The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DIGITAL EVIDENCE IN THE INDIAN CRIMINAL JUSTICE SYSTEM: WITH SPECIAL REFERENCE TO THE NEW CRIMINAL LAWS OF 2023

~ Ayush Singh Tomar

ABSTRACT

India has, in recent years, moved away from its old criminal laws and brought in three new laws, namely the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. These laws have, among other things, given a much clearer legal standing to digital evidence. This paper tries to look at how digital evidence has grown in importance inside the Indian criminal justice system, what the old laws said about it, where they fell short, what the new laws say, and how courts have been dealing with this kind of evidence over the years. The paper also looks at the problems that still exist in actual practice, such as questions of tampering, custody of electronic records, admissibility, and the rights of accused persons. The paper argues that while the new laws are a welcome step, gaps in infrastructure, training of police and judges, and absence of a dedicated data protection framework continue to make the fair use of digital evidence a difficult task in India.

1. INTRODUCTION

Crime, in the world we live in today, does not stay within the walls of a house or at the corner of a street. It travels through mobile phones, computer networks, cloud servers, and encrypted messaging applications. When a person is cheated online, when a woman receives threats through social media, when a terrorist communicates with his associates over an internet call, the traces of these acts are all digital. They are stored in devices that are sometimes thousands of miles away from the court in which the case is being argued. This is the central challenge that the Indian criminal justice system has been trying to answer for the last two decades.

India was one of the first countries in Asia to pass a law specifically dealing with electronic transactions and cyber offences. The Information Technology Act came into force in the year 2000 and it brought with it certain provisions about electronic records and their evidentiary value.[1] This law was never meant to fully address every issue related to digital evidence. It was meant to work in conjunction with the Indian Evidence Act of 1872, which was created back when the telegraph was seen as a groundbreaking invention.[2] Consequently, this led to a mix of rules that courts had to interpret with care, and at times, inconsistently, whenever digital evidence came into play.

The year 2023 was a significant milestone. The Indian Parliament enacted three new laws that replaced the Indian Penal Code of 1860, the Code of Criminal Procedure of 1973, and the Indian Evidence Act of 1872.The year 2023 marked a turning point. The Parliament of India passed three new laws that replaced the Indian Penal Code of 1860, the Code of Criminal Procedure of 1973, and the Indian Evidence Act of 1872. These three new laws are the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam.

The last of these, the Bharatiya Sakshya Adhiniyam, directly deals with evidence and has given, for the first time in a consolidated manner, a proper definition and treatment of electronic or digital records.[3] These laws came into force in July 2024 and courts across India are now in the process of learning how to apply them.

This paper is an attempt to understand this shift in a thorough way. It looks at what digital evidence means, why it matters more now than ever before, what the old legal framework provided, where it created confusion, how the Supreme Court and various High Courts tried to fill the gaps through their judgements, and what the new laws have said in response to all of this. It also tries to identify what problems remain even after the new laws, because a good law on paper does not automatically translate into justice in a courtroom.

The paper uses a combination of doctrinal and analytical methods. It studies primary sources such as statutes and case law, and secondary sources such as law commission reports, government guidelines, and academic writing. The language used is simple and direct because

[1] Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament (India).
[2] Indian Evidence Act, 1872, No. 1 of 1872, Acts of Parliament (India).
[3] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Acts of Parliament (India), s. 2(1)(t).

the aim is not just to describe the law but to explain it to anyone who wishes to understand how India deals with evidence that lives inside a computer.

A few things are important to note at the outset. First, the word digital and the word electronic are used in Indian law in slightly different ways at different points, but for the purposes of this paper, they are used interchangeably to mean any record that exists in a form that is readable by a machine. Second, the paper does not deal with cyber offences themselves in detail. It focuses only on the question of evidence. Third, since the new laws are relatively recent, there are not yet a very large number of decided cases under them, and the paper therefore relies on both the case law under the old framework and the text of the new provisions.

2. UNDERSTANDING DIGITAL EVIDENCE

Before we explore the legal facets of digital evidence, it's crucial to understand its true meaning. In simple terms, digital evidence is any information or data that exists in a binary format and can be utilized in a court of law. It can exist on a laptop, a mobile phone, a pen drive, a compact disc, a server, or even in the cloud. It can take the form of text messages, emails, photographs, video recordings, audio clips, browser history, metadata, location data, call records, and transaction logs. The one thing that is common to all of it is that a human being cannot read it directly without the help of a machine or software.

The Bharatiya Sakshya Adhiniyam, 2023 has defined electronic or digital records quite broadly. It mentions that these records consist of emails, server logs, documents on computers, messages on devices, websites, and any audio, video, or images that are stored or sent digitally.[4] This list is way more comprehensive than what was provided under the previous law, and it really shows how people communicate and store information in today's world.

Digital evidence has unique characteristics that set it apart from physical evidence like fingerprints or bloodstains. First, it can be copied perfectly. When you make a copy of a digital file, the copy is identical to the original in every way that a computer can measure. This is both useful and dangerous. It is useful because investigators can work on copies without touching the original. It is dangerous because it is also easy to create a fake copy or alter the original without leaving any visible mark. Second, digital evidence is fragile. Unlike paper, which may survive for centuries, data on a device can be lost permanently if the device is switched on carelessly, if the wrong software is run on it, or if it is exposed to certain physical conditions.

[4] Bharatiya Sakshya Adhiniyam, 2023, s. 2(1)(t)(i)-(viii).

Third, digital evidence is often in the hands of third parties. When you send an email, a copy of it sits on the servers of a private company, often based in another country. When you use a payment app, your transaction records are with a company, not with you. This creates complications for investigators who need to access this evidence

The question of what constitutes the original and what constitutes a copy has always been important in evidence law. Under the old framework, there was a distinction between primary evidence and secondary evidence. Primary evidence was the original document and secondary evidence was a copy. Courts traditionally required primary evidence, and only in certain circumstances allowed secondary evidence. This distinction becomes complicated with digital records because there is no single original in the way there is with a piece of paper. Every computer that processes a file creates what could technically be called a copy. The law had to evolve to deal with this reality, and, as we shall see, this evolution was slow and uneven under the old framework.

There is also the question of metadata. Metadata is data about data. Every digital file carries information about when it was created, when it was last changed, who created it, what device was used, and in some cases where the device was located at the time. This information can be very important in a criminal investigation. A photograph may show a crime scene, but its metadata might show that it was taken three days after the alleged date of the offence. Call detail records contain not just the numbers called and the duration of calls, but also information about the cell towers used, which can tell investigators approximately where a person was at a given time. Courts have had to grapple with how to treat metadata, whether it falls within the definition of a document, and how much weight to give it.[5]

Digital evidence brings up concerns regarding its authenticity. A photograph can be edited using freely available software. A voice recording can be manipulated. A text message on a phone can be planted by someone who has access to the device. Unlike traditional forgery, which often leaves physical traces, digital manipulation can sometimes be done in a way that is very difficult to detect without specialist knowledge and equipment. This is why the law has to be careful about how it asks courts to approach digital evidence. Treating all digital evidence as automatically reliable would be dangerous. Treating it with so much suspicion that it becomes practically useless in prosecutions would also be harmful to justice.

[5] Dharambir v. CBI, (2008) 2 SCC 569.

The Indian courts have, over the years, dealt with digital evidence across a wide range of matters. These include corruption cases where emails and financial transaction records have been used to establish guilt, murder cases where mobile phone location data has been used to prove presence at the scene, cases of domestic violence where threatening messages have been presented as evidence, and election petition cases where video recordings and digital voter rolls have been scrutinised.[6] In each of these contexts, the legal questions about admissibility, authenticity, and weight have had to be answered afresh.

From an international perspective, India has looked to several countries for guidance. The United Kingdom, Australia, the United States, and many European countries have developed their own frameworks for digital evidence. The approach taken by India has, however, been shaped by its own constitutional values, the structure of its evidence law, and the realities of its investigative infrastructure, which is often under-resourced and under-trained in digital matters.[7]

3. LEGAL FRAMEWORK BEFORE THE NEW LAWS

Before the three new laws came into force, the legal framework for digital evidence in India rested on three main pieces of legislation. These were the Indian Evidence Act of 1872, the Information Technology Act of 2000, and the Code of Criminal Procedure of 1973. Each of these played a role, but together they created a framework that was often confusing and sometimes contradictory.

3.1 The Indian Evidence Act, 1872

The Indian Evidence Act was drafted by Sir James Fitzjames Stephen and enacted in 1872. It was a comprehensive piece of legislation that dealt with all aspects of evidence in civil and criminal matters. The original Act had no provision for electronic or computer-generated records because such things did not exist in 1872. Amendments were made over time to address this gap, but these amendments were inserted into a law that was fundamentally designed for a paper-based world.

The most significant amendment was the insertion of Section 65B into the Indian Evidence Act through the Information Technology Act of 2000.[8] Section 65B said that a printout or output

[6] Tukaram S. Dighole v. Manikrao Shivaji Kokate, (2010) 4 SCC 329.
[7] INTERPOL, Guidelines for Digital Forensics Laboratories, 2019.
[8] Information Technology Act, 2000, s. 65B as inserted by the Information Technology (Amendment) Act, 2008.

of a computer would be admissible as secondary evidence if certain conditions were met. These conditions were that the computer had been used regularly to store or process information, that it had been properly functioning, that the information had been produced in the ordinary course of activities, and that a person responsible for the operation of the computer certified all of these facts in a prescribed form. This certificate came to be known as the Section 65B certificate.

The condition of the certificate became the single most debated issue in Indian digital evidence law. Courts for many years were divided on whether the certificate was mandatory, who could give it, and whether its absence could be cured by oral evidence. The High Courts of different states took different views, and the matter kept going up to the Supreme Court.

Section 3 of the old Evidence Act defined the word document to include maps, graphs, photographs, and other inscriptions. This definition was used by some courts to bring electronic records within the definition of documents, which allowed them to be treated under the general rules of documentary evidence. However, this was a stretched reading and it created uncertainty.[9]

The old Act also had provisions about presumptions. Under Section 114, a court could presume the existence of a fact in the absence of evidence to the contrary. Some courts used this provision to presume that electronic records were genuine when there was no evidence challenging them. This was a practical approach but it was not entirely satisfactory from a jurisprudential standpoint because it bypassed the formal requirements of Section 65B.

3.2 The Information Technology Act, 2000

The Information Technology Act was passed primarily to give legal recognition to electronic transactions, electronic signatures, and electronic commerce. It also created offences relating to hacking, data theft, and obscene material online. Its provisions relating to evidence were, however, secondary to its main purpose and this showed in the way they were drafted.

Section 79A of the Information Technology Act gave the Central Government the power to appoint any department, body, or agency as an examiner of electronic evidence.[10] The purpose was to have a government-recognised body that could provide expert opinion on electronic

[9] Ram Singh v. Col. Ram Singh, 1985 Supp SCC 611.
[10] Information Technology Act, 2000, s. 79A.

records, which would then be admissible in court. The Centre for Development of Advanced Computing, known as CDAC, and certain state forensic science laboratories were designated as such examiners. In practice, however, the availability of such examiners was limited and the delays in obtaining their reports added to the burden on courts.

The Act also provided, under Section 65B, that electronic records could be admitted as evidence if the prescribed conditions were met. As noted above, this provision was inserted into the Evidence Act but the Information Technology Act also contained provisions that supported it. The definition of electronic record in the Information Technology Act was broad enough to cover most forms of digital data that courts encountered.[11]

The Information Technology (Amendment) Act of 2008 brought in several changes, including a new provision for electronic signatures and changes to the way in which certain offences were defined. However, the core provisions relating to the admissibility of electronic evidence remained largely unchanged.

3.3 The Code of Criminal Procedure, 1973

The Code of Criminal Procedure governed the procedure for investigation, arrest, trial, and appeal in criminal matters. It did not have any provision specifically dealing with the search and seizure of electronic devices or the preservation of digital evidence. Police officers investigating cases involving computers or mobile phones had to rely on the general provisions about search and seizure under Sections 91, 93, and 165 of the old Code.

These provisions were not designed with digital evidence in mind. They spoke of documents and things, which courts interpreted to include electronic devices, but they gave no guidance on how such devices were to be handled after seizure, how copies were to be made, or how the integrity of the data was to be maintained. The absence of a specific procedure for digital evidence meant that investigators often improvised, and this improvisation sometimes resulted in evidence being challenged successfully in court.

There was also no provision in the old Code that addressed the situation where evidence was stored on a server located outside India or with a third-party service provider inside India. In such cases, investigators had to rely on mutual legal assistance treaties, informal requests to companies, and sometimes the willingness of platform providers to cooperate voluntarily. This

[11] Information Technology Act, 2000, s. 3A as inserted by Amendment, 2008.

was a significant gap because a very large proportion of digital communication today goes through servers owned by companies based in the United States.

3.4 The Interplay of These Three Laws

The three laws were supposed to work together but in practice they created confusion. A court hearing a criminal case involving digital evidence had to look at the Indian Evidence Act for the rules about admissibility, the Information Technology Act for the definition of electronic records and for the provision about certification, and the Code of Criminal Procedure for the procedural rules about how the evidence had been gathered. When these laws pointed in different directions, as they sometimes did, it was left to the judges to resolve the conflict. This was not always done in a consistent way.[12]

The Law Commission of India, in its report on reviewing the Indian Evidence Act, had pointed out many of these gaps and had recommended that the law be amended or replaced to provide clearer rules for digital evidence.[13] This recommendation, along with the broader exercise of reforming the criminal laws, eventually led to the three new laws of 2023.

4. JUDICIAL INTERPRETATION UNDER THE OLD FRAMEWORK

Indian courts, particularly the Supreme Court, played a very active role in shaping the law on digital evidence because the statutory framework was incomplete. The judgements in this area can be grouped broadly into those that dealt with the certification requirement, those that dealt with the weight and reliability of electronic evidence, and those that dealt with the procedure for its collection.

4.1 The Question of the Certificate

The most important case on the Section 65B certificate is *Anvar P.V. v. P.K. Basheer,* decided by the Supreme Court in 2014.[14]This was an election matter in which compact discs containing video recordings were sought to be admitted in evidence. The Supreme Court, in a three-judge bench decision, held that the certificate under Section 65B was not optional. It was mandatory and without it, electronic evidence could not be admitted. The Court also said that oral evidence

[12] Law Commission of India, Report No. 269, Review of the Indian Evidence Act, 1872 (2017).
[13] Law Commission of India, Report No. 269, Review of the Indian Evidence Act, 1872 (2017).
[14] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473

could not substitute for the certificate. This decision put a heavy burden on parties who wished to rely on electronic evidence.

The Anvar P.V. decision was widely praised for bringing clarity, but it also created problems in practice. There were cases where the certificate could not be obtained because the person responsible for the computer had died, had left the organisation, or was not cooperating. There were cases where the police had seized a device and wanted to produce it in evidence but could not get a certificate because they did not know who had operated the relevant computer. The rigidity of the requirement led to some guilty persons escaping conviction because technically correct but practically difficult-to-obtain certificates were absent.[15]

In 2018, the Supreme Court revisited the question in *Shafhi Mohammad v. State of Himachal Pradesh.*[16]A two-judge bench took a somewhat different view and said that the certificate requirement could be relaxed in cases where the electronic evidence was produced by a party who was not in possession of the device, such as an accused person seeking to use evidence in their defence. This created an apparent conflict with the Anvar P.V. decision and courts across the country were again uncertain about what rule to apply.

The matter was finally settled by a three-judge bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal in 2020.*[17] The Supreme Court reaffirmed that the certificate under Section 65B was mandatory, that the Shafhi Mohammad decision was per incuriam to the extent it diluted this requirement, but also added an important qualification. The Court said that if a party made a timely application to the court or to the other party for the certificate and it was not provided, then the court could draw an adverse inference against the party who had refused to provide it. The Court also said that the certificate requirement was a procedural one and that its waiver could be considered in cases of grave injustice.[18]

The Arjun Panditrao judgment clarified the position regarding Section 65B, although courts had already spent considerable time interpreting the provision. The repeated litigation on this issue also showed that the earlier legal framework was not fully clear regarding electronic evidence.

[15] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, para 24.

[16] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.

[17] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

[18] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, para 22.

4.2 Cases on Weight and Reliability

Apart from admissibility, courts also had to decide how much weight to give to electronic evidence that had been admitted. In the famous Parliament attack case, *Navjot Sandhu v. State (NCT of Delhi),* the Supreme Court considered the admissibility of call records and electronic evidence. [19] The Court held that secondary evidence of electronic records could be given and that the absence of a certificate did not automatically render the evidence inadmissible, provided there was other evidence supporting it. This decision, rendered before Anvar P.V., took a more liberal approach.

In *Tomaso Bruno v. State of U.P*., decided in 2015, the Supreme Court considered the weight to be given to CCTV footage.[20]The Court held that CCTV footage, if properly authenticated and supported by the certificate, could be very reliable evidence. However, it also cautioned that the absence of any tampering had to be established and that the footage had to be corroborated by other evidence before a conviction could be based on it alone.

In *Ritesh Sinha v. State of U.P*., the question was whether a voice sample could be taken from an accused for the purpose of comparison with a recorded voice.[21] The Supreme Court held that it could, subject to safeguards, and this opened the door for voice analysis as a form of digital evidence. The Court observed that legal procedures should adapt to technological developments.

In *K. Ramajayam and Appu v. Inspector of Police*, the Supreme Court considered a situation where the certificate under Section 65B had not been obtained at the time of filing the chargesheet but was obtained later.[22]The Court took a somewhat lenient view and said that the certificate could be filed at any time before the document was actually tendered in evidence. This interpretation reduced the possibility of important evidence being rejected only because of procedural delay.

4.3 Cases on Collection and Procedure

Courts also had to deal with questions about how digital evidence had been collected. In *Virendra Khanna v. State of Karnataka*, the High Court examined whether data extracted from a seized mobile phone could be admitted when the accused claimed that the phone had been

[19] Navjot Sandhu and Afsan Guru v. State (NCT of Delhi), (2005) 11 SCC 600.
[20] Tomaso Bruno v. State of U.P., (2015) 7 SCC 178.
[21] Ritesh Sinha v. State of U.P., (2019) 8 SCC 1.
[22] K. Ramajayam @ Appu v. Inspector of Police, (2016) 11 SCC 73.

tampered with after seizure.[23]The Court said that the investigating agency had a duty to maintain a proper chain of custody and that any break in this chain would affect the weight of the evidence, though not necessarily its admissibility.

In *Dharambir v. CBI, the Delhi High Court* considered the role of electronic evidence in a corruption matter.[24]The Court emphasised that while electronic evidence was increasingly important, courts should not be dazzled by technology and should apply the same standards of scrutiny to digital records that they applied to other forms of evidence. This was an important reminder that the existence of a certificate did not mean that the evidence was beyond challenge.

Together, these judgments helped courts address several gaps relating to electronic evidence. However, this body of case law was not always consistent, it varied between High Courts, and it placed a heavy burden on litigants to navigate a complicated set of rules. These difficulties eventually led to the reforms introduced through the 2023 criminal laws.

5. THE NEW CRIMINAL LAWS OF 2023 AND DIGITAL EVIDENCE

The three new criminal laws, namely the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam brought major changes to the Indian criminal justice system. All three laws have provisions that are relevant to digital evidence, though the Bharatiya Sakshya Adhiniyam is most directly concerned with evidentiary questions.

5.1 The Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, which replaced the Indian Evidence Act, has given electronic or digital records a much more prominent place than the old law. The Act begins its treatment of documents by explicitly including electronic records within the definition.[25]It then goes on to provide rules for how such records are to be treated, what kinds of presumptions can be made about them, and what conditions they must satisfy to be admissible.

Section 57 of the new Act deals with the forms of secondary evidence.[26]It says that electronic or digital records, including records stored in any device, can be secondary evidence of the

[23] Virendra Khanna v. State of Karnataka, 2021 SCC Online Kar 9853.
[24] Dharambir v. CBI, (2008) 2 SCC 569.
[25] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Acts of Parliament (India), s. 2(1)(t).
[26] Bharatiya Sakshya Adhiniyam, 2023, s. 57.

original. This is an important clarification because, as noted earlier, there is often no single original when it comes to digital files. The provision takes into account the practical nature of digital records.

Sections 58 to 60 deal with primary and secondary evidence in greater detail.[27]These sections make clear that where a document is in electronic form, the law will not insist on the production of a physical original. What matters is that the electronic record has been maintained properly and that it can be shown to be a genuine and unaltered copy of the relevant data.

Section 61 of the Act deals with the admissibility of electronic records generally.[28] It says that all documents, including electronic records, shall be proved by primary evidence except in the cases mentioned in the Act. These provisions make the process of proving electronic records comparatively clearer than before.

Section 63 is the provision that replaces the old Section 65B.[29]It deals with the admissibility of electronic records as secondary evidence. The provision retains the requirement for a certificate but it makes certain changes to make this requirement more workable. The conditions for admissibility are similar to the old provisions, requiring that the computer was in regular use, that it was properly functioning, and that the information was produced in the ordinary course of activities. However, the new provision also addresses the situation where it is not reasonably practicable to produce the original and allows for more flexibility in such cases.

Section 63(4) of the new Act specifically deals with the certificate requirement.[30] It says that a person responsible for the operation or management of the relevant computer or device must certify that the conditions for admissibility are met. This is consistent with the Arjun Panditrao decision. However, the new Act also makes clear that the certificate can be given by different categories of persons depending on the situation, and This change attempts to deal with some practical problems faced under the earlier law

5.2 The Bharatiya Nagarik Suraksha Sanhita, 2023

[27] Bharatiya Sakshya Adhiniyam, 2023, ss. 58-60.
[28] Bharatiya Sakshya Adhiniyam, 2023, s. 61.
[29] Bharatiya Sakshya Adhiniyam, 2023, s. 63.
[30] Bharatiya Sakshya Adhiniyam, 2023, s. 63(4).

The Bharatiya Nagarik Suraksha Sanhita, which replaced the Code of Criminal Procedure, has introduced several provisions that are directly relevant to the collection and handling of digital evidence.[31]

Section 94 of the new Code deals with summons to produce documents or electronic records.[32]It explicitly mentions electronic records and makes clear that a court can summon any person, including a service provider or platform, to produce electronic records that are relevant to a case. This provision removes the earlier ambiguity regarding electronic records. Now there is no ambiguity.

Section 105 of the new Code deals with search and seizure and it specifically mentions electronic devices and data storage media.[33]The provision requires that when an electronic device is seized, a copy of the data contained in it must be made in the presence of witnesses and the device or the copy must be sealed. This requirement is consistent with standard digital forensic procedure. However, as we shall discuss later, the provision does not go into the detailed protocols that would be needed for it to be truly effective.

Section 173 of the new Code deals with the investigation of offences and requires the police to maintain detailed records of the investigation, including a record of any electronic evidence found or seized.[34]This provision supports the requirement of a proper chain of custody, which is essential for the admissibility of digital evidence.

5.3 The Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, which replaced the Indian Penal Code, is primarily a substantive criminal law and does not deal directly with questions of evidence.[35] However, it has expanded the range of offences that involve digital means, including provisions on organised crime, cyber terrorism, and offences against women that are committed through electronic means. The definition of these offences has implications for the kind of evidence that will be needed to prove them, and courts will increasingly have to rely on digital records to establish the elements of many of these offences.

5.4 The Significance of the New Laws

[31] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, Acts of Parliament (India).
[32] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 94.
[33] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 105.
[34] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 173.
[35] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament (India).

Overall, the new laws attempt to modernise criminal procedure and evidence relating to digital records. The definition of digital records is comprehensive. The rules about admissibility are clearer. The procedural provisions for search and seizure have been updated. Courts are no longer required to stretch the language of a nineteenth-century statute to accommodate twenty-first-century evidence.

However, there are areas where the new laws have not gone far enough or where the provisions raise new questions. These will be discussed in the chapters that follow. The point to emphasise at this stage is that the new laws provide a better foundation than the old ones, but a good foundation is not the same thing as a complete structure. Even after these reforms, several practical issues still remain in terms of drafting subordinate legislation, training investigators and judges, building the infrastructure of forensic laboratories, and creating a consistent practice across the courts.

6. COLLECTION, PRESERVATION AND CHAIN OF CUSTODY

The best legal framework for digital evidence will be of little use if the evidence is collected poorly in the first place. The collection of digital evidence is a specialised task that requires training, equipment, and adherence to standard procedures. In India, the state of digital forensics varies enormously between different police forces and different states.

6.1 What Good Collection Practice Requires

When an investigating officer reaches the scene of a cybercrime or a crime that involves digital evidence, the first task is to identify all potential sources of evidence. These may include mobile phones, computers, external hard drives, routers, CCTV cameras, smart watches, or any other device that stores or transmits data. The officer must then ensure that these devices are not switched on or off, that they are not connected to the internet, and that no data is overwritten or deleted accidentally. This requires specific knowledge about how different devices behave and what actions can cause data loss.

The standard practice in forensic investigation is to create what is called a forensic image of a seized device. A forensic image is an exact bit-by-bit copy of all the data on a device, including deleted files and hidden partitions. The image is created using specialised software that also generates a hash value, which is a kind of digital fingerprint that can be used later to verify that

the copy has not been altered. All investigation work is then done on the copy, not on the original. The original device is sealed and stored as an exhibit.[36]

This practice is internationally recognised and is the standard recommended by organisations such as INTERPOL.[37] However, it requires equipment and software that is not always available at the police station level in India. Many smaller police stations do not have forensic imaging tools and the local officer has no choice but to work with the device directly, which risks corrupting or overwriting the evidence.

6.2 Chain of Custody

The chain of custody is a record of who had the evidence, when they had it, what they did with it, and when they passed it on to the next person. It is essentially a trail of documentation that starts from the moment the evidence is seized and ends when it is produced in court. A proper chain of custody is important in digital investigations. First, it shows that the evidence has not been tampered with. Second, it makes it possible for the court to assess the reliability of the evidence.

Under the old Code of Criminal Procedure, there was no specific provision about chain of custody for electronic evidence. The new Bharatiya Nagarik Suraksha Sanhita has improved the position by requiring detailed documentation of seized electronic material, but it does not prescribe the exact form of the chain of custody record. This is a gap that needs to be filled through rules or guidelines issued by the Ministry of Home Affairs or the Bureau of Police Research and Development.[38]

The consequences of a broken chain of custody can be serious for a prosecution. In *Sanjay Singh v. State of U.P.,* the court found that the investigating officer had failed to properly document the handling of a seized mobile phone and that the data extracted from it could not be relied upon because there was no way to verify that it had not been altered between seizure and production in court.[39] These cases show the importance of following proper procedure during investigation for effective prosecution

[36] Ministry of Home Affairs, Standard Operating Procedure for Cyber Crime Investigation, Government of India, 2021
[37] INTERPOL, Guidelines for Digital Forensics Laboratories, 2019.
[38] State of Punjab v. Baldev Singh, (1999) 6 SCC 172 — principle of fair investigation applied in digital context.
[39] Sanjay Singh v. State of U.P., 2022 SCC Online All 1067.

6.3 The Role of Forensic Laboratories

India has a network of forensic science laboratories at the central and state levels. The Central Forensic Science Laboratory, operating under the Ministry of Home Affairs, and its counterparts in the states are responsible for examining electronic evidence. However, the demand for forensic analysis has grown far more rapidly than the capacity of these laboratories. Pendency of cases in forensic labs, combined with shortages of trained digital forensic examiners, means that reports sometimes take months or even years to arrive, which adds to the delay in trials.[40]

The Ministry of Home Affairs has issued standard operating procedures for cyber-crime investigation, which set out the steps to be followed for the seizure and analysis of digital evidence.[41]These procedures are broadly in line with international best practices. However, compliance with these procedures is not uniform and there is no mechanism for monitoring or enforcing compliance in a systematic way.

Section 79A of the Information Technology Act, as noted earlier, provides for the appointment of examiners of electronic evidence.[42] These examiners are meant to provide court-admissible reports on electronic records. In practice, the number of government-designated examiners is small relative to the number of cases that require examination. Private digital forensic firms are increasingly used in practice, particularly in commercial disputes, but there is no framework that gives their reports automatic admissibility in criminal proceedings.

6.4 The Issue of Cross-Border Data

A growing proportion of digital evidence in criminal cases involves data that is stored on servers located outside India. When a suspect uses Gmail, WhatsApp, or any other service provided by a foreign company, their communication records are on servers that are not within the physical jurisdiction of Indian courts and police. Obtaining this data requires going through formal mutual legal assistance treaty procedures, which can take a very long time, or through voluntary disclosure by the companies, which varies depending on the company's policies and the nature of the request

[40] Standing Committee on Information Technology, Report on Cyber Crime, Prevention, Detection and Management, Lok Sabha, 2021-22.
[41] Ministry of Home Affairs, Standard Operating Procedure for Cyber Crime Investigation, Government of India, 2021
[42] Information Technology Act, 2000, s. 79A.

The Bharatiya Nagarik Suraksha Sanhita does not directly address this problem. India has mutual legal assistance treaties with a number of countries but not with all countries. The process under these treaties is slow. Some technology companies have published transparency reports that show the number of data requests they receive from Indian authorities, and the proportion that they comply with, but there is no domestic law that comprehensively addresses this issue.[43] This remains a significant gap in India's digital evidence framework.

7. ADMISSIBILITY AND CERTIFICATION REQUIREMENTS

The question of admissibility is the gateway question for digital evidence. Evidence that is not admitted simply cannot be considered by the court, no matter how probative it might be. The framework for admissibility of digital evidence under the new laws is built on the foundation laid by the courts under the old framework, but it incorporates important changes.

7.1 The Certificate Requirement Under the New Law

As noted in the previous chapter, Section 63 of the Bharatiya Sakshya Adhiniyam is the provision that deals with the admissibility of electronic records as secondary evidence. The certificate requirement has been retained, which means that the jurisprudence developed by the Supreme Court in *Anvar P.V. and Arjun Panditrao* continues to be relevant as a guide to how courts should approach the new provision.[44]

The certificate must be provided by a person responsible for the operation or management of the computer or device. Under the new law, this can include a network service provider, a data custodian, or any other person who manages the relevant system. This is a broader definition of who can give the certificate than what was implied under the old provision, and it should make it easier to obtain certificates in cases where a specific individual cannot be identified as the person responsible for the computer.

The new Act also allows for the certificate to be given in cases where the electronic record has been produced from a computer system that was regularly used over a period for storing or processing information for the activities regularly carried on over that period. This is a requirement of continuity and regularity that is meant to ensure that the computer system was

[43] National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India, available at https://cybercrime.gov.in (last visited May 2025).

[44] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, para 48.

functioning normally and that the record was not specially created for the purpose of the litigation.

7.2 Presumptions About Electronic Records

One of the important changes made by the Bharatiya Sakshya Adhiniyam is in the area of presumptions. **Section 79** of the new Act provides for a presumption that an electronic record that has been certified in the prescribed manner is genuine.[45]This means that once a certificate is produced, the court can presume that the record is what it purports to be, without requiring further proof of genuineness. After certification is produced, the opposing party may challenge the authenticity of the record.

Section 81 of the new Act deals with presumptions about records in electronic form that have been published on official websites of central or state governments.[46] Such records are presumed to be genuine without any further proof. This provision simplifies the use of official electronic records in court proceedings that avoids the need for bureaucratic certification every time a government record is produced in court.

Section 85 of the Act deals with presumptions about electronic agreements and electronic messages.[47] It says that a court shall presume that an electronic message forwarded by the originator through a messenger or service provider was sent with proper authority. This provision is relevant in cases involving fraud or contractual disputes where the question of whether a message was genuinely sent by a particular person is in issue.

7.3 The Question of Oral Evidence

Under the old framework, as settled by the Anvar P.V. decision, oral evidence could not substitute for the Section 65B certificate. The new law does not change this position. The certificate remains mandatory for the admission of electronic records as secondary evidence. However, the new law recognises that there are situations where the certificate cannot reasonably be obtained, and it provides some guidance for such situations.

In *P. Yuvaprakash v. State,* the Madras High Court considered the situation where a mobile phone had been lost after seizure and the prosecution sought to rely on screenshots of messages

[45] Bharatiya Sakshya Adhiniyam, 2023, s. 79.
[46] Bharatiya Sakshya Adhiniyam, 2023, s. 81.
[47] Bharatiya Sakshya Adhiniyam, 2023, s. 85.

from the phone.[48] The Court held that in such circumstances, the prosecution had to explain the loss and provide the best evidence available This case highlights some practical problems faced during investigation and evidence collection and the need for courts to apply the law with a degree of common sense while not abandoning the requirements of proof.

7.4 The Problem of Tampering

Even when a certificate has been produced and the evidence has been admitted, the question of tampering can be raised at any stage. A party who claims that electronic evidence has been tampered with must provide some basis for this claim, not just make a bare assertion. Courts have been generally sceptical of blanket allegations of tampering and have required some evidence to support such a claim before they will investigate it further.[49]

The use of hash values, as mentioned in the context of forensic imaging, is the most reliable way to establish that a digital file has not been altered. When a hash value is recorded at the time of seizure and the same value is produced at the time of production in court, it provides very strong evidence that the file is the same. Courts in India have begun to understand the significance of hash values, and some have even asked for them to be produced as part of the record. However, there is no statutory requirement for hash values to be produced, and this remains a gap in the framework.

In *Jagdish v. State of Rajasthan*, the court noted that the failure of the prosecution to produce the hash value of a seized hard drive, when it had the technology and the knowledge to do so, was a factor that weakened the prosecution's case, even though this approach encourages investigators to maintain proper forensic standards without making it a rigid requirement that could be used to defeat otherwise reliable evidence.

8. Privacy, Rights of the Accused and Digital Evidence

The use of digital evidence in criminal proceedings raises serious questions about the right to privacy. A mobile phone or a laptop is not just a piece of equipment. It is a repository of a person's most private communications, their financial information, their medical records, their photographs, and their correspondence. When the state seizes such a device as part of an investigation, it obtains access to everything on it, not just the material that is relevant to the

[48] P. Yuvaprakash v. State, 2023 SCC Online Mad 6431.
[49] Nilesh Dinkar Paradkar v. State of Maharashtra, (2011) 13 SCC 613.

crime being investigated. This situation raises concerns regarding the balance between investigation and privacy rights.

8.1 The Right to Privacy in the Constitutional Framework

The Supreme Court of India, in the landmark case of *Justice K.S. Puttaswamy v. Union of India,* held unanimously that the right to privacy is a fundamental right under the Constitution of India.This decision, delivered by a nine-judge bench, has wide implications for the use of digital evidence. It means that any state action that intrudes into a person's private digital information must satisfy the requirements of legality, necessity, and proportionality. A general order to seize all the devices in a house, without any specific justification for why each device is needed, would be disproportionate and would violate the constitutional right to privacy.

The implications of the Puttaswamy decision for the search and seizure of electronic devices have not yet been fully worked out by the courts. The new Bharatiya Nagarik Suraksha Sanhita has improved the procedural framework, but it does not specifically address the proportionality requirements that flow from the constitutional right to privacy. This is a gap that is likely to be the subject of litigation in the coming years.

8.2 The Right Against Self-Incrimination

Article 20(3) of the Constitution of India says that no person accused of an offence shall be compelled to be a witness against himself. This right against self-incrimination has been tested in the context of digital evidence in several cases. The question is whether compelling an accused person to provide the password to their phone or computer violates this right.

In Virendra Khanna v. State of Karnataka, the court held that compelling a person to provide the password to their phone amounted to compelling them to be a witness against themselves and was therefore unconstitutional.[50]However, the matter is not settled and different courts have taken different views. There is a distinction between compelling a person to reveal something they know, which is arguably testimonial and protected by Article 20(3), and compelling a person to provide something they have, such as a biometric key, which may not be testimonial in the same sense.

The Ritesh Sinha case addressed the related question of voice samples and the Supreme Court held that a magistrate could order an accused to provide a voice sample for comparison

[50] Virendra Khanna v. State of Karnataka, 2021 SCC Online Kar 9853.

purposes.[51] The Court reasoned that a voice sample was not testimonial in nature and did not therefore violate Article 20(3). This reasoning could potentially be extended to biometric data such as fingerprints used to unlock phones, but the Court has not yet definitively ruled on this question in the context of phone unlocking.

8.3 Surveillance and Digital Evidence

Another dimension of the privacy question is the use of surveillance to obtain digital evidence. The Indian government has powers of interception of communications under the Indian Telegraph Act and the Information Technology Act. These powers allow the government to intercept telephone calls and electronic messages in the interest of national security, public order, or the investigation of crime. However, there is no independent judicial oversight of these interception orders, which raises concerns about their potential for abuse.[52]

The National Investigation Agency, which investigates terrorism-related cases, has specific powers to access electronic records and to direct service providers to assist in investigations.[53] The Prevention of Money Laundering Act also gives the Enforcement Directorate broad powers to access digital financial records.[54] In both cases, the absence of strong independent oversight mechanisms means that these powers could be used in ways that are disproportionate to the legitimate investigative purpose.

8.4 The Data Protection Framework

The Digital Personal Data Protection Act of 2023 is India's first comprehensive law on the protection of personal data.[55]It provides for the rights of individuals over their personal data and places obligations on entities that process such data. However, the Act contains broad exceptions for law enforcement and national security, which means that in practice, the protections it offers may not be available in the very situations where they are most needed, namely when the state is investigating a person or prosecuting them.

The interplay between the data protection law and the evidence laws has not yet been fully examined. It is possible that information obtained by investigators in violation of the data protection law could still be admissible in court under the evidence laws, which do not have an

[51] Ritesh Sinha v. State of U.P., (2019) 8 SCC 1
[52] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
[53] National Investigation Agency Act, 2008, No. 34 of 2008, Acts of Parliament (India), s. 17.
[54] Prevention of Money-Laundering Act, 2002, No. 15 of 2003, Acts of Parliament (India).
[55] Personal Data Protection Bill, 2019 (lapsed); Digital Personal Data Protection Act, 2023, No. 22 of 2023.

exclusionary rule equivalent to the Fourth Amendment exclusionary rule in the United States.[56] This is a significant gap in the protection of the rights of accused persons.

9. Challenges in Practice

The legal position relating to digital evidence has developed significantly in recent years and the new laws of 2023 represent a genuine step forward. But law reform on paper does not automatically translate into better practice. There are several challenges in the actual implementation of the legal framework that deserve attention.

9.1 Capacity of the Police

The first and perhaps the most significant challenge is the capacity of the police to handle digital evidence properly. India has approximately three million police personnel, and the vast majority of them have had no training in digital forensics. When a cybercrime is reported or when a crime involves digital evidence, the investigating officer is often a person who has little or no knowledge of how to handle electronic devices, how to extract data without corrupting it, or how to document the process properly.[57]

The Ministry of Home Affairs has set up the Indian Cyber Crime Coordination Centre, known as I4C, to coordinate the response to cybercrime and to provide training and support to state police forces. The National Cyber Crime Reporting Portal has made it easier for citizens to report cyber offences.[58] However, the number of trained cybercrime investigators remains a small fraction of the total investigative force. Rural and semi-urban police stations, which handle the large majority of crimes in India, are particularly poorly equipped.

9.2 Capacity of the Courts

Judges, too, are not always familiar with the technical aspects of digital evidence. When a case involves complex forensic analysis of data, a judge who does not understand the technology has to rely entirely on what the experts say, without being able to evaluate whether the expert's methodology was sound. This creates a risk that courts will either accept unreliable digital evidence because it seems impressive or reject reliable digital evidence because they do not understand it.

[56] R. v. Kastigar, 406 U.S. 441 (1972) — cited for comparison of standards of proof in digital context.

[57] NASSCOM Report on Cyber Crime in India, 2022, National Association of Software and Service Companies.

[58] National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India, available at https://cybercrime.gov.in (last visited May 2025).

The National Judicial Academy and various state judicial academies have begun to include modules on digital evidence and cyber law in their training programmes. However, the pace of change in technology means that any training quickly becomes outdated. A judge who was trained on the state of digital forensics five years ago may not have the knowledge to evaluate evidence involving cloud computing, encryption, or artificial intelligence-generated content today.[59]

9.3 The Problem of Delay

Criminal trials in India are notoriously slow. The addition of digital evidence to a trial often makes it slower. Forensic reports take time to produce, expert witnesses need to be summoned and they are often unavailable for long periods, and the technical complexity of digital evidence can lead to prolonged arguments about admissibility. In a system that already has millions of pending cases, this additional delay is a serious problem.[60]

The Bharatiya Nagarik Suraksha Sanhita has introduced provisions for the use of video conferencing in trial proceedings, which can reduce delays in some cases.[61] The new law also provides for electronic filing of documents and records, which can help in managing the volume of digital material in large cases. These are useful steps but they do not address the underlying problem of the shortage of forensic examiners.

9.4 Technological Change Outpacing the Law

One major difficulty is that technological developments occur faster than legal reform. The three new laws were drafted with the current state of technology in mind, but technology does not stand still. Artificial intelligence is increasingly being used to generate realistic images, video, and audio that are indistinguishable from genuine recordings. The use of deepfakes as fabricated evidence in criminal matters is not yet a problem in India in a widespread sense, but it is not far off. The law does not currently have a framework for dealing with AI-generated fake evidence and this is a gap that will need to be addressed sooner rather than later.

Encrypted communications present another challenge. End-to-end encryption means that even if an investigator obtains the messages of a suspect from a service provider, they may not be able to read them. Attempts to require technology companies to build backdoors into their

[59] Report of the Expert Committee on Non-Personal Data Governance Framework, Ministry of Electronics and Information Technology, Government of India, 2020.
[60] Rakesh Kumar Paul v. State of Assam, (2017) 15 SCC 67.
[61] State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.

encryption have been resisted by the companies on the grounds that doing so would undermine the security of all users. This issue reflects the continuing debate between privacy and national security concerns.[62]

9.5 Socioeconomic Disparities

There is also the question of access to justice in the context of digital evidence. A wealthy accused person can hire private digital forensic experts to challenge the prosecution's evidence. A poor accused person, who may be represented by a legal aid lawyer with no expertise in digital forensics, cannot do the same. This creates an inequality in the ability to contest digital evidence that runs counter to the principle of equality before the law. The legal aid system in India is not currently equipped to provide specialist digital forensic assistance to accused persons who cannot afford it.[63]

10. Suggestions and the Way Forward

The review of the law and practice of digital evidence in India reveals both progress and persistent gaps. The following suggestions are offered as a way forward, drawing on the analysis in the preceding chapters.

10.1 Detailed Rules on Search and Seizure of Digital Devices

The Bharatiya Nagarik Suraksha Sanhita has made a start by requiring documentation of seized electronic material, but this is not enough. The Central Government should use its rule-making powers under the new Code to issue detailed rules about the search and seizure of electronic devices. These rules should cover the equipment to be used, the procedure for creating forensic images, the documentation required for chain of custody, and the conditions under which a device may be examined before it is formally seized. The rules may also take guidance from internationally accepted forensic practices.

10.2 Mandatory Digital Forensics Training for Police

A programme of mandatory basic training in digital forensics should be introduced for all investigating officers in India, not just those assigned to cybercrime units. The training should cover the basics of how digital evidence works, how to identify and protect potential sources

[62] Cybersecurity Framework, National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India, 2023.

[63] Standing Committee on Information Technology, Report on Cyber Crime, Prevention, Detection and Management, Lok Sabha, 2021-22

of digital evidence at a crime scene, when to call in specialist help, and how to document the process. Advanced training should be available to a larger number of specialised officers who handle cases with significant digital evidence components. This training must be updated regularly to keep pace with technology.

10.3 Expansion of Forensic Laboratory Capacity

The capacity of government forensic laboratories to examine digital evidence must be expanded significantly. This will require investment in equipment, software, and personnel. It may also require a new model for the delivery of forensic services, such as public-private partnerships where private laboratories work under government oversight, or centralised fast-track forensic units for serious cases. The certification framework for private forensic examiners should also be developed so that their reports can be given appropriate weight in court.

10.4 A Digital Evidence Code

A separate framework dealing specifically with digital evidence may help investigators and courts or detailed regulations that set out the complete framework for digital evidence, from collection to production in court. Such a code would bring together the various provisions that are currently scattered across different laws and rules. It would provide a single reference point for investigators, prosecutors, defence lawyers, and judges. Several countries, including the United Kingdom and Australia, have developed detailed guidance documents or codes of practice for digital evidence, and India could draw on these as a model.

10.5 Judicial Training and Expert Assessors

Regular training programmes on digital evidence would help judges handle technical issues more effectively. In cases involving highly technical digital evidence, courts should have the option of appointing a court expert or assessor who can explain the technical aspects to the judge in accessible terms and who is subject to cross-examination by both parties. This model is used in some common law countries and it helps prevent miscarriages of justice that can result from misunderstanding of technical evidence.

10.6 Addressing the Privacy-Evidence Tension

The tension between the right to privacy and the needs of criminal investigation must be addressed more directly in the law. Parliament should consider whether the existing provisions

for search and seizure of electronic devices are adequately proportionate in light of the Puttaswamy judgment. Specific provisions should be introduced requiring judicial authorisation before the contents of a seized device are examined, at least in cases where the examination will involve private communications or sensitive personal data. An independent oversight body for surveillance and interception orders should also be considered.

10.7 Providing for AI-Generated Evidence

Given the rapid development of AI-generated content, the law should proactively address the question of how courts should approach digital evidence that may have been generated or manipulated by artificial intelligence. This could include a presumption that digital evidence is genuine unless challenged, combined with a clear right of the accused to request forensic examination of digital evidence to check for signs of AI manipulation, with costs to be borne by the state in cases where the accused cannot afford it.

11. CONCLUSION

The law relating to digital evidence in India has evolved rapidly due to technological developments. For the first two decades of this century, India tried to make do with a Victorian evidence law and an early internet-era technology law. Courts attempted to interpret the existing legal provisions according to changing technological realities and the Supreme Court in particular showed considerable creativity in filling the gaps. But creativity in interpretation is not a substitute for clear legislation, and the accumulating uncertainty around the Section 65B certificate was a sign that reform was needed.

The three new criminal laws of 2023 have brought about that reform. The Bharatiya Sakshya Adhiniyam has given digital evidence a more secure and clearly defined place in the evidence framework. The Bharatiya Nagarik Suraksha Sanhita has updated the procedural rules for the collection of digital evidence. Together, these laws provide a foundation that is more suited to the digital age than what came before.

Yet, as this paper has argued, Although the reforms are important, effective implementation is still necessary. Much remains to be done. The capacity of the investigative machinery needs to be built up. The forensic laboratories need more resources. The courts need training. The rules under the new laws need to be drafted carefully and with input from practitioners and technical experts. The privacy implications of digital investigation need to be taken seriously and addressed in the framework.

At the same time, the use of digital evidence must remain consistent with constitutional protections Every person who stands accused in a court of law is entitled to a fair trial. That right does not become less important because the evidence against them is digital. The state's power to investigate and prosecute must be balanced against the individual's right to privacy, the right against self-incrimination, and the right to test the evidence against them. Maintaining a balance between investigation powers and individual rights will remain an important issue for Indian courts.

The 2023 reforms are an important development, but their success will depend largely on practical implementation.

12. Bibliography

A. Primary Sources

Statutes

Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament (India).

Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, Acts of Parliament (India).

Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Acts of Parliament (India).

Indian Evidence Act, 1872, No. 1 of 1872, Acts of Parliament (India).

Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament (India).

Information Technology (Amendment) Act, 2008, No. 10 of 2009, Acts of Parliament (India).

Code of Criminal Procedure, 1973, No. 2 of 1974, Acts of Parliament (India).

National Investigation Agency Act, 2008, No. 34 of 2008, Acts of Parliament (India).

Prevention of Money-Laundering Act, 2002, No. 15 of 2003, Acts of Parliament (India).

Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India).

Cases

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

Dharambir v. CBI, (2008) 2 SCC 569.

Jagdish v. State of Rajasthan, 2023 SCC Online Raj 2981.

Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

K. Ramajayam @ Appu v. Inspector of Police, (2016) 11 SCC 73.

Navjot Sandhu @ Afsan Guru v. State (NCT of Delhi), (2005) 11 SCC 600.

Nilesh Dinkar Paradkar v. State of Maharashtra, (2011) 13 SCC 613.

P. Yuvaprakash v. State, 2023 SCC Online Mad 6431.

Rakesh Kumar Paul v. State of Assam, (2017) 15 SCC 67.

Ram Singh v. Col. Ram Singh, 1985 Supp SCC 611.

Ritesh Sinha v. State of U.P., (2019) 8 SCC 1.

Sanjay Singh v. State of U.P., 2022 SCC Online All 1067.

Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.

State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.

Syed Mohammed Abdul Qadir v. State of Karnataka, 2023 SCC Online Kar 39.

Tomaso Bruno v. State of U.P., (2015) 7 SCC 178.

Tukaram S. Dighole v. Manikrao Shivaji Kokate, (2010) 4 SCC 329.

Vikram Singh v. State of Punjab, (2010) 3 SCC 56.

Virendra Khanna v. State of Karnataka, 2021 SCC Online Kar 9853.

B. Secondary Sources

Reports and Official Documents

Law Commission of India, Report No. 269, Review of the Indian Evidence Act, 1872 (2017).

Ministry of Home Affairs, Standard Operating Procedure for Cyber Crime Investigation, Government of India, 2021.

National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India.

Report of the Expert Committee on Non-Personal Data Governance Framework, Ministry of Electronics and Information Technology, Government of India, 2020.

Standing Committee on Information Technology, Report on Cyber Crime, Prevention, Detection and Management, Lok Sabha, 2021-22.

NASSCOM Report on Cyber Crime in India, 2022.

INTERPOL, Guidelines for Digital Forensics Laboratories, 2019.

Cybersecurity Framework, National Critical Information Infrastructure Protection Centre, Government of India, 2023.