

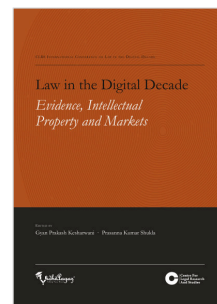
CHAPTER 1

Digital Forensic Readiness in India: Rethinking Criminal Investigations in the Digital Age

Tamanna Khatri and Grishma Bhavsar

in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 3–13

DOI <https://doi.org/10.63108/VAB.LDD.2.1>



CITATIONS

BLUEBOOK (21ST ED.)

Tamanna Khatri & Grishma Bhavsar, *Digital Forensic Readiness in India: Rethinking Criminal Investigations in the Digital Age*, in *LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS* 3 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Tamanna Khatri and Grishma Bhavsar, 'Digital Forensic Readiness in India: Rethinking Criminal Investigations in the Digital Age' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 3.

CHICAGO (17TH ED.)

Khatri, Tamanna, and Grishma Bhavsar. "Digital Forensic Readiness in India: Rethinking Criminal Investigations in the Digital Age." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 3–13. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.2.1>.

APA (7TH ED.)

Khatri, T., & Bhavsar, G. (2026). Digital forensic readiness in India: Rethinking criminal investigations in the digital age. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 3–13). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.2.1>

SOURCE

<https://doi.org/10.63108/VAB.LDD.2.1>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 1

Digital Forensic Readiness in India: Rethinking Criminal Investigations in the Digital Age

TAMANNA KHATRI* AND DR. GRISHMA BHAVSAR**

With the increasing reliance on smartphones, cloud computing technologies, social media sites, mobile money transfer systems, security networks and internet of things (IoT), the modus operandi of criminals along with that of conducting crime investigations, has been transformed to a great extent. Digital evidence has become crucial not only for cyber-crime investigations but also for traditional crimes. Nevertheless, it all depends upon whether the investigation agencies are proficient in handling the digital evidence before it becomes inaccessible through deletion or any other means. In this research, an effort has been made to assess the level of preparedness in digital forensics within the criminal justice process in India. This study aims at determining if the investigating bodies and forensics establishments have the necessary infrastructure, human resources, procedural framework and coordination mechanisms to deal with digital evidence in a timely and legal manner. The research methodology employed in this research is doctrinal and analytical. The current paper draws a distinction between digital forensic readiness and traditional digital forensics. In particular, whereas forensic investigation usually starts after the occurrence of a crime, forensic readiness implies advance preparation through retention of evidence, secure logging, first response training, incident response strategies and proper forensic labs. The main problems associated with digital forensic readiness in India include unequal distribution of infrastructure, lack of specialized experts, poor first response training, delay in forensic investigation and challenges in getting information from foreign and private service providers. This paper emphasizes that the mere legal recognition of electronic evidence is insufficient without any other preparations. It suggests creating a strategy for digital forensic readiness that relies on standardized procedures, professional training, accreditation of laboratories, secure evidence management system and collaboration of the criminal justice system.

Keywords: Digital Forensic Readiness, Digital Evidence, Criminal Investigation, Forensic Infrastructure, Institutional Preparedness, Criminal Justice System.

1 INTRODUCTION

The increased reliance on digital technologies has transformed the way crimes are committed, detected and investigated. Many of today's human activities leave behind a digital footprint. Mobile phone communications, financial transactions done online, social media communications, location tracking services, online cloud computing, closed-circuit television systems and other connected devices can all produce information which might become important for the purposes of criminal investigation. As a consequence of this development, digital evidence has ceased being confined to the category of cybercrimes. Digital evidence may be useful in cases of homicide, kidnapping, organized crime, financial crimes, drug trafficking, corruption, sexual offences and many other traditional crimes.¹ These developments have put

* PhD Scholar at Faculty of Law, GLS University, Ahmedabad, Gujarat, India.

** Assistant Professor at Faculty of Law, GLS University, Ahmedabad, Gujarat, India.

¹ United Nations Office on Drugs and Crime, *Digital Evidence*, Cybercrime Module 4; INTERPOL, *Metaverse: A Law Enforcement Perspective—Use Cases, Crime, Forensics, Investigation, and Governance*.

additional obligations on the investigative agencies. The mere presence of digital evidence does not mean it will be useful in the course of an investigation. The usefulness of digital evidence will depend on its timely identification, its preservation in its original state, proper acquisition techniques and finally analysis by the qualified specialists. Electronic evidence can be overwritten, deleted, modified remotely, encrypted and stored on devices outside the control of the investigating agency. In other words, the success of any digital investigation depends on the pre-investigatory work done in advance.²

This is how the idea of digital forensic readiness emerges. In general terms, forensic readiness can be understood as an institution's/forensic investigation system's capacity to foresee the possibility of using the digital evidence and develop the necessary systems for collecting and using it. This idea draws attention from the reactive model of forensic investigation towards a more systematic one.³ Similarly, international forensic guidelines have underlined the importance of incorporating forensics into incident response procedures instead of carrying out the forensic examination independently.⁴ India has introduced legislative measures regarding the use of electronic evidence. According to the Bharatiya Sakshya Adhiniyam, 2023, electronic or digital evidence is allowed to be used and such evidence cannot be refused admission just on account of its being stored in the electronic form. The Information Technology Act, 2000 also allows the central government to designate government departments or bodies as Examiners of Electronic Evidence.⁵

In addition to this, the Bharatiya Nagarik Suraksha Sanhita, 2023 has added further technological components to criminal procedure like the recording of searches and seizures by audio-visual means of electronics and processes of seeking help in investigation with regard to foreign territories.⁶ All these factors clearly prove that digitization has now become an integral part of the criminal justice process. But then, mere legalization of digitalization and procedural reform do not guarantee forensic readiness. It depends also on the preparedness of the officers of police, cyber-crime unit, forensic labs, prosecutor and other agencies. Hence, the issue is not just limited to the permissibility of the use of digital evidence in the Indian law, but the preparedness of the concerned authorities to obtain and process such evidence. The present paper attempts to analyze this issue in a doctrinal way. It defines the concept of forensic readiness with respect to digitalization, differentiates it from traditional digital forensics, looks at the present Indian institutional and legal framework, discusses the major problems involved in this issue and suggests measures to develop forensic readiness.

2 UNDERSTANDING DIGITAL FORENSIC READINESS

Digital forensics usually implies a series of procedures by which information kept or sent via electronic means is found, collected, acquired, retained, analysed and interpreted for investigative purposes. Standards like ISO/IEC 27037 offer recommendations related to identification, collection, acquisition and

² International Organization for Standardization, *ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (2012).

³ Robert Rowlingson, *A Ten Step Process for Forensic Readiness*, 2 Int'l J. Digital Evidence 1 (2004).

⁴ Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006).

⁵ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 61; Information Technology Act, No. 21 of 2000, § 79A.

⁶ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 105, 112–13.

retention of digital evidence.⁷ However, digital forensic readiness is a slightly different issue. It has to do with making sure that organizations are prepared for a situation when digital information could become evidence at some point in the future. More precisely, while traditional digital forensics seeks to find out how evidence could be analysed after a problem arose, forensic readiness focuses on how well the organization was prepared to retain evidence in the first place.⁸ The significance of this is that digital evidence has a limited life span. Logs could be auto-erased from the systems, cloud storage information would have been saved for limited periods, CCTV footage could be erased once space constraints are achieved and information stored on personal devices could have been tampered with during regular usage. If pertinent information is not captured at the right time, it will later be difficult for a sophisticated forensic laboratory to recreate it.⁹ Preparedness for forensics is more than just the availability of forensic tools. It entails having the infrastructure, skilled staff, roles and responsibilities, documentation process and methods of retaining evidence.¹⁰ At the level of the investigation, preparedness starts with the first officer that comes across any digital device or digital environment which could possibly provide relevant information. That officer should have the ability to identify whether the information available in the mobile phone, computer, security cameras, etc., is relevant and know how to preserve it until more specialized help arrives.¹¹ At the organizational level, preparedness refers to the ability of the forensic laboratory to collect, preserve, analyse and provide information about the digital evidence within an appropriate time frame. This also includes collaboration between investigators, forensics, prosecutors and technology service providers. Thus, the idea denotes the transition from a forensic to a preparedness-based investigation approach.¹²

3 IMPORTANCE OF DIGITAL FORENSIC READINESS IN MODERN CRIMINAL INVESTIGATION

Forensic readiness becomes necessary due to the evolving nature of evidence. Physical evidence is always in some tangible form that can be segregated from its surroundings. On the other hand, digital evidence is usually present in multiple devices, networks, platforms and jurisdictions. Hence, the process of its identification and acquisition requires investigators to know not just the physical device, but also the larger digital environment where the evidence is stored.¹³ One investigation might involve information from the mobile phone of the accused, as well as information from CCTV cameras, social media websites, cloud-based storage, financial institutions, telecommunications providers and third-party applications. The information from all of these sources is not controlled by the same agency and might not even be located in the jurisdiction conducting the investigation. Therefore, forensic readiness enables the

⁷ International Organization for Standardization, *ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (2012).

⁸ Robert Rowlingson, *A Ten Step Process for Forensic Readiness*, 2 Int'l J. Digital Evidence 1 (2004).

⁹ Barbara Guttman, Douglas R. White & Tracy Walraven, *Digital Evidence Preservation: Considerations for Evidence Handlers*, NISTIR 8387 (2022).

¹⁰ Robert Rowlingson, *A Ten Step Process for Forensic Readiness*, 2 Int'l J. Digital Evidence 1 (2004).

¹¹ National Institute of Justice, U.S. Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* (2d ed. 2008).

¹² Karen Kent et al., *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006).

¹³ International Organization for Standardization, *ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*.

investigator to identify such sources right at the beginning rather than confining the investigation to the device seized at the crime scene.¹⁴

The importance of preserving such information is more significant in cases where evidence is vulnerable and time sensitive. Logs could have been overwritten; cloud data could have been saved for limited times; CCTV footage could have been automatically deleted and there could be cases whereby the data changes through use of the device. Thus, delay would lead to loss of information, change in metadata or expiry of retention periods. Therefore, digital investigations are greatly dependent on the speed at which relevant sources are identified and preservation measures taken.¹⁵ Forensic readiness is directly proportional to the integrity and reliability of evidence collected in a case. Forensic readiness makes it easy for investigators to put in place standard procedures for seizing, documenting, forensic imaging, storage and transfer of digital devices. These standard procedures reduce unnecessary handling of electronic evidence and make it easy to establish an undisturbed chain of custody. The chain of custody is very crucial especially when the authenticity of the electronic evidence collected is challenged.¹⁶

The second key factor is investigative efficiency. When the investigators know what kind of evidence could possibly exist in the crime scene and how it needs to be handled, the forensic laboratories get much better-quality evidence for their analysis. Proper standardisation will also help to eliminate unnecessary delays that can occur due to inadequate documentation or failure of seizure or loss of evidence prior to its specialist analysis. Thus, forensic readiness allows using available technical capabilities more efficiently.¹⁷ It is important from the standpoint of forensic readiness that the digital forensic examination does not start when the evidence arrives at the specialized laboratory. It should start right from the first investigator who comes into contact with the digital crime scene. Forensic readiness can have a major impact on the usefulness of evidence.¹⁸ It follows that forensic readiness should not be considered just from a cybersecurity standpoint. In the criminal justice setting, forensic readiness is very much linked with investigative efficiency, evidentiary soundness and organizational competence. A legal system which accepts digital evidence but has not made the preparations to seize and secure the evidence could actually fail to gather crucial evidence for forensic analysis.

4 LEGAL FOUNDATION FOR DIGITAL EVIDENCE IN INDIA

The legal framework in India has increasingly acknowledged the role of electronic and digital records as a valid mode of evidence. The Bharatiya Sakshya Adhiniyam, 2023, which commenced from 1st July 2024, addresses the issue of the law of evidence in general in India. Sections 61 to 63 are particularly relevant for discussing electronic or digital records and their admissibility as evidence. While Section 61 defines that an electronic or digital record shall not be regarded as inadmissible simply on account of being in electronic form, Section 63 lays down the condition of computer outputs and electronic

¹⁴ Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006).

¹⁵ Id.; International Organization for Standardization, *ISO/IEC 27037:2012*.

¹⁶ International Organization for Standardization, *ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*.

¹⁷ Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006).

¹⁸ Id.; Eran Salfati & Michael Pease, *Digital Forensics and Incident Response Framework for Operational Technology*, NISTIR 8428 (2022).

records.¹⁹ There is also provision in the legislation regarding the involvement of experts. Section 39 of the Bharatiya Sakshya Adhiniyam is concerned with expert opinion and provides for relying on persons having special knowledge in relevant subjects. Furthermore, Section 79A of the Information Technology Act, 2000, gives power to the Central Government to notify an appropriate government department, body or agency as an Examiner of Electronic Evidence to give expert opinion in courts and other authorities.²⁰ This becomes particularly significant in cases in which the validation, acquisition or interpretation of electronic evidence requires particular forensic expertise. The application of such a technique is particularly significant in the context of forensic readiness in that it allows one to develop an organizational framework within which specialized laboratories can contribute to judicial proceedings in a formal manner. For instance, the Directorate of Forensic Science, Gandhinagar, Gujarat, was notified as an Examiner of Electronic Evidence under Section 79A in 2018.²¹

The procedural regime has become technology-centric as well. Under Section 105 of the Bharatiya Nagarik Suraksha Sanhita, 2023, the process of conducting search and seizure shall be recorded electronically using audio-visual electronic method, preferably using a mobile phone.²² Such recording will help achieve more transparency and proper documentation of the investigative process. The legislation has mechanisms dealing with letters of request and cooperation in investigations where the evidence or person is located in foreign territories.²³ All in all, such provisions indicate greater acceptance of technology in the fields of evidence laws and criminal procedure regime. The law has accepted the use of electronic records, specialist expertise and technological aid in investigation. However, such provisions ensure only the creation of legal authorization and safeguard of evidence, not necessarily the ability to handle digital evidence. This dichotomy plays an important role in the idea of forensic readiness. The law can allow for the collection and use of electronic evidence, yet readiness will determine if that evidence is able to be found, collected, analyzed and presented. This means that a sound legal basis needs to be paired with forensic capabilities in order for digital evidence to reach its full potential.

5 INSTITUTIONAL DEVELOPMENTS FOR DIGITAL FORENSIC INVESTIGATION IN INDIA

A lot of institutional developments have taken place in India, which aim at improving the capacity of the state to investigate cyber-crimes through digital forensic investigation. The term “institutional development” means that a state tries to develop infrastructure and process of coordination that would enable it to handle digital evidence in criminal investigations. For instance, the Ministry of Home Affairs formed the Indian Cyber Crime Coordination Centre (I4C) which serves as a coordinating body to handle cyber-crimes within India. The institutional bodies include the National Cybercrime Threat Analytics Unit, National Cybercrime Reporting Portal, Platform for Joint Cybercrime Investigation Teams, National Cybercrime Forensic Laboratory (NCFL) Ecosystem, National Cybercrime Training Centre, Cybercrime Ecosystem Management Unit, and National Cyber Crime Research and Innovation Centre.²⁴ The NCFL Ecosystem is particularly important in the context of forensic readiness since it seeks to support forensic

¹⁹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

²⁰ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 39; Information Technology Act, No. 21 of 2000, § 79A.

²¹ Ministry of Electronics and Information Technology, Government of India, Notification under § 79A of the Information Technology Act, 2000, notifying the Directorate of Forensic Science, Gandhinagar, Gujarat as an Examiner of Electronic Evidence (2018).

²² Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 105.

²³ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 112–113.

²⁴ Ministry of Home Affairs, Government of India, *Indian Cyber Crime Coordination Centre (I4C) Scheme*.

investigations using innovative technologies. According to the I4C, adequate facilities with the necessary equipment and sufficient numbers of skilled personnel should be available in order to keep up with technological advancements and support investigations.²⁵ These specialized facilities will help in carrying out investigations where the investigating officers do not have the required technical capabilities to conduct the examination of evidence collected.

In addition, the Ministry of Home Affairs has assisted in setting up cyber forensic and training laboratories in the States and Union Territories, besides conducting skill enhancement programs for law enforcement personnel, prosecuting officers and judicial officers. By June 2026, there were 33 laboratories set up in States and Union Territories, while over 24,600 law enforcement officers, prosecuting officers and judicial officers were trained in various subjects including cybercrime investigation and forensics.²⁶ It is especially pertinent because forensic readiness is highly dependent on human resources as well. More efforts have been devoted to developing forensics infrastructure at the State level. The government's initiatives aimed at improving DNA and cyber forensics have helped improve cyber-forensic infrastructure in State Forensic Science Laboratories. As mentioned by the Ministry of Home Affairs, the assistance provided through such initiatives has enabled the upgrade of DNA and cyber-forensic laboratories in State FSLs, with the aim of improving scientific examination in criminal investigation cases.²⁷

The described steps show that India has achieved considerable progress in building its institutional digital forensics capacity. Creation of specialized laboratories, training programs and national coordination systems is very important for building forensic readiness. Nevertheless, forensic readiness is not only about national laboratories or cybercrime units. Relevant capacity must be available at the stage of the first investigation to ensure proper preservation and documentation of digital evidence. The problem here then lies in making sure that the specialised institutional capabilities are converted into effective operational readiness at various levels of the criminal justice process. The national level infrastructure will be able to offer expertise and advanced forensic capability; however, the success of such an effort is contingent on collaboration with State authorities and the local authorities at the frontline.

6 MAJOR CHALLENGES TO DIGITAL FORENSIC READINESS IN INDIA

6.1 Inequalities in Institutional Capacities

Among the main challenges that can arise when trying to create forensic readiness is the issue of creating equal capacity in different geographical and institutional environments. Digital evidence can occur in any police station and in any criminal investigation, and not only in the specialized departments for dealing with cybercrime. This means that forensic knowledge, adequate tools, and specialists must be available in all large urban centres and not only in specialized institutions. A high-tech forensic lab can give an advanced forensic analysis, but its efficiency depends on how good the evidence brought to the lab is. If the evidence was poorly handled, documented, or preserved at the beginning of the process, it can considerably affect the whole forensic investigation. Acknowledging the significance of making forensic readiness available to more people, parliamentary committees have pointed out the need to improve forensic

²⁵ Ministry of Home Affairs, Government of India, *National Cybercrime Forensic Laboratory Ecosystem*, I4C Scheme.

²⁶ Press Information Bureau, Government of India, Ministry of Home Affairs, *National Cyber Crime Data* (July 21, 2026).

²⁷ Ministry of Home Affairs, Government of India, *Strengthening of DNA Analysis and Cyber Forensic Capacities in State FSLs* (updated Feb. 20, 2026).

infrastructure and use mobile forensic labs.²⁸ Forensic readiness should thus not be limited to national or State institutions, but rather reach the local investigating officer. The efficiency of advanced forensic infrastructure ultimately relies on readiness from the point where digital evidence is discovered.

6.2 First Responder Training

A critical role is played by the first responder coming across any digital evidence. Digital devices cannot always be treated like regular physical exhibits, as the interaction with the device might change some of the potential evidence. Interaction with an unlocked mobile phone, for instance, may change system data. Unplugging or turning off the specific devices without knowing all the facts may lead to loss of volatile data. Likewise, not detecting other connected accounts, networks, or cloud storage services may cause investigators to look at only the physical device and miss the remote location evidence. It is crucial, therefore, to have the correct first response procedure in place to make sure the value of digital evidence remains intact. It is unrealistic to train every police officer to become a forensic scientist. On the contrary, the investigating officers need enough knowledge of how to detect digital evidence, secure and document the scene, preserve potential evidence and seek help from specialists where needed. In this regard, the Bureau of Police Research and Development itself has specialized courses on cybercrime investigation, mobile forensics, and crime scene investigation.²⁹

6.3 Lack of Specialized Expertise

Forensic analysis is becoming more and more specialized. Current cases could involve mobile operating systems, encrypted apps, cloud computing, cryptocurrencies, Internet-of-things devices, malware, or a lot of multimedia data. Every one of these areas might demand its own tools, methods, and type of technical knowledge. It is difficult to possess expertise in all these areas due to the continuous evolution of technologies, operating systems, and forensic tools. Knowledge obtained during training could, thus, become obsolete due to the emergence of new technologies, platforms and ways of information storage or concealment. Forensic preparedness calls for continuous professional development and regular updating of technical skills. The very approach of the Indian institutions demonstrates awareness of this need. The National Cybercrime Training Centre within I4C aims at standardized training in cybercrimes, investigative training and training in simulated cyber environment, including a proposal of Cyber Range.³⁰ The Ministry of Home Affairs in India realizes the necessity to train forensic manpower and improve the existing forensic infrastructure.³¹

7 DIGITAL EVIDENCE STORED WITH PRIVATE SERVICE PROVIDERS

In modern-day investigations, evidence might not always be physically present in the possession of the person under investigation or even in the jurisdiction where the investigation is being conducted. Such

²⁸ Department-related Parliamentary Standing Committee on Home Affairs, Rajya Sabha, Report No. 252, Demands for Grants (2025–2026), Ministry of Home Affairs, paras. 4.14.6–4.14.7 (Mar. 10, 2025); Ministry of Home Affairs, Government of India, Reply to Lok Sabha Unstarred Question No. 3452, Infrastructure in Forensic Laboratories (Dec. 17, 2024).

²⁹ Bureau of Police Research and Development, Government of India, *Training Material and Courses on Investigation of Cyber Crime, Mobile Forensics and Crime Scene Investigation*.

³⁰ Ministry of Home Affairs, Government of India, *Indian Cyber Crime Coordination Centre—National Cybercrime Training Centre*.

³¹ Ministry of Home Affairs, Government of India, Reply to Lok Sabha Unstarred Question No. 3452, Infrastructure in Forensic Laboratories (Dec. 17, 2024).

evidence could be available with telecommunications companies, social media providers, cloud storage providers, or any other technology companies. In cases like these, while investigators might have physical possession of a device, the information, which could include account information, communication information, cloud storage backup, or transaction information, could be under the possession of the third-party service provider.³² It thus becomes a major challenge in terms of forensic readiness as the investigators would need to rely on the third-party service provider to preserve the information and provide the information at a later stage. It becomes imperative for the investigators to be able to figure out who the third-party service provider is, the type of information that is available from that service provider and how preservation or disclosure can be done in a legal manner.³³

Cooperation is particularly crucial when the data storage or control happens out of India. As a framework of comparative international law, the Budapest Convention on Cybercrime incorporates procedures and international cooperation provisions related to cybercrime and electronic evidence. In addition, the Budapest Convention serves as a model or guideline for international development of a country's approach to the use of electronic evidence and the Second Additional Protocol to it covers enhanced cooperation and disclosure of electronic evidence.³⁴ The criminal procedure law in India provides for the procedure for the seeking of assistance in investigations from other countries. Sections 112 and 113 of the Bharatiya Nagarik Suraksha Sanhita, 2023 deal with letters of request for investigation in a country or place outside India and letters of request received from foreign countries or places for investigation in India, respectively.³⁵ However, conventional processes of international assistance are not always as swift as the life cycle of digital evidence. The evidence in question might be fleeting, scattered over different jurisdictions or held by service providers situated in other countries. For this reason, current international talks regarding electronic evidence tend to address rapid evidence preservation, cooperation with service providers and efficient means of access from abroad.³⁶ Preparedness in the field of forensics implies, among other things, knowledge not only about the way digital evidence needs to be preserved technically, but also about its whereabouts, its controllers and the procedure according to which it needs to be preserved. Identification of service providers in good time, prompt making of preservation requests and knowledge about cooperation procedures at home and abroad can greatly minimize the chances of losing the evidence.

8 INTERNATIONAL STANDARDS AND THEIR SIGNIFICANCE FOR INDIA

Any good forensic readiness approach should take note of international standards on digital evidence collection and analysis. ISO/IEC 27037 is a standard providing recommendations concerning the identification, collection, acquisition and preservation of possible digital evidence. This includes a wide variety of evidence sources including computers, mobile devices, digital cameras, CCTV systems, networks and

³² Council of Europe, *Effective Access to Electronic Evidence*; Council of Europe, *COVID-19-Related Cybercrime and Electronic Evidence in Asia* (2022).

³³ Council of Europe, Convention on Cybercrime (Budapest Convention), arts. 16–18, E.T.S. No. 185 (2001); Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention), T-CY(2015)16 (adopted Feb. 28, 2017).

³⁴ Council of Europe, *Convention on Cybercrime (Budapest Convention); Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, CETS No. 224.

³⁵ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 112–113.

³⁶ Council of Europe, *International Cooperation on Cybercrime and Electronic Evidence; Second Additional Protocol to the Budapest Convention on Cybercrime*.

related technologies.³⁷ Also, NIST Special Publication 800-86 focuses on incorporating forensics into the incident response process. Instead of treating forensics as an independent and last resort procedure, this guide recommends understanding available data sources and developing approaches to conduct the proper forensics. Another NIST guidance about digital forensics and incident response regarding operational technology underlines the importance of preparation for incidents in advance, including formation of incident response teams and respective procedures.³⁸ Such an approach is significant for criminal investigations in India as it focuses on planning, standardization and forensics preparation instead of simple laboratory examination. India is not obligated to adopt all the international standards as they were designed for different legal frameworks. However, the ideas of documentation, responsibility distribution, data preservation, personnel and procedures validation can serve as an inspiration for the country.

9 TOWARDS A DIGITAL FORENSIC READINESS FRAMEWORK FOR INDIA

In order to ensure digital forensic readiness, it is necessary to establish such readiness as an integral criminal justice policy rather than an isolated technical approach. This involves integrating investigation, evidence collection, forensic analysis, prosecution and cooperation between institutions in order to ensure efficient management of digital evidence through its entire life cycle. First of all, there must be standard procedures developed for the first responders to follow. The investigating officers need to be provided with guidance regarding the identification of digital evidence, securing of devices, documentation of electronic scene, and acquisition of specialists' help. Such procedures should also define responsibilities for the first responder to prevent destruction of evidence before forensic analysis starts.³⁹ Secondly, it is vital to have continuous capacity building. Digital evidence awareness should be included into the usual training, whereas the specialists should undergo additional training which takes into account rapid change of technology. The National Cybercrime Training Centre within the I4C already shows the importance of training.⁴⁰

Thirdly, there needs to be more focus on laboratory capacity and quality assurance. Under Section 79A of the Information Technology Act, 2000, provision has been made for formally notifying Government Departments, bodies or agencies as Examiners of Electronic Evidence so that they may give expert opinions.⁴¹ It is therefore imperative that the necessary laboratory infrastructure is backed up with qualified personnel, valid forensic processes and quality control measures. Fourthly, there is a need to have better systems of managing digital evidence. Digital evidence should be properly managed right from the process of seizure to examination and finally production before the court. The use of access controls, audit trails, chain-of-custody and standardization can increase accountability and reduce disputes about the integrity or management of electronic evidence. Even international digital-evidence standards

³⁷ International Organization for Standardization, *ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (2012).

³⁸ Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006); Eran Salfati & Michael Pease, *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*, NISTIR 8428 (2022).

³⁹ International Organization for Standardization, *ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (2012).

⁴⁰ Ministry of Home Affairs, Government of India, *Indian Cyber Crime Coordination Centre (I4C) Scheme*, National Cybercrime Training Centre.

⁴¹ Information Technology Act, No. 21 of 2000, § 79A.

emphasize the systematic identification, collection, acquisition and preservation of digital evidence.⁴² Fifthly, forensic preparedness should facilitate coordination among agencies. Investigating agencies, forensic labs, prosecution and cybercrime units cannot operate in silos. The I4C framework has already incorporated this in its architecture with various mechanisms for joint cybercrime investigation, forensic support, training, research and coordination among law enforcement agencies and other stakeholders.⁴³

Sixth, there should be more effective mechanisms for working with private technology companies and handling cross-border digital evidence. Police should be trained not only in handling digital evidence but also in following the processes of collecting digital evidence through legal means. Sections 112 and 113 of the Bharatiya Nagarik Suraksha Sanhita, 2023 give mechanisms concerning letters of request for investigations pertaining to a foreign jurisdiction.⁴⁴ Other international conventions also recognize the need for urgent preservation and collaboration when it comes to cross-border electronic evidence. Lastly, readiness should be seen as a continuous process and not just an infrastructure development project. There will always be new types of devices, new platforms, storage devices, and problems related to investigation. Procedures, forensic methods, and professional training therefore need constant update to remain capable.⁴⁵

10 CONCLUSION

Digital evidence has become an ordinary and growing aspect of modern criminal investigations. The key issue before the criminal justice process then is not just whether the electronic evidence is legally recognized, but whether it is properly prepared to discover, secure, analyze and employ it. Under these circumstances, digital forensic readiness becomes the move from a reactive method to an environment where investigative agencies anticipate their need for digital evidence and prepare for it. India is well on its way in this regard. Not only is the Bharatiya Sakshya Adhiniyam, 2023 explicit about electronic and digital documents, the Information Technology Act makes provision for the appointment of Examiners of Electronic Evidence while the Bharatiya Nagarik Suraksha Sanhita, 2023 recognizes technology in criminal proceedings. There have been national initiatives such as I4C, cyber forensics labs and training centers among others. However, the last remaining task is to implement these laws and institutions as consistent readiness throughout the entire process of criminal investigations. Digital forensic readiness cannot be limited to the availability of sophisticated laboratories at institutional levels. Instead, digital forensic readiness must start from the very beginning with the officer in charge of investigating a case to include the processes of digital evidence recognition, collection, examination, interpretation, prosecution, and finally presentation in court. At any single stage of the process, weaknesses can render important digital evidence practically useless. In this light, there needs to be a national approach towards forensic readiness which includes standard operating procedures, training programs, laboratory facilities, good digital evidence management systems, inter-agency collaboration and effective measures for acquiring data owned by foreign and privately held service providers. International standards on information

⁴² International Organization for Standardization, ISO/IEC 27037:2012, *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (2012).

⁴³ Ministry of Home Affairs, Government of India, *Indian Cyber Crime Coordination Centre (I4C) Scheme*.

⁴⁴ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 112–113; Council of Europe, *International Cooperation Against Cybercrime*.

⁴⁵ Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006).

security management like ISO/IEC 27037 and forensic guidelines from NIST can help establish useful principles for evidence preservation, documentation, preparation, and incident response in the Indian context.

Forensic readiness, on the other hand, is a continuous process and should not be considered as a one-off technological or infrastructural investment. Digital technologies, storage mediums, means and modes of communications and modes of committing crimes are advancing at a very fast pace. It follows that forensic practices, techniques and skills have to be continuously assessed and updated to ensure that criminal justice institutions are able to respond to these changing modes of digital evidence. The general point is that technology alone cannot improve the efficiency of criminal investigation. Digital evidence will become effective only if the institutions charged with its handling are ready to act in the appropriate manner and at the appropriate time. The development of an organized process of digital forensic readiness will thus be an important component of the ongoing efforts of India to create an efficient and effective criminal justice system.

* * *