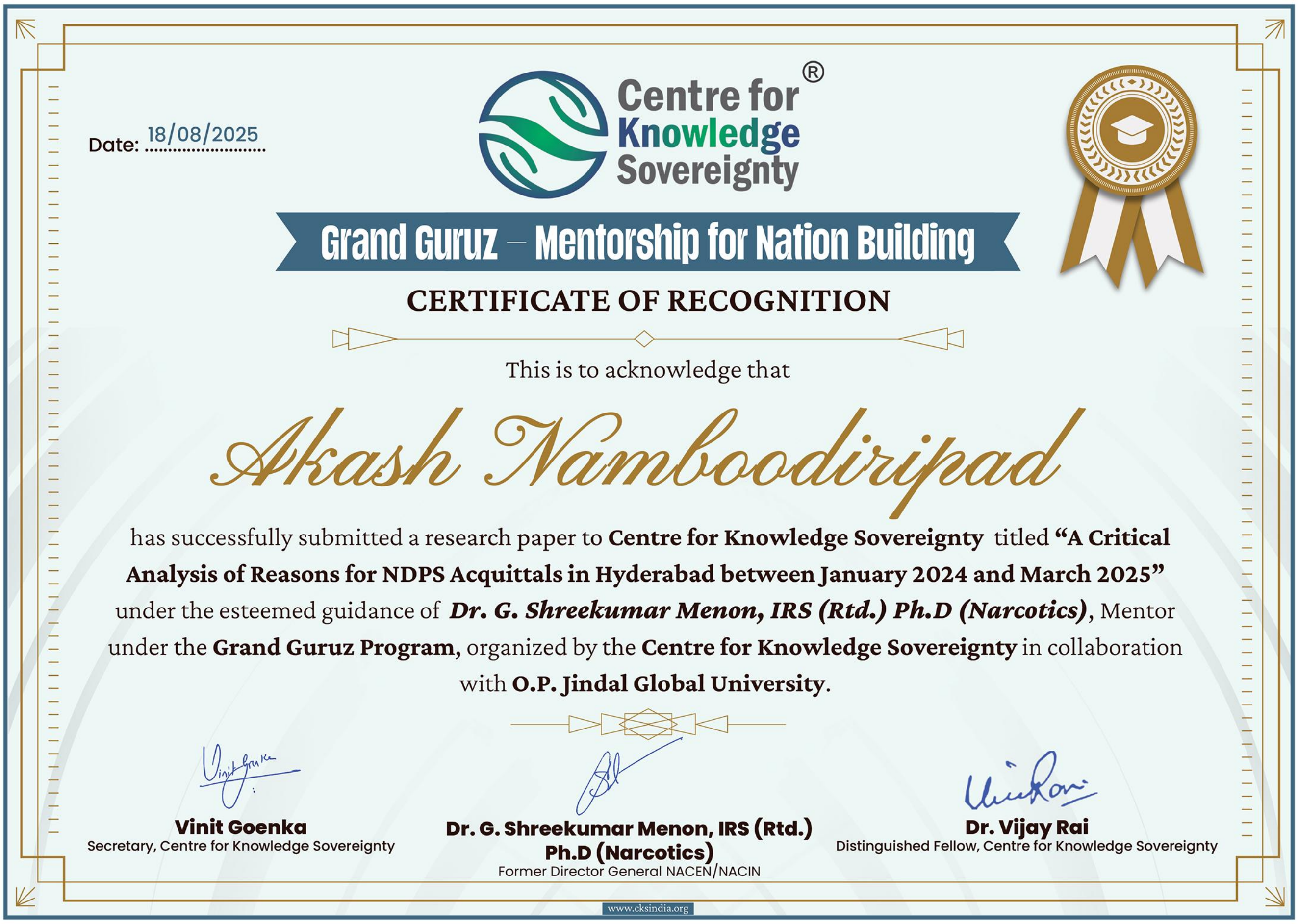
Vinit Goenka
Secretary
Centre for Knowledge Sovereignty

Lt. General Vinod Khandare
PVSM, AVSM, SM (Retd.)
Fmr Principal Advisor, Ministry of Defence, Government of India, Fmr Military Advisor NSCS, Fmr DG Defence Intelligence Agency

Lt. General Sanjay Kulkarni
PVSM, AVSM, SC, SM, VSM (Retd.)
Fmr DG Infantry and Siachen Pioneer

Dr. Vijay Rai
Distinguished Fellow
Centre for Knowledge Sovereignty

www.cksindia.org



Date: 18/08/2025

Centre for Knowledge Sovereignty®

Grand Guruz – Mentorship for Nation Building

CERTIFICATE OF RECOGNITION

This is to acknowledge that

Akash Namboodiripad

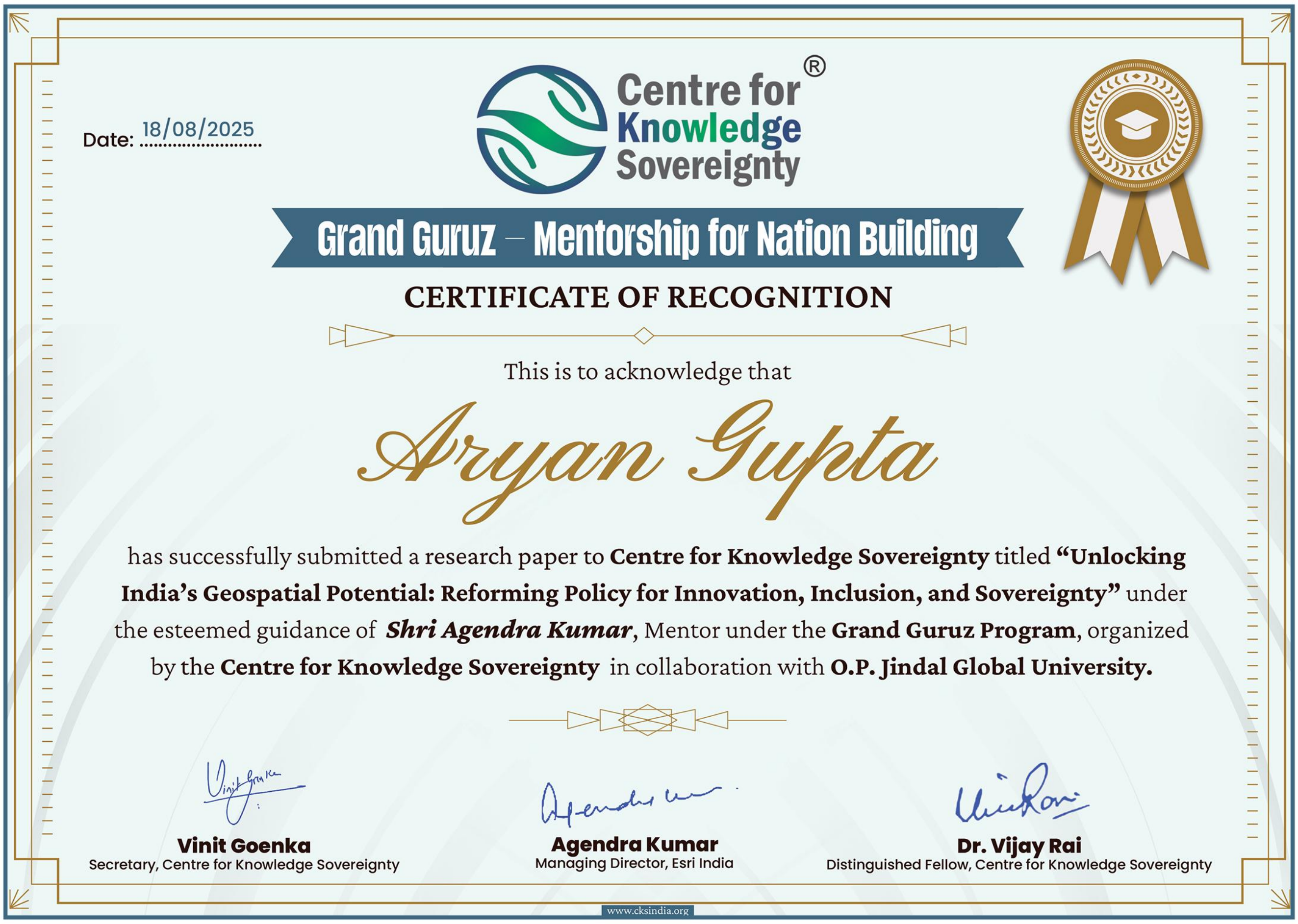
has successfully submitted a research paper to **Centre for Knowledge Sovereignty** titled **"A Critical Analysis of Reasons for NDPS Acquittals in Hyderabad between January 2024 and March 2025"** under the esteemed guidance of ***Dr. G. Shreekumar Menon, IRS (Rtd.) Ph.D (Narcotics)***, Mentor under the **Grand Guruz Program**, organized by the **Centre for Knowledge Sovereignty** in collaboration with **O.P. Jindal Global University**.

Vinit Goenka
Secretary, Centre for Knowledge Sovereignty

Dr. G. Shreekumar Menon, IRS (Rtd.) Ph.D (Narcotics)
Former Director General NACEN/NACIN

Dr. Vijay Rai
Distinguished Fellow, Centre for Knowledge Sovereignty

www.cksindia.org



Date: 18/08/2025

Centre for Knowledge Sovereignty®

Grand Guruz – Mentorship for Nation Building

CERTIFICATE OF RECOGNITION

This is to acknowledge that

Aryan Gupta

has successfully submitted a research paper to **Centre for Knowledge Sovereignty** titled **"Unlocking India's Geospatial Potential: Reforming Policy for Innovation, Inclusion, and Sovereignty"** under the esteemed guidance of ***Shri Agendra Kumar***, Mentor under the **Grand Guruz Program**, organized by the **Centre for Knowledge Sovereignty** in collaboration with **O.P. Jindal Global University.**

Vinit Goenka
Secretary, Centre for Knowledge Sovereignty

Agendra Kumar
Managing Director, Esri India

Dr. Vijay Rai
Distinguished Fellow, Centre for Knowledge Sovereignty

www.cksindia.org

Letters of Recommendation

Next ▶

Centre for®
Knowledge
Sovereignty

Letter of Recommendation

To Whomsoever It May Concern

I am pleased to write this letter of recommendation for **PV Vineet**, a postgraduate student at O.P. Jindal Global University, who has successfully completed a research paper under our **(Lt. General Vinod Khandare PVSM, AVSM, SM (Retd.)** & **Lt. General Sanjay Kulkarni, PVSM, AVSM, SC, SM, VSM (Retd.))** guidance as part of the **Grand Guruz** – Mentorship for Nation Building program, organized by the Centre for Knowledge Sovereignty (CKS) in collaboration with O.P. Jindal Global University.

His research paper, titled **"State Exemptions and Surveillance Overreach: Challenges and Reform Pathways Under India's Digital Personal Data Protection Act"** stands out for its critical engagement with emerging issues in data governance and digital rights. Vineet has demonstrated strong analytical abilities in dissecting the interplay between state power, individual privacy, and national security. His paper offers balanced and forward-thinking recommendations to address institutional overreach while safeguarding democratic values.

With a strong foundation in policy analysis and a deep awareness of constitutional principles, Vineet shows great promise in the fields of digital governance, privacy law, and strategic affairs.

I recommend him with confidence for roles requiring intellectual rigor and ethical policy engagement.

Khandare

Lt. General Vinod Khandare
PVSM, AVSM, SM (Retd.)
Fmr Principal Advisor, Ministry of
Defence, Government
of India, Fmr Military Advisor NSCS, Fmr
DG Defence Intelligence Agency

Kulkarni

Lt. General Sanjay Kulkarni
PVSM, AVSM, SC, SM, VSM (Retd.)
Fmr DG Infantry and Siachen Pioneer

Vinit Goenka

Vinit Goenka
Secretary
Centre for Knowledge Sovereignty

ViRai

Dr. Vijay Rai
Distinguished Fellow
Centre for Knowledge Sovereignty

Centre for Knowledge Sovereignty®

Letter of Recommendation

To Whomsoever It May Concern

I am pleased to write this letter of recommendation for **Akash Namboodiripad**, a postgraduate student at O.P. Jindal Global University, who has successfully completed a research paper under my **(Dr. G. Shreekumar Menon, IRS (Rtd.) Ph.D (Narcotics))** guidance as part of the **Grand Guruz** – Mentorship for Nation Building program, organized by the Centre for Knowledge Sovereignty (CKS) in collaboration with O.P. Jindal Global University.

His research paper, titled **"A Critical Analysis of Reasons for NDPS Acquittals in Hyderabad between January 2024 and March 2025"** reflects a deep commitment to empirical legal research and systemic reform. Akash has meticulously analyzed judicial data to highlight procedural gaps and structural inefficiencies in narcotics law enforcement. His work contributes meaningfully to the intersection of criminal justice, public administration, and legal policy.

Akash brings analytical sharpness, policy sensitivity, and a problem-solving mindset to his work, qualities essential for roles in legal reform, governance, or academia.

I recommend him strongly for any opportunity that requires critical inquiry and a grounded understanding of institutional policy.

Dr. G. Shreekumar Menon, IRS
(Rtd.) Ph.D (Narcotics)
Former Director General NACEN/NACIN

Dr. Vijay Rai
Distinguished Fellow
Centre for Knowledge Sovereignty

Vinit Goenka
Secretary
Centre for Knowledge Sovereignty

Centre for Knowledge Sovereignty®

Letter of Recommendation

To Whomsoever It May Concern

I am pleased to write this letter of recommendation for **Aryan Gupta**, a postgraduate student at O.P. Jindal Global University, who has successfully completed a research paper under my **(Shri Agendra Kumar)** guidance as part of the **Grand Guruz** – Mentorship for Nation Building program, organized by the Centre for Knowledge Sovereignty (CKS) in collaboration with O.P. Jindal Global University.

His research paper, titled **"Unlocking India's Geospatial Potential: Reforming Policy for Innovation, Inclusion, and Sovereignty**," is a testament to his academic rigor, originality, and clarity of thought. The paper provides timely and actionable insights into India's geospatial policy landscape and offers a forward-looking framework for balancing innovation with strategic interests. Aryan has demonstrated a nuanced understanding of complex policy environments and the implications of spatial data governance for national development.

His commitment to detail and his ability to synthesize technical and policy perspectives make him a valuable contributor to the evolving discourse on geospatial intelligence and strategic planning.

I recommend him wholeheartedly for further research opportunities or roles in public policy and technology governance.

Agendra Kumar
Managing Director
ESRI India

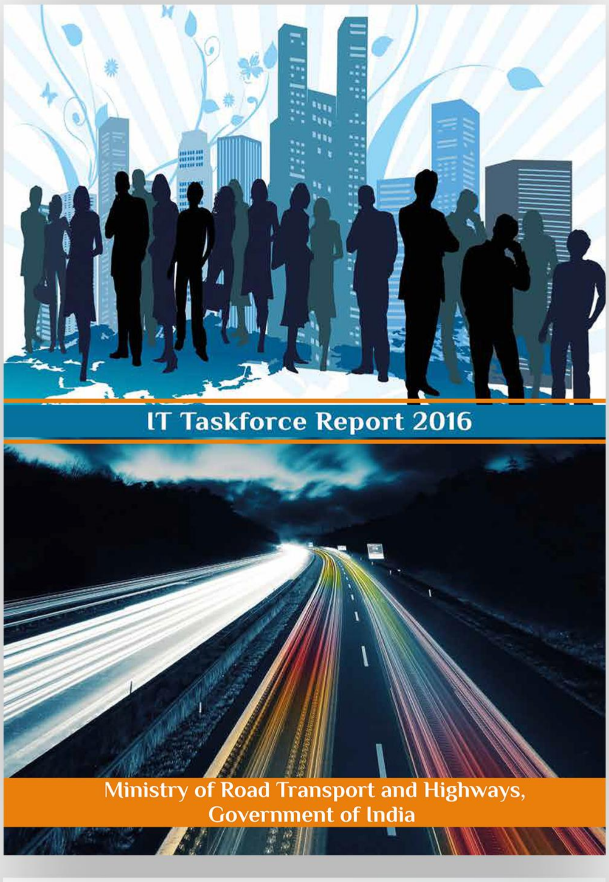
Dr. Vijay Rai
Distinguished Fellow
Centre for Knowledge Sovereignty

Vinit Goenka
Secretary
Centre for Knowledge Sovereignty

Publications Reports & Books

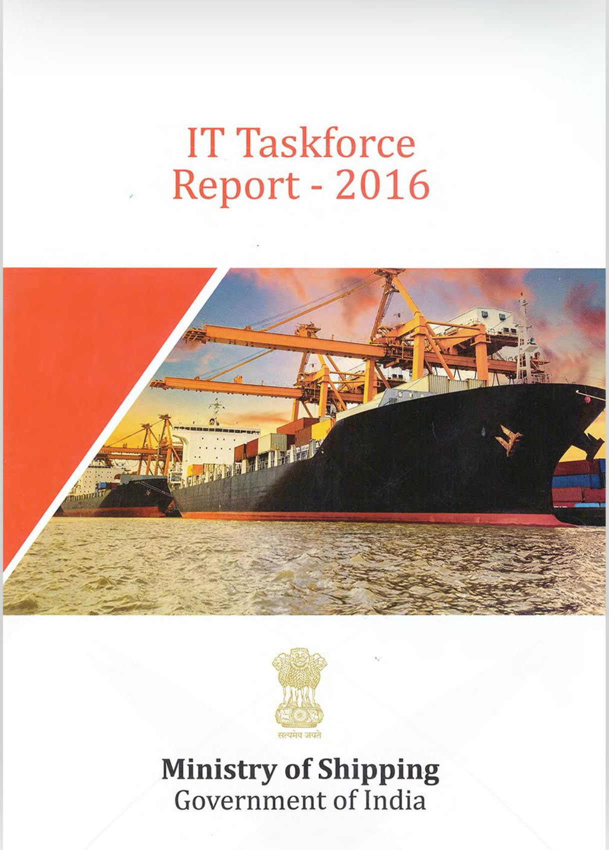
Next ▶

Taskforce Reports



IT Taskforce Report 2016

Ministry of Road Transport and Highways,
Government of India



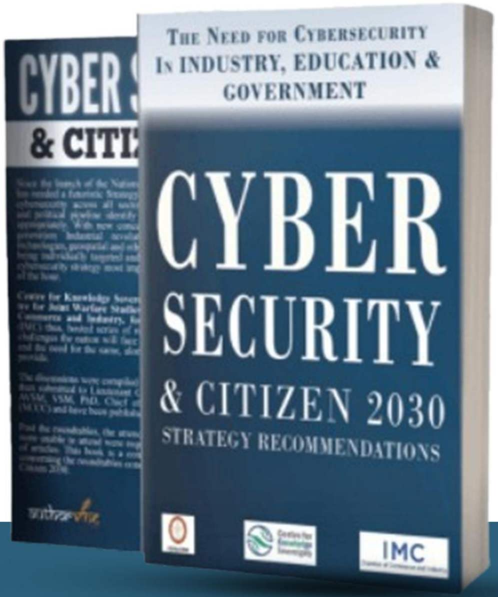
IT Taskforce
Report - 2016

सत्यमेव जयते

Ministry of Shipping
Government of India

Publications

Data Sovereignty: The Pursuit of Supremacy


THE NEED FOR CYBERSECURITY IN INDUSTRY, EDUCATION & GOVERNMENT
CYBER SECURITY
& CITIZEN 2030
STRATEGY RECOMMENDATIONS
Centre for Knowledge Sovereignty
IMC

Cyber Security & Citizen 2030 : Strategy Recommendations

Recommendations

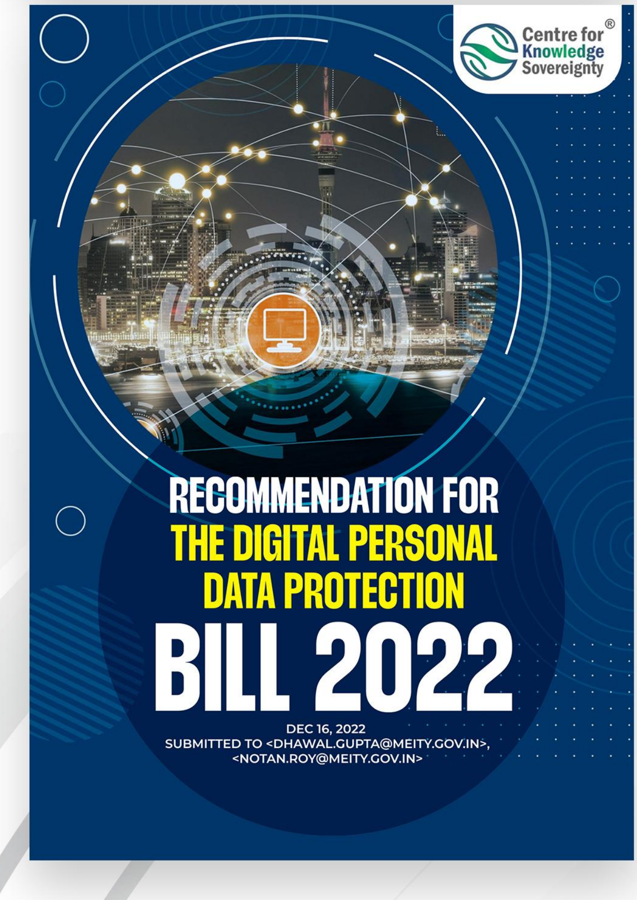
RECOMMENDATIONS FOR NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020)

Hosted By:

Centre for Knowledge Sovereignty®

CENJOWS

IMC Chamber of Commerce and Industry



Centre for Knowledge Sovereignty®

RECOMMENDATION FOR THE DIGITAL PERSONAL DATA PROTECTION BILL 2022

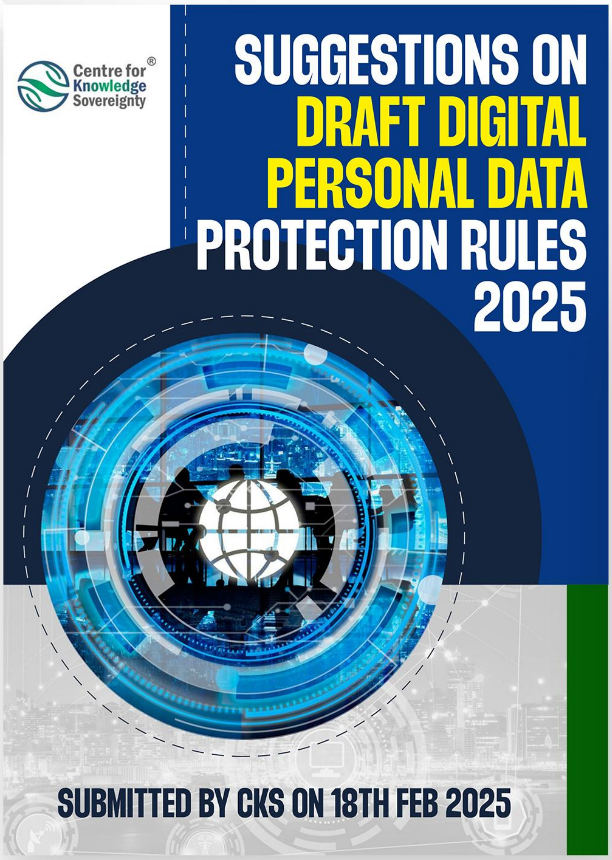
DEC 16, 2022
SUBMITTED TO <DHAWAL.GUPTA@MEITY.GOV.IN>,
<NOTAN.ROY@MEITY.GOV.IN>

Centre for Knowledge Sovereignty®

STRATEGY to DEAL WITH NATIONAL SECURITY THREAT EMANATING FROM SOCIAL MEDIA

www.cksindia.in

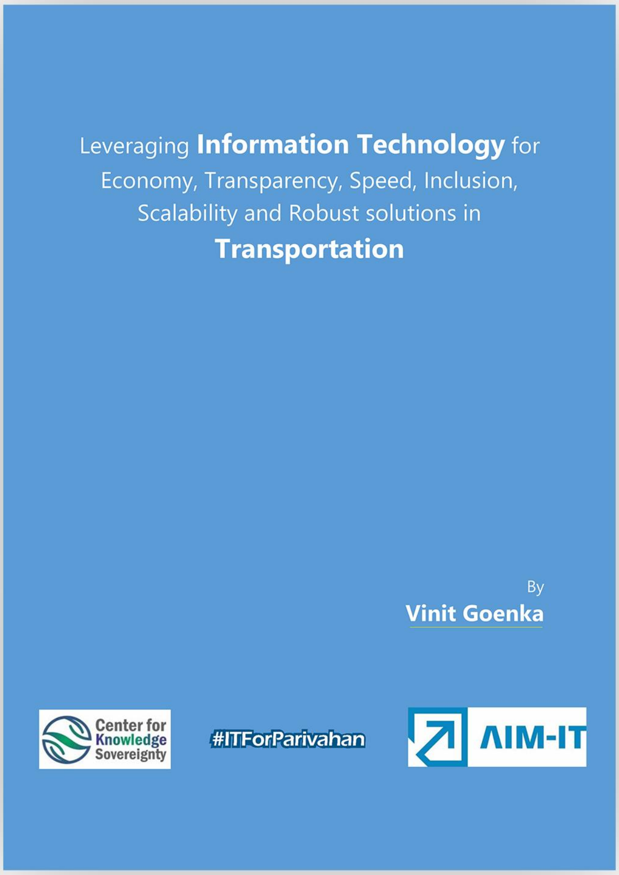
Reports



Centre for Knowledge Sovereignty®

SUGGESTIONS ON DRAFT DIGITAL PERSONAL DATA PROTECTION RULES 2025

SUBMITTED BY CKS ON 18TH FEB 2025



Leveraging **Information Technology** for Economy, Transparency, Speed, Inclusion, Scalability and Robust solutions in **Transportation**

By **Vinit Goenka**

Center for Knowledge Sovereignty #ITForParivahan AIM-IT

Centre for Knowledge Sovereignty®

MoM of CKS Internal Discussion on Draft DPDP Rules 2025

~Chatam House

Reports

Centre for Knowledge Sovereignty®

GAMBLING AWAY INDIA'S SOVEREIGNTY

WHITEPAPER ON

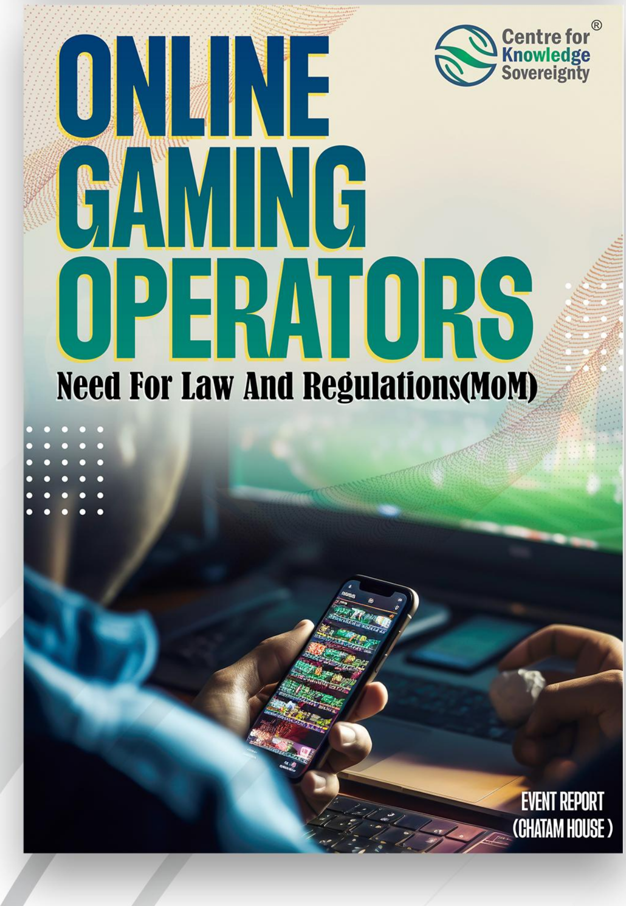
ILLEGAL GAMBLING AND BETTING IN INDIA

RISKS, CHALLENGES, AND RESPONSES

BY

LT. GEN VINOD G. KHANDARE, PVSM, AVSM, SM (Retd.)
Principal, Adviser, Minister of Defence Gov. of India

VINIT GOENKA
Secretary, Centre for knowledge sovereignty



Centre for Knowledge Sovereignty®

ONLINE GAMING OPERATORS

Need For Law And Regulations(MoM)

EVENT REPORT
(CHATAM HOUSE)

CYBERSECURITY CITIZENS OF 2030

Click Safe. Stay Safe.

Cybersecurity Citizens of 2030

Flagship Initiatives

Next ▶

By
Guest of Honour
Padma Shri A S Kiran Kumar
Former Chairman ISRO, Vikram Sarabhai Professor
on
Tuesday 21st May 2019, 05:00 pm to 07:00 pm
At
International Convention Hall, Bombay Stock Exchange, Mumbai 400001
Foreword by A. S. KIRAN KUMAR, Former Chairman, ISRO

Inauguration at Bombay Stock Exchange, Mumbai by Former Chairman of ISRO and Vikram Sarabhai Professor Shri A S Kiran Kumar and other dignitaries.

Book Release ceremony
Data Sovereignty: The Pursuit of Supremacy

Inauguration at Constitution Club of India, New Delhi by then Organising Secretary of ABVP and current Akhil Bharatiya Prachar Pramukh, RSS Shri Sunil Ambekar ji and other dignitaries.

Flagship Initiative

THUS SPAKE GENERALS

THUS SPAKE GENERALS means "Experts Speak", is a platform for high-level discussions and presentations by experts, leaders, and scholars on military, geopolitical, strategic, and knowledge-related topics.

Over the past few years, CKS is privileged to host on its platform, several discussions, round tables in person and since Covid19, CKS has initiated Virtual discussions as well. **#THUSSPAKEGENERALS** is among the flagship programs which has completed **Thirty** Talks.

We had the privilege of hosting strategists and thought leaders on our platform such as Lt Gen Dr D B Shekatkar, Lt Gen P R Shankar, Lt Gen S Kulkarni, Lt Gen Ata Hasnain, Vice Admiral Sekhar Sinha, Air Marshal SS Soman. AVM Arjun Subramaniam, Air Marshal Anil Khosla, Lt Gen D S Hooda, Lt Gen Z U Shah, Vice Admiral Anil Chopra, Lt Gen Rakesh Sharma, Rear Admiral Sudarshan Shrikhande, Air Marshal D Choudhary, Ambassador Ashok Sajjanhar, Lt Gen Shokin, Lt Gen Vinod Bhatia, Lt Gen Vinod Khandare, Lt Gen Satish Dua and many more.

PROGRAM MODERATORS

1. AVM PRANAY SINHA
2. UMA SUDHINDRA
3. DR. DEEPA PRAKASH
4. SUMITRA V GOENKA
5. DR. NAGARATHNA A.
6. BIPINDRA NC

WATCH MORE DETAILS ON YOUTUBE CHANNEL

CKSINDIA

Centre for Knowledge Sovereignty®

Flagship Initiative

MASTER MENTORS GEO-ENABLING INDIAN SCHOLARS - (MMGEIS)

Master Mentors Geo-enabling Indian Scholars (MMGEIS), an online program aims to inculcate geospatial thinking and develop a research-oriented mindset amongst students who will form the future workforce of the country. The program will be open to students from 6th grade to undergraduate and will be delivered in a completely virtual mode over 5 months to provide them with much-needed exposure about what goes behind the common apps that we use to navigate our way to someplace or hail a cab or order food or other stuff from our mobile devices, or how GIS and remote sensing is playing a role in smart cities, utilities, transportation, disaster management, sustainable development etc. It is about kindling geospatial thinking which will become foundation for them to use the geospatial approach in which ever career they adopt.

ABOUT THE PROGRAM

Isaac Newton's famous words, "If i have seen further, it is by standing on the shoulders of giants," underscore the profound impact of mentors. The significance of finding excellent mentors cannot be overstated, especially for students on the cusp of pivotal life decisions. Proper guidance becomes instrumental in shaping their paths and propelling them to greater heights. The Master Mentor's Geo-enabling Indian Scholars (MMGEIS) program presents a unique opportunity for students to delve into geospatial technology and be mentored by experts in the field A joint initiative of the Centre for knowledge Sovereignty and Esri India, MMGEIS is a "not-for-profit" endeavour designed to inculcate thinking of Geospatial-innovation amongst indian scholars who will form the future workforce of India. This program is aimed at students from 6th grade to undergraduate levels and provides them a foundation on which they can develop ideas to discover new technologies ami methods in geospatial arena. The program will tap pan-India talent through a competitive process. It will bridge the gap between academia and industry access and collaborate to create a best-in-class ecosystem for geospatial innovation and Intellectual property development which will contribute towards our goal of becoming a developed nation by the year 2047

OBJECTIVE

Create awareness on the importance of "geospatial thinking" and "geospatial skills" at college/school level.
Encourage educational institutions to incorporate "geospatial thinking" and strengthen "geospatial skills" in their pedagogy and curriculum. Highlight the strategic value of geospatial in economic, social, and environmental spheres.
Strengthen geospatial learning, research, and knowledge towards creating intellectual property.

ELIGIBILITY

- High School Students
- Senior School Students
- Undergraduate Students

No prior experience required-just a curiosity to explore, learn and problem-solving attitude !

WHY ATTEND THE PROGRAM?

- Vision Talks and Interaction with Master Mentors
- One-on-One Mentoring by Experts
- Engaging Lessons
- Interactive Activities
- Spatial Thinking in Action
- Knowledge Towards Creating Intellectual Property

PRIZES & REWARDS

- Certificate of Achievement
- Letter of Recommendation (LoR)
- ArcGIS Online Software (21 days)

MASTER MENTORS & BOARD MEMBERS

A.S. Kiran Kumar

Member, Space Commission &
Fmr. Chairman, ISRO

Dr. K. J. Ramesh

Advisor Regional Integrated Multi-Hazard
Early Warning System (RIMES) &
Fmr. Director General, India
Meteorological Department (IMD)

Lt. Gen. Girish Kumar, VSM (Retd.)

Advisor, Government of
Haryana and Fmr. Surveyor General of
India

BOARD MEMBERS

Vinit Goenka

Secretary
Centre for Knowledge Sovereignty

Agendra kumar

Managing Director
Esri India

ADVISORY BOARD MEMBERS

Lt. Gen. Vinod G. Khandare, PVSM, AVSM, SM (Retd.)
Fmr. Principal Advisor, Ministry of Defence, GOI
Fmr. Military Advisor NSCS, Fmr. DG Defence
Intelligence Agency.

Dr. Mrutyunjay Mohapatra
Director General
India Meteorological Department

Dr. Prakash Chauhan
Director, National Remote Sensing Centre (NRSC)

Dr. Arun Kumar Sarma
Director General, Northeast Centre for Technology
Application and Reach (NECTAR)

Dr. Raj Kumar Khatri, IAS
Co-ordinator for World Bank Project on
Land Policies (Karnataka State)

Rajesh Chandra Mathur
Senior Director - Strategy, Esri India

Lt. Gen. PJS Pannu PVSM AVSM, VSM(Retd.)
Fmr. Deputy Chief, Indian Integrated Defence Staff
(Operations)

Dr. Sultan Singh
Head GIS Division, GDMA

Dr. D. Vasudevan
Senior Consultant (Information Systems),
NAFED New Delhi

V Uday Kumar
DDG, National Informatics Centre

Dr. Sameer Saran
DGM RC North - RRSC, ISRO

Vishnu Chandra
Advisor, Ministry of Panchayati Raj

Ravindra Kumar
Chief Scientist & Head ILT. CRRI

Dr. Shikha Dixit
Deputy Director (Enviromental Health & Geospatial
Science), INCLEN Trust, New Delhi

Pawan K Jushi PhD
Professor School of Environmental Sciences
(SES), JNU

Prof. Dheeraj Kumar
Dy. Director & Project Director (Mining Technology
Innovation Hub(TEXMiN)), IIT (ISM)

About CKS

Formed in the Year 2011, The Centre for Knowledge Sovereignty **(CKS)** is a is a leading autonomous, non-partisan public policy think-tank focusing on technology's impact on **data, security, and policymaking.** CKS is dedicated to **promoting and protecting** the rights of Indian citizens over their 'Knowledge' and 'Data'. Its core mission is to ensure that indigenous and local knowledge systems are preserved, respected and enhanced that data sovereignty— the right of communities to control their own 'Knowledge' and 'Data' is upheld.

At CKS, we have a firm belief in forming a sovereign future for India, we visualize India as a forerunner in creating impact through policymaking and heralding as a prominent voice for the discourse pertaining to disruptive technologies, and technological integration. We achieve this by conducting in-depth research and providing policy solutions across inter-sectoral fields, while pioneering technology and its extensive connotations.

We are empowering India's future through research and policy intervention to edifice a sovereign and sustainable digital age.

Our Value Lies in: **Shaping the Knowledge Landscape: For a Sovereign Future.**

14+

Years of Existence

40,000+

Copies of Book
"Data Sovereignty Pursuit of
Supremacy" in circulation

1M+

Students Reached through Programs like MMGEIS, CS 2030, Grand Guru etc.

500+

Roundtable Discusions, Conferences, Policy Consultations, Academic Forums Events etc.

Vision

Centre for Knowledge Sovereignty strives to be the region's intellectual hub and thought leader for research, analysis and advocacy on impacting policies, disruptive technologies and bring new perspectives to the policy makers.

Mission

Centre for Knowledge Sovereignty will promote sustainable and pragmatic policy initiatives collaboratively to influence the stakeholders, drive change and provide better understanding of global trend and their consequences for society, economy and national security.

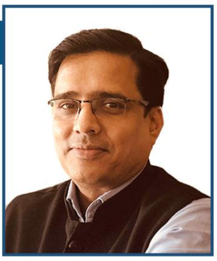
Centre for Knowledge Sovereignty®

Team CKS

Chairman

Lt. Gen. Dr. D. B. Shekatkar PVSM, AVSM, VSM (Retd.)

Chancellor , Sikkim Central University
Chairman of the Committee of Experts (CoE) constituted by the Ministry of Defence (Shekatkar Committee)
Co-Author Data Sovereignty The Pursuit of Supremacy



Secretary

Vinit Goenka

Governing Council Member - Centre for Railway Information System (CRIS), Ministry of Railways, GoI. (2016 to 2024)
Member IT Task Force, Ministry of Road Transport Highways and Shipping, GoI. (2015 to 2016)
Co-Author- Data Sovereignty The Pursuit of Supremacy

Joint Secretary

Uma Sudhindra

Board of Governors, IIM Visakhapatnam
Strategy Consultant, Managing Partner at Go Magic Trails

Dr. K. J. Ramesh

Former Director General, Indian Meteorological Department

Dr. G. Shreekumar Menon, IRS (Retd.)

Fmr. Director General, NA of Customs Indirect Taxes & Narcotics

Air Vice Marshal Pranay Kumar Hridayash Sinha, VSM (Retd.)

Presently Strategic Advisor of IIT Mandi
Ex-AOC of E W System, BRD,
Ex- Commandant, Software Dev Inst. B'lore,
Ex- Advisor, BEL

Sumitra Goenka

Entrepreneur & Board Member
Independent Director at listed Company

Bhola Nath Sharma

Former Inspector General Border Security Force

Mark Barnes

Chairman, Nirman Foundation
Director at embee & Co

Col. VD Singh (Retd.)

Fmr. Joint Director IT with DG Info System at Army HQ,
Visiting Faculty at Institutes

Thirunarayanan Varadadesigan

Senior Technologist & Principal Technical Program Manager

Centre for Knowledge Sovereignty ®

secretariat@cksindia.in

www.cksindia.org CKSINDIA CKSINDIA