

Digital Trails and Policing in India: How Data Is Reshaping Crime Detection

December 24, 2025 • vajiramandravi.com



Digital Trails in Policing Latest News

- The arrest of Ravindra Soni, alleged mastermind of the ₹1,000-crore **BlueChip Group scam**, highlights how **digital footprints are transforming policing in India**.
- Tracked down in Dehradun after a year on the run, Soni was caught not through traditional surveillance but via a food delivery order.
- The case underscores law enforcement's growing use of everyday digital data—OTPs, delivery logs, and e-commerce histories—to trace suspects, showing how routine online activity now leaves an electronic trail that can unravel even sophisticated criminal networks.

The BlueChip Scam: How a Global Investment Fraud Unfolded

- Ravindra Soni, in 2021, founded the BlueChip Group, claiming to trade in forex and commodities like gold, oil, and metals. The firm drew investors from India, the UAE, Malaysia, Canada, and Japan.

- By 2024, investigators found the operation to be an elaborate fraud, with the company disappearing along with investors' money.
- After nearly a year on the run, Soni was traced back to India and arrested in Dehradun on November 30, when police tracked him via a food delivery.
- Authorities allege he ran multiple investment fronts, with the scam's scale estimated at up to ₹1,000 crore.

Digital Residue as Evidence: A New Tool for Law Enforcement

- Investigators are increasingly using digital residue—data from everyday apps and services—as key evidence.
- In a ₹5,300-crore GST fraud, uncovered in May 2024, seemingly minor data points such as OTPs from food-delivery apps and FASTag alerts helped map suspect movements and expose networks of fake firms and forged tax credits.

Tracking Evasion Tactics

- Suspects tried to evade detection by frequently changing phones, SIM cards, and hotel identities, keeping devices switched off except to receive OTPs. This pattern itself became a tell.
- FASTag toll data was used to trace luxury vehicles along the Delhi-Noida-Lucknow corridor, narrowing locations despite constant digital churn.

Multi-App Linkages Crack Cyber Rings

- In October, Delhi Police dismantled a ₹22 lakh cyber-fraud network after a nine-day, 1,800-km operation across four states.
- WhatsApp data indicated overseas operations from Malaysia, while footprints from Flipkart, Swiggy, and Zomato helped identify suspects despite frequent location changes.

Legal Pathways for Data Sharing

- Most apps' **privacy policies** permit data sharing with law enforcement when required to investigate or prevent illegal activity or to comply with legal processes—making such digital traces admissible and actionable.

Beyond Financial Crime: Global Parallels

- The evidentiary shift isn't limited to financial cases.
- In the United States, prosecutors investigating the **2025 Palisades Fire** in California used digital evidence to build their case.
- They cited the suspect's interactions with ChatGPT, including questions about starting fires and AI-generated images of burning landscapes.
- These digital records were used to link the accused to the fire, which burned over 23,000 acres and destroyed thousands of homes.

Regulatory Changes to Tackle Digital Crime

- Cybersecurity incidents in India have surged from 10.29 lakh in 2022 to 22.68 lakh in 2024, reflecting the growing scale and sophistication of digital crime.
- The financial impact is also rising, with cyber fraud losses of ₹36.45 lakh reported on the **National Cyber Crime Reporting Portal** by February 2025.

SIM-to-Device Binding for Messaging Apps

- To curb misuse of digital platforms, the Department of Telecommunications (DoT) has directed messaging services like WhatsApp, Telegram, and Signal to enforce SIM-to-device binding.
- These apps must remain continuously linked to the SIM used at registration and deny access if the device does not contain that SIM.

New Legal Basis: Telecommunication Cybersecurity Amendment Rules, 2025

- The Centre is using powers under the Telecommunication Cybersecurity Amendment Rules, 2025 to regulate digital identifiers more tightly.
- The rules introduce the concept of a Telecommunication Identifier User Entity (TIUE).
- A TIUE is any non-telecom entity that uses telecommunication identifiers, such as mobile numbers, to identify users.
- This means apps that require phone numbers for registration fall within the regulatory scope.

Possible Expansion Beyond Messaging Apps

- The current directive targets messaging platforms.
- However, experts note that the broad TIUE definition could extend to other services, including food delivery apps like Swiggy and Zomato, since they also rely on mobile numbers for user onboarding.

Source: IE

Source: <https://vajiramandravi.com/current-affairs/digital-trails-and-policing-in-india-how-data-is-reshaping-crime-detection/>

© Vajiram & Ravi. For personal use only.