





Overview

The three new criminal laws, the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhinyam, which replace the Indian Penal Code (IPC), the Code of Criminal Procedure (CrPC), and the Indian Evidence Act respectively, will come into force from 1 July this year.

The new laws aim to consolidate the traditional provisions and procedures, making them more concise, contemporary, and relevant. The Bharatiya Nyaya Sanhita, specifically addressing organised crime, represents a significant shift in the legal landscape in India, with immense potential to empower a forensic investigation process.

Recent developments

The fight against organised crime is a relentless pursuit, demanding meticulous evidence gathering and data analysis to unravel intricate criminal networks. The three laws mark a welcome evolution in defining and tackling organised crime. Its comprehensive definition now encompasses extortion, cybercrime, and economic offences (financial scams) perpetrated by syndicates, offering greater investigation clarity and direction. Additionally, "petty organised crime" brings smaller yet harmful operations under the legal microscope, widening the scope for intervention.

The amendments, which include stricter penalties and punishments, will help enhance deterrence. This, along with extended police custody durations, could potentially lead to a surge in investigations and prosecutions, consequently increasing the demand for experts with forensic investigation experience.

However, the power of these amendments extends beyond numbers. The implementation of Bharatiya Sakshya Adhinyam recognises the pervasiveness of technology in criminal operations, with the legislation now allowing electronic records to be admissible evidence. This puts the impetus on law enforcement agencies to build further and use digital forensics infrastructure and expertise, ensuring evidence acquisition in a legally sound and secure manner for admissibility in courts.

Digital evidence—the game changer?

The integration of digital evidence presents a new frontier for forensic investigators. Analysing vast datasets, deciphering encrypted messages, and reconstructing digital timelines require specialised skills and sophisticated tools. Therefore, the growing need for specialised skill sets and greater expertise in the forensic domain, bolstered by this new legislation, places the onus on the community to further improve their methods, adopt new technologies, and play a key role in breaking down complicated criminal networks.

Existing frameworks, such as the Crime and Criminal Tracking Network and Systems (CCTNS) initiative, paved the way for digital integration in investigations. CCTNS has been successfully deployed across 16,347 police stations nationwide.¹ Complementing this, the Inter-operable Criminal Justice System (ICJS) represents an initiative striving to facilitate seamless data and information exchange among the key pillars of the criminal justice framework, including courts, police, jails, and forensic science laboratories, all unified under a single platform. Phase I has achieved individualised IT systems enabling efficient record searches. The focus of ongoing phase

¹ <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1863407>

It is towards effective modern policing methodologies and the adoption of one data, one entry principle, wherein information is entered only once within a given pillar (possibly directly from the crime scene through a hand-held device), yet seamlessly accessible across others without duplication of efforts. This framework streamlines digital evidence usage and significantly reduces the time traditionally required for data transfer and re-entry across different pillars of the criminal justice system.

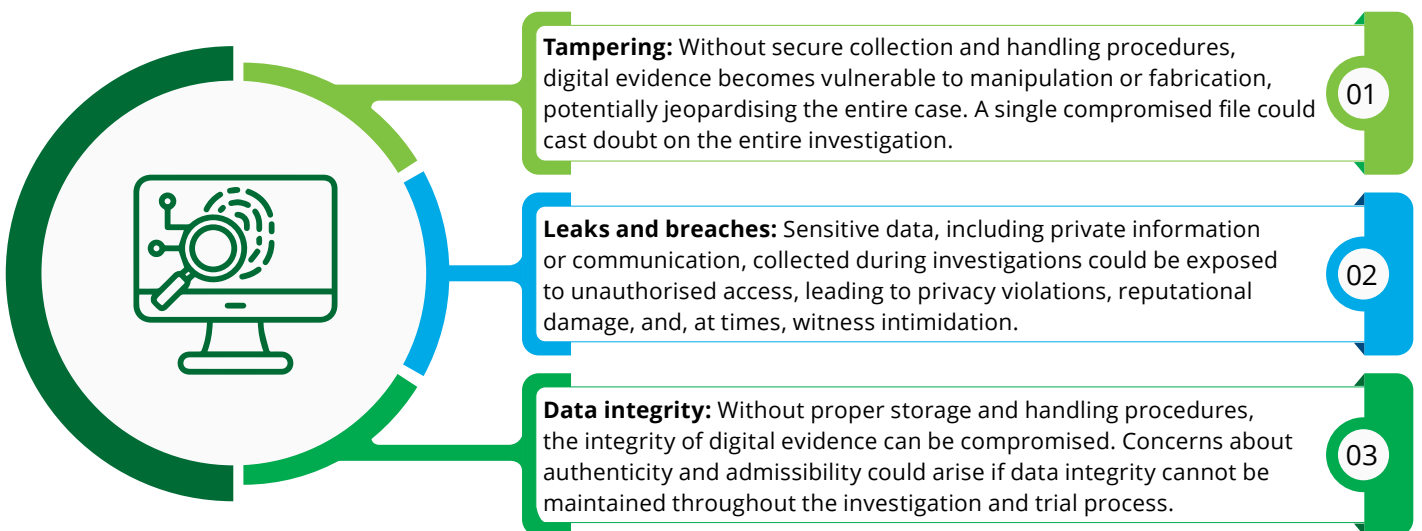
In addition, many states and Union Territories (UTs) in India are already building internal capacities to digitally capture and analyse financial transactions, online communication, social media links, traffic data, CCTV footage, and digital footprints.

The recent amendments, which allow electronic records to be admissible evidence, will drive more resources towards optimising the entire process of digital evidence flow from its origin to its use, thus maximising its impact.



Digital evidence and the possible uncertainties

While these reforms embrace the crucial role of digital evidence, a critical void remains unaddressed, i.e., the absence of robust chain-of-custody protocols. The lack of safeguards could result in issues such as:



These vulnerabilities could undermine the effectiveness of the legislation and may result in a loss of public trust in the justice system and a reluctance to cooperate with investigations. Therefore, it becomes crucial to follow guidelines that will help maintain the integrity and authenticity of the evidence collected while building and implementing these new policing technologies.

The way forward

The new laws represent a positive step towards combating crime. However, addressing the gap in digital evidence security is crucial to ensure its effectiveness and ethical implementation. We recommend:



Implementing robust chain-of-custody protocols

Establishing clear guidelines and procedures for collecting, storing, and transmitting digital evidence throughout the investigation process is essential. This includes maintaining detailed logs, employing encryption, and limiting access to an authorised workforce.



Enhancing investigator training

Training programmes should cover digital forensics techniques, chain-of-custody protocols, data security best practices, and legal considerations around electronic evidence.



Fostering industry collaboration

Encouraging collaboration between law enforcement agencies, forensic experts, e-courts, and technology companies can facilitate information sharing, knowledge exchange, and the development of innovative solutions to help secure digital evidence.

The new laws are a welcome change and will positively affect the future of policing in our country. However, these changes will also require the ability to embrace new working methodologies. Hence, integrating change management strategies and engaging stakeholders should be pivotal elements from the outset.



Connect with us

Rohit Berry

President
Strategy, Risk & Transactions
Deloitte India
rohitberry@deloitte.com

Nikhil Bedi

Partner and Leader – Risk, Regulatory & Forensic
Strategy, Risk & Transactions
Deloitte India
nikhilbedi@deloitte.com

KV Karthik

Partner and Leader - Forensic & Financial Crime
Strategy, Risk & Transactions
Deloitte India
kvkarthik@deloitte.com

Himanshu Arora

Partner – Forensic & Financial Crime
Strategy, Risk & Transactions
Deloitte India
himanshuarora@deloitte.com

Contributors

Runa Ray

Abhishek Jain

Malika Bhasin







Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

© 2024 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited