

Daily Editorial Analysis 30 June 2025

June 30, 2025 • vajiramandravi.com

Revisit Digital Search Powers Under the I-T Bill 2025

Context

- The Finance Minister's proposal under the Income-Tax Bill, 2025, allows tax authorities to **access an individual's "virtual digital space"** during search and seizure operations.
- While justified as necessary due to increasing online financial activity, the move raises serious concerns about privacy, government overreach, and expanded surveillance powers.

Existing Legal Framework

- India's current tax law, under Section 132 of the Income-Tax Act, 1961, allows for search and seizure in physical spaces like homes, offices, and lockers.
- These powers are justified by a direct link between the location and the suspected undisclosed income or assets.

Expansion to Digital Space

- The new Income-Tax Bill, 2025, proposes to expand search powers to include an individual's "virtual digital space"—such as emails, cloud drives, social media accounts, and digital platforms.
- The inclusion of "any other space of similar nature" makes this scope open-ended and undefined.
- **Concerns Over Privacy and Overreach**
 - Digital spaces often hold far more information than required for a tax investigation, including data involving friends, family, and colleagues.
 - This significantly increases the risk of disproportionate intrusion and the violation of privacy.
- **Implications for Confidential Professions**
 - The move is particularly worrying for professionals like journalists, whose devices may hold confidential sources and unpublished materials.
 - Seizures based on vague suspicion could impair press freedom and violate protected communication.
- **Operational Challenges**
 - The Bill also allows tax authorities to override access codes to digital devices.
 - However, it remains unclear how this will work in practice—especially for encrypted apps like WhatsApp, which were specifically mentioned by the Finance Minister.
- **Judicial Safeguards and Supreme Court Intervention**

- India's judiciary has consistently upheld that search and seizure powers are to be exercised with restraint, requiring solid evidence beyond suspicion.
- In 2023, the Supreme Court issued **interim guidelines on digital device seizures** and called on the government to draft appropriate protocols.

Criticism of this Move

- **Lack of Transparency and Oversight**

- The proposed provision lacks essential safeguards such as judicial oversight, accountability, and clarity, violating core democratic principles.
- It does not require authorities to disclose the "reason to believe," undermining transparency.

- **Ignoring the Nature of Digital Data**

- The law fails to appreciate the complexity and sensitivity of digital information.
- Electronic devices often hold vast, layered personal and professional data that require higher standards of protection.

- **Absence of Legal Guardrails**

- There are no clear checks and balances in the proposed provision.
- Without specific procedural safeguards, it opens the door to potential misuse and abuse of power by tax authorities.

Global Best Practices Emphasize Safeguards

- Canada's Section 8 of the Charter of Rights and Freedoms protects against unreasonable searches, requiring:
 - Prior authorisation
 - Approval by a neutral authority
 - Reasonable and probable cause
- In the United States, the Taxpayer Bill of Rights guarantees due process and limits intrusive action.
 - The Supreme Court ruling in *Riley vs California* requires warrants to access digital devices, acknowledging the highly personal nature of such data.

Violation of the Proportionality Principle

- The proposed provision grants sweeping access to personal digital data without requiring warrants, relevance checks, or distinctions between financial and non-financial data.
- This violates the proportionality test laid down in the **Justice K.S. Puttaswamy vs Union of India judgment**.
- **Supreme Court's Four-Fold Test**
 - The Supreme Court mandates that **restrictions on privacy** must:
 - Serve a legitimate aim
 - Be necessary
 - Use the least intrusive means
 - Be proportionate
 - The proposed provision **fails to meet these criteria**, particularly on necessity and intrusiveness.

Way Forward

- **Digital Enforcement Must Respect Rights**

- The solution isn't to discard digital enforcement, but to align it with principles of legality, proportionality, and transparency.
- Enforcement must protect, not erode, constitutional rights.

- **Unchecked Surveillance Is Overreach**

- Allowing unfettered access under the guise of regulation amounts to surveillance, not governance. It undermines public trust and violates the right to privacy.

- **Hope for Reform Through Legislative Scrutiny**

- There is still scope for correction. The Select Committee reviewing the Bill should:
 - Narrow the definition of "virtual digital space"
 - Mandate prior judicial warrants
 - Require disclosure of reasons
 - Establish grievance redress mechanisms

Conclusion

- The path forward must **balance enforcement with constitutional protections**. Without adequate checks, the proposed law risks becoming a tool of intrusion rather than accountability.
-

A Year Later — Colonial-Era Laws to New Criminal Codes

Context

- **In 2023, the Government of India undertook a sweeping reform of its colonial-era criminal laws** by introducing three new criminal laws.
- One year into their implementation, **the early outcomes of these legislative changes are beginning to take shape**, particularly in the realm of policing and investigation.
- After a year, **now it becomes imperative to critically examine the new criminal laws' implementation, highlight technological innovations**, evaluate progress, and underscore continuing challenges.

Key Features of New Criminal Codes

- **Legislative Overhaul and Structural Transition**

- The central government's legislative reforms **marked a significant departure from colonial jurisprudence**, attempting to modernize the administration of criminal justice.
- As part of this process, **the transition to the new codes has largely been smooth**, thanks in part to digital platforms like the **Crime and Criminal Tracking Network and Systems (CCTNS)**, a backbone of the **Inter-operable Criminal Justice System (ICJS)**.

- The CCTNS has enabled jurisdictional routing of zero FIRs and streamlined police operations across states.
- The **Ministry of Home Affairs (MHA)** deserves credit for overseeing this crucial phase of systemic transformation at the ground level.

- **Technological Integration through ‘e-Sakshya’**

- The hallmark of this reform has been the **e-Sakshya mobile application**, developed by the **National Informatics Centre (NIC)** in collaboration with the MHA.
- This app allows **real-time recording and preservation of evidence**, such as photographs and videos, embedded with **geo-coordinates and time stamps**.
- It complies with several mandatory provisions under the BNSS, including Sections 105, 173, 176, 180, 185, and 497, all of which emphasize the digital documentation of searches, seizures, statements, and property disposal.
- Feedback from **Investigating Officers (IOs)** has been encouraging.
- The app has introduced **greater accountability**, prevented delegation of investigation tasks to unauthorised personnel, and increased the **credibility of the evidence** by visibly involving witnesses at crime scenes.
- **Mandatory selfies and digital footprints** left by IOs help ensure responsibility and eliminate ambiguities.

- **Strengthening Forensic Practices**

- Another critical reform is the **mandatory visit of a Forensic Science Laboratory (FSL) expert** to crime scenes, as per Section 176 of the BNSS.
- Despite limited growth in forensic infrastructure, **this mandate ensures scientific rigor in crime scene analysis**.
- The government has responded with plans for institutions like the **National Forensic Science University (NFSU)** and a **Central Forensic Science Laboratory (CFSL)** in Raipur, which could address current deficiencies.

An Overview of Operational Challenges and Gaps

- **Implementation of E-Sakshya**

- Courts have not yet integrated with the ICJS to directly access evidence from the **National Government Cloud (NGC)**. As a result, IOs must still resort to submitting pen drives manually, adding to costs and redundancy.
- The dependence on personal mobile phones for official tasks has been problematic.
- The app requires **Android 10+ devices with at least 1 GB storage**, compelling IOs to upgrade at their own expense.
- **Limited tablets provided to police stations are insufficient** to meet operational demand.
- There are also **software limitations. In non-linked FIR scenarios, only five Sakshya IDs can be generated offline**, and image or video errors cannot be rectified in linked cases.
- These **constraints may undermine the app’s utility** in critical situations.

- **Reluctance from accused persons to be digitally recorded while revealing crime details** has emerged as another barrier, although such documentation could significantly boost conviction rates.
- **Legal Ambiguities and Incomplete Digitization**
 - **Section 303 of the BNS** does not clearly define when thefts under ₹5000 are to be treated as cognizable offences, while **Section 112** on organised petty offences remains overly broad.
 - Furthermore, provisions such as **video-conferencing for witness examination** under **Section 530 of the BNSS are underutilised**, despite being legally permissible.
 - Although the seven-day limit for forwarding **medical examination reports of rape survivors** has been successfully implemented, **post-mortem reports** continue to be delayed.
 - The **MedLEaPR system, still under testing in Chhattisgarh**, promises to streamline this process by digitally linking hospitals with police systems.

The Way Forward: Feedback and Resource Allocation

- For the reforms to succeed fully, **feedback loops** from IOs, courts, and state governments must be institutionalised.
- An **ongoing review mechanism** should be established to revise ambiguous provisions, address legal loopholes, and simplify procedural bottlenecks.
- Moreover, the **allocation of additional resources** to forensic units, IT infrastructure, and training programs is urgently required.
- **Ensuring that every police station is equipped with sufficient tablets and that officers no longer rely on personal devices** is not just practical, it is essential for professionalism and data security.

Conclusion

- One year after their implementation, the new criminal laws, the BNS, BNSS, and, BSA represent a **paradigm shift in India's criminal justice system**.
- The **integration of technology**, particularly through tools like **e-Sakshya**, has brought a tangible difference to policing and investigations.
- Yet, operational challenges, infrastructural limitations, and legal ambiguities persist, calling for **adaptive policymaking, robust training, and resource augmentation**.

A Year Later — Colonial-Era Laws to New Criminal Codes FAQs

Q1. What replaced the Indian Penal Code in 2023?

Ans. The Indian Penal Code was replaced by the Bharatiya Nyaya Sanhita (BNS) in 2023.

Q2. What is the purpose of the e-Sakshya app?

Ans. The purpose of the e-Sakshya app is to help police officers record and preserve digital evidence such as photos and videos in real time with location and time data.

Q3. Which system connects police, courts, and forensic labs?

Ans. The Inter-operable Criminal Justice System (ICJS) is the system that connects the police, courts, forensic

laboratories, prosecution, and prisons.

Q4. What is a major challenge with the e-Sakshya app?

Ans. A major challenge with the e-Sakshya app is that many investigating officers are forced to use their personal mobile phones due to a shortage of official devices.

Q5. What reform helps ensure FSL experts visit crime scenes?

Ans. Section 176 of the Bharatiya Nagarik Suraksha Sanhita (BNSS) mandates the visit of Forensic Science Laboratory (FSL) experts to the crime scene.

Source: **The Hindu**

Source: <https://vajiramandravi.com/current-affairs/daily-editorial-analysis-30-june-2025/>

© Vajiram & Ravi. For personal use only.