Criminal Justice – The ‘e-Evidence’ Standard

Context: The Supreme Court’s guidelines on *"Seizure of Digital Devices"* (January 2026) and the operational challenges of the **Bharatiya Nagarik Suraksha Sanhita (BNSS)**. **Key Theme:** *From 'Paper-Based' to 'Pixel-Based' Justice.* **Keywords:** *Section 105 BNSS, Section 61 BSA, Hash Value, Chain of Custody, e-Malkhana.*

1. The Context: The "End of Seizure Raj"?

For decades, the seizure of phones and laptops was a legal grey area. Police often seized devices without sealing them properly, leading to allegations of **"Data Planting"** (as seen in the Bhima Koregaon case).

In **January 2026**, the Supreme Court operationalized strict guidelines aligning with **Section 105 of the BNSS**. The Court ruled that *“Digital Evidence is fragile. Without a verifiable Chain of Custody, it is just digital noise, not legal proof.”*

2. The Legal Shift: Mandatory Videography (Section 105)

The BNSS has fundamentally changed the "Search and Seizure" protocol.

- **The Mandate:** Under Section 105, the *entire process* of search and seizure (from entering the house to sealing the device) **must be videographed**, preferably on a mobile phone.
- **Governance Impact:** This is a check on **Police Discretion**. If the videography is missing or has "unexplained cuts," the seizure can be declared void. It aims to end the era of police claiming *"We found this laptop under his bed"* without proof of recovery.

3. The 'Hash Value' Shield (Integrity)

The most technical but critical governance reform in January 2026 is the enforcement of the **"Hash Value"** rule.

- **The Concept:** A "Hash Value" is a unique digital fingerprint of a file/device. Even if one comma is changed in a document, the hash value changes completely.
- **The New Protocol:** The Supreme Court has mandated that the **Hash Value** of a seized device must be generated **at the scene of the crime** and recorded in the *Seizure Memo* before the device is taken to the police station.
- **Why it matters:** This ensures that the police cannot tamper with the device (e.g., adding a folder named 'Bomb Plans') *after* bringing it to the station. If the Hash Value in court doesn't match the Hash Value in the memo, the evidence is thrown out.

4. Admissibility: The BSA Section 61 Shift

The **Bharatiya Sakshya Adhiniyam (BSA)** has replaced the old Section 65B of the Evidence Act.

- **Old Law:** Electronic records were "Secondary Evidence" and needed a certificate that was often hard to get.
- **New Law (Section 61):** Electronic records are now treated as **"Documents"** (Primary Evidence) if they meet security standards. This simplifies the trial process but raises the bar for *storage security*.

5. The Infrastructure Crisis: 'e-Malkhanas'

While the law is ready, the infrastructure is struggling.

- **The Challenge:** Police stations traditionally have "Malkhanas" (store rooms) for guns and swords. They lack **"e-Malkhanas"** (Servers/Cloud Storage) to store Petabytes of HD video footage from body cams and seizures.
- **The Risk:** In January, several states reported **"Data Rot"**—video evidence corrupted due to improper storage on cheap pen drives. Without a standardized **National Cloud for Justice**, the reforms risk collapsing under their own data weight.

6. Mains Analysis: Privacy vs. Procedure

- **The "Right to Silence" (Article 20):** Can the police force an accused to give their **Password/Biometric** to unlock a seized phone? The BNSS implies they can, but the Supreme Court (in the January guidelines) held that *"Forcing a password is akin to self-incrimination,"* leaving a legal conflict that a Constitution Bench must resolve.
- **Conclusion:** The 'e-Evidence' standard is a double-edged sword. It protects the accused from *planting* (via Hash Value) but exposes them to *state surveillance* (via unbridled device access). The Governance challenge is to build the **Cyber-Forensic Capacity** to handle this shift.