VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ELECTRONIC EVIDENCE UNDER CRIMINAL LAW: DOCTRINAL FOUNDATIONS

- Naiya J Patel[1]

Abstract

Digital technology has changed the situation in terms of the law of evidence fundamentally, requiring a thorough re-evaluation of traditional doctrinal principles. The paper discusses the legal bases of electronic evidence within Indian criminal law including the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). It examines the way in which Sections 56-64 of the BSA redefine the concept of primary evidence, admissibility and certification of computer-generated records, and traces the judicial history of Navjot Sandhu to Anvar P.V. to Arjun Panditrao that brought about the present certificate-based admissibility regime in fact. The paper evaluates critically the compulsory forensic obligation in Section 176(3) BNSS, and finds a structural compliance gap in which the procedural compliance to the standards of cloud evidence does not meet the requirements. It also questions the four pillars of authenticity, integrity, attribution, and reliability of the standard doctrines in that excessive reliance on certification is likely to drive evidence law towards bureaucratic formalism. The paper concludes that the statutory framework in place though highly modernized, needs to be supplemented with additional guidelines and interpretive flexibility in order to offer solutions to the evidentiary complexities which come about as a result of distributed cloud infrastructure, attribution across multiple devices, and records produced by AI.

Keywords: *Electronic Evidence, BSA 2023, Section 63, Certificate, Cloud Evidence, Digital Forensics, Attribution, Admissibility.*

1.1 INTRODUCTION

Electronic evidence needs a different approach to traditional documentary evidence[2]. Digital

[1]Student at Unitedworld School of Law, Karnavati University, Gandhinagar

[2] Stephen Mason and Daniel Seng (eds), *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies 2017) 1.

records have no physical form (photographs, chat messages, server logs etc.) as opposed to physical documents[3]. They are generated, distributed and archived automatically and in a systemic way without human intervention. This renders them vulnerable to editing, biasing editing and deletion of context[4]. Digital records can also reside simultaneously on a number of systems, and this is a challenge to old concepts of singular possession and custodianship.

The key issue with evidence law here thus does not concern whether or not a digital recording can be accepted in a court but when a court can consider a digital recording to be credible. Courts should make a distinction of relevance, admissibility, authenticity, integrity, attribution and weight[5]. The chat message may be relevant and inadmissible[6]. An image of the screen can be presented in court but is not a sure method of establishing authorship. A server log might appear to be objective but it can cast doubts on who created it and under what supervision and whether the contents of the log are exhaustive[7].

The law of evidence in India has been slowly shifting towards a digital reality form other than an analogue system. The repeal of Indian Evidence Act, 1872 (IEA) was very much triggered by the judiciary in the case of State (NCT of Delhi) v. Navjot Sandhu, Anvar P.V. v. P.K Basheer, Arjun Panditrao Khotkarv. Kailash Kushanrao Gorantyal.

1.2 THE CONCEPT OF A DOCUMENT IN THE DIGITAL AGE

The BSA describes the way of processing digital documents. Section 2(1)(d)[8] refers to a document as any issue articulated, reported or documented on any material in any way including, by name, electronic and digital recordings. It is not merely a cosmetic issue, but it establishes that electronic records are not a distinct and suspicious category, but they are subject to the general law of proof, and that there are special rules governing the proving of the contents[9].

[3] Bharatiya SakshyaAdhiniyam 2023 (India), s 57.

[4] Mason and Seng (n 17) 45.

[5] Bharatiya SakshyaAdhiniyam 2023 (India), ss 62–63;

[6] Bharatiya SakshyaAdhiniyam 2023 (India), s 62.

[7] Mason and Seng (n 17) 55.

[8] Bharatiya SakshyaAdhiniyam 2023 (India), s 2(1)(d).

[9] Bharatiya Sakshya Adhiniyam 2023 (India), ss 57, 62–63

The concept of documentary evidence is also changing with the rise in levels of data. Electronic records today are capable of storing more than visible data, a message or image, metadata, like the date of creation, a history of modifications, the identity of the sender, routing information, a fingerprint of the device, and its location. The metadata can be more conclusive than content[10]. In a conspiracy case, such as, the fact that a message was sent out by one device using a specific account at a specific time of time might be more significant than the words of the message[11]. In the case of digital forgery, a PDF's visible content may appear genuine, but the properties embedded in the file indicate that the file was created after the time that it claims to have been created.

These reverses had the effect of creating the concept of evidence, when there are multiple copies of a document which are identical the concept of one original is meaningless. Information stored in a remote server where the information is not owned and/or held becomes a problem. What is brought before the court is never the live system that created it, but is always an output; a printout, a screenshot, an exported file or a forensic disk copy. Therefore, the statute differentiates between the acknowledgment of digital documents on the one hand, and the way of proving the contents of the documents on the other[12]. BSA section 57 and section 63 provide such a distinction a structural form.

1.3 STATUTORY FRAMEWORK UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

The Indian law regarding electronic evidence is found in the main sections 56-64 of the BSA[13]and the Expert Opinion and Presumptions provisions. Section 56 says that the content of a document can be proved in two ways; primary or secondary evidence[14]. Section 57 defines primary evidence to be the document itself and Explanations 4 through 7 introduce important changes for electronic records[15]. Explanation 4 Where an electronic record is

[10] Mason and Seng (n 17) 76.

[11] ibid 77.

[12] Bharatiya Sakshya Adhiniyam 2023 (India), ss 57, 63

[13] Bharatiya Sakshya Adhiniyam 2023 (India), ss 56–64.

[14] Bharatiya Sakshya Adhiniyam 2023 (India), s 56.

[15] Bharatiya SakshyaAdhiniyam 2023 (India), s 57.

created or stored in more than one file, each file is primary evidence[16]. Explanation 5 states that record that is in a proper custody is to be recorded when it becomes primary evidence, except in case there is a cause of dispute[17]. Explanation 6 considers each video that is stored at the same time as primary evidence[18]. According to explanation 7, any automated storage facility, and any temporary storage facility within a computer system, is primary evidence of the record in the storage facility[19].

These interpretations are very important. They forego the old rule that there must be one unique paper copy, and permit many copies to be used as primary evidence in a digital world. It does not imply that all copies are credible however. The number of copies is no longer a matter of interest to the actual investigation, but rather the proper custody, disputes, integrity, and how it was produced[20].

Sections 61, 62 and 63 provide the gate way of the electronic records[21]. Section 61 says that an electronic or digital record cannot be excluded from admissibility because it is electronic[22]. The record, provided in Section 63, is as effective as any other document[23]. Section 62 makes provision to prove the contents of electronic records under Section 63[24]. Section 63 lays down the conditions of admitting computer outputs.

Section 63(1) considers any material in electronic form; printed, stored or recorded in electronic media to be a document provided the conditions of the section are fulfilled[25]. A list of the routine-use conditions is provided in section 63(2)[26] the routine use of the computer in the activity that caused the record; the information in question must have been regularly

[16] Bharatiya SakshyaAdhiniyam 2023 (India), s 57, Explanation 4.

[17] Bharatiya SakshyaAdhiniyam 2023 (India), s 57, Explanation 5.

[18] Bharatiya SakshyaAdhiniyam 2023 (India), s 57, Explanation 6.

[19] Bharatiya SakshyaAdhiniyam 2023 (India), s 57, Explanation 7.

[20] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (Supreme Court of India)

[21] Bharatiya SakshyaAdhiniyam 2023 (India), ss 61–63.

[22] Bharatiya SakshyaAdhiniyam 2023 (India), s 61.

[23] Bharatiya SakshyaAdhiniyam 2023 (India), s 63.

[24] Bharatiya SakshyaAdhiniyam 2023 (India), s 62.

[25] Bharatiya SakshyaAdhiniyam 2023 (India), s 63(1).

[26] Bharatiya SakshyaAdhiniyam 2023 (India), s 63(2).

entered; the computer must have been used normally; the computer output must be a normal result of the input. Section 63(3) is the cloud evidence section: therefore, when the creation, storage or processing of information is done over time using more than one computer, all the computers would be treated as a single computer under this section. This directly deals with the distributed multi-device nature of cloud infrastructure.

Section 63(4) retains the requirement of a certificate[27]. To all electronic records which are presented in evidence a certificate must be included. The certificate specifies the record, how it was created, the devices that were used and deals with the conditions in Section 63(2)[28]. It should be signed by an accountable manager of the device or activities and perhaps the statement of an expert.[29] The BSA formulation is a twin-axis of assurance, operational accountability and technical assurance that is essentially intended to close the epistemic divide between the digital system it has to judge and the court. The certificate is not a mere form, but it is the instrument which enables one to have a working knowledge to translate the working of the system to the statement which the law can act upon.

The BSA framework is not completely permissive and neither is it absolutely exclusionary. It provides electronic documents the legal status of paper records, extends the concept of primary evidence to cover computer-generated records, and mandates a formal procedure to prove computer-generated records[30]. With BSA, the levels of the electronic evidence include recognition, categorization, proof strategy, authentication, expert intervention and judicial appraisal.

1.4 EXPERT OPINION, PRESUMPTIONS, AND PROPER CUSTODY

The entire doctrinal image of electronic evidence transcends Section s 61 to 63[31]. Section 39(1) of the BSA states that expert evidence is relevant if the court needs to form an

[27] Bharatiya SakshyaAdhiniyam 2023 (India), s 63(4).

[28] ibid, s 63(2).

[29] Bharatiya SakshyaAdhiniyam 2023 (India), s 63(4); Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (Supreme Court of India).

[30] Bharatiya SakshyaAdhiniyam 2023 (India), ss 57, 62–63

[31] Bharatiya SakshyaAdhiniyam 2023 (India), ss 61–63.

opinion on scientific matters, artistic matters, handwriting and other specialized matters.[32] Section 39(2) states that in case the court must take into account information sent or stored in a computer or electronic device, the opinion of an electronic evidence examiner, under Section 79A of the I.T act [33] should be admitted as a fact. This is to achieve two things: firstly, in most cases in electronic disputes there will be technical aspects that cannot be resolved by mere judicial inference, and secondly, the admission of evidence and its analysis should be disaggregated. A record can be admissible, however, it might be required to have an expert examine the extraction methods, the reliability of the timestamp, data integrity problems, whether the software acted as intended and whether there has been evidence of interference[34].

The BSA also presupposes the electronic signatures, contracts and secure electronic records under the Sections 85 to 87[35]. These presumptions help to shift the burden of proof in appropriate cases and help to prove authenticity in cases where statutory conditions are met.

1.5 SECTION 176(3) BNSS: THE MANDATORY FORENSIC REQUIREMENT AND ITS CLOUD EVIDENCE GAP

Section 176(3) of the BNSS 2023[36] brings in a provision that assumes great significance for the relation between criminal procedure and the law relating to digital evidence. It gives that where an offence punishable by imprisonment of a period of seven years or above is under investigation, the police station officer should make sure that the forensic evidence is gathered at the crime scene[37]. If required, the officer has to call in the services of a mobile forensic unit[38]. The mandatory obligation of this is achieved by the use of shall, which is not the case with the C.R.P.C [39] which did not have a similar forensic obligation. Its interaction with the cloud evidence admissibility structure of Sections 61 to 63 BSA brings about a structural challenge, which requires specific consideration.

[32] Bharatiya SakshyaAdhiniyam 2023 (India), s 39(1).

[33] Information Technology Act 2000 (India), s 79A.

[34] Bharatiya SakshyaAdhiniyam 2023 (India), s 39(2).

[35] Bharatiya SakshyaAdhiniyam 2023 (India), ss 85–87.

[36] Bharatiya Nagarik Suraksha Sanhita 2023 (India), s 176(3).

[37] ibid.

[38] ibid.

[39] Code of Criminal Procedure 1973 (India) (repealed).

The provision has certain assumptions about a physical crime scene where the forensic collection can be performed[40]. Mobile forensic teams are armed and enabled to retrieve information of physical devices through well-established forensic tools. They do not in general have the capability to create formal preservation requests to clouds, to authenticate a multi-factor cloud account or to generate the server-side exports required to fulfill the Section 63(4) certification requirements[41]. The outcome is a compliance gap in forensics. The investigating authority adheres to the letter of Section 176 (3) by introducing a forensic unit, but the gathering of the unit strengths are less than the evidentiary criterion of the cloud-based evidence[42]. Compliance with procedures formally is not admissible trial evidence.

Section 176(3) has to be amended with some form of sub-ordinate legislation or official guidelines that outline minimum requirements of the evidence of cloud collection. Such guidelines must contain: a procedure of issuing preservation requests as soon as any cloud data of interest has been identified; documentation considerations that will include account, platform, extraction method and time stamp requirements; minimum qualifications of personnel handling cloud evidence[43]; and protocol to issue preservation requests[44]. In the absence of such guidance, Section 176(3) will be a formal requirement and empty in the cloud context. The obligatory forensic stipulation will be periodically obliterated in every situation where the corresponding evidence is stored on the remote server rather than on a device.

1.6 JUDICIAL EVOLUTION OF THE LAW ON ELECTRONIC EVIDENCE

To comprehend the current doctrine, it is necessary to trace the significant cases that resulted in its formation. There was no uniformity in the Indian courts of action, the law evolved in phases of flexibility, formal retraction, practical anxiety and doctrinal consolidation.

[40] Bharatiya Nagarik Suraksha Sanhita 2023 (India), s 176(3);

[41] Bharatiya SakshyaAdhiniyam 2023 (India), s 63(4); Bharatiya Nagarik Suraksha Sanhita 2023 (India), s 176(3).

[42] Ibid.

[43] Bharatiya Nagarik Suraksha Sanhita 2023 (India), s 176(3); Information Technology Act 2000 (India), s 79A.

[44] ibid.

The first of the landmark cases is that of State (NCT of Delhi) v. Navjot Sandhu, 2005[45] Case which arose out of an attack on Parliament. The prosecution used call records and other electronic records. The Supreme Court ruled that the provisions of Section 65B of IEA was not to be strictly adhered to and that electronic records may be established by referring to the provisions of Sections 63 and 65 of IEA which makes reference to secondary evidence. Navjot Sandhu demonstrated the willingness of the Court to admit electronic evidence without having full compliance with legislation[46].

The Court overruled the same in Anvar P.V. v. P.K. Basheer, 2014[47]. It believed that Sections 65A and 65B of the IEA are a special code of admitting electronic records, and that secondary electronic evidence must be in line with Section 65B of the IEA[48]. Thus, Anvar overruled the Navjot Sandhu. The ruling put the burden of the case not on the expediency of the judicial system but on the preeminence of statutes and the certificate was a precondition to the admission of secondary electronic evidence[49]. This is significant since electronic documents are easily compromised, and they should not be left to the loose interpretation[50].

The Supreme Court, in the case of Tomaso Bruno v. State of U.P., 2015[51], concluded that the prosecutors could have drawn an adverse inference in case of the failure to produce the electronic evidence provided the latter was available like the CCTV footage. The ruling reiterated the existence of a requirement by investigators to maintain and submit pertinent electronic evidence[52]. Metadata and account logs, preservation requests and acquisition documents have become part of the responsibility of today's cloud-based world[53].

In Sonu @ Amar v. State of Haryana 2017[54] the Supreme Court held that an objection to

[45] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600 (Supreme Court of India).

[46] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600 (Supreme Court of India).

[47] Anvar PV v PK Basheer (2014) 10 SCC 473 (Supreme Court of India).

[48] Indian Evidence Act 1872 (India), ss 65A–65B (repealed).

[49] Anvar PV v PK Basheer (2014) 10 SCC 473 (Supreme Court of India).

[50] ibid.

[51] Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178 (Supreme Court of India).

[52] ibid.

[53] Mason and Seng (n 17) 130; Bharatiya SakshyaAdhiniyam 2023 (India), s 63.

[54] Sonu @ Amar v State of Haryana (2017) 8 SCC 570 (Supreme Court of India).

missing Section 65B certificate must be raised at the earliest opportunity instead of at the first instance on appeal[55].

As in Shafhi Mohammad v. State of Himachal Pradesh, 2018[56] two-judge bench suggested that the provision of the Section 65B certificates is a formality and could be waived when the party lacks the device[57]. Although this was pragmatic and attractive, it caused doctrinal uncertainty when a statutory requirement was treated as being a discretionary protection. This doubt was resolved in the case of Arjun Panditrao v. Kailash Kushan Rao Goyntyal, 2020. This was overruled by a three-judge bench which affirmed Anvar and declared that a Section 65(4) Certificate is a pre-condition to the admission of secondary electronic evidence[58]. The Court ruled that the certificate is unnecessary when the original electronic record is available; failure to get a certificate by a party despite his best efforts could be corrected by the court either by summons the person in question or the document itself under the right circumstances; and a procedural flaw in the certification might be rectified before the trial is finished under appropriate circumstances[59]. It is a mixture of some degree of doctrinal austerity, and a procedure realism, the governing power in the structure of the BSA.[60]

1.7 AUTHENTICITY, INTEGRITY, ATTRIBUTION, AND RELIABILITY

The doctrines of electronic evidence are based on four basic concepts: authenticity, integrity, attribution and reliability. Authenticity is a question as to whether the record is what it purports to be. In digital cases this means a number of questions: Was the screenshot taken from the device stated? Is this the chat that is being exported by this pertinent account? Were the system generated logs mentioned? Does the email come with a domain and sender path that it says it comes with? Digital facsimiles can be easily forged. Courts, thus, turn to certificates, metadata that is specific to devices, self-extractor-evidence, and, where necessary, expert-evidence about the system and processes[61].

[55]Ibid.

[56]Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801 (Supreme Court of India).

[57] ibid.

[58] ibid.

[59] ibid.

[60] Bharatiya SakshyaAdhiniyam 2023 (India), s 63; Mason and Seng (n 17) 135.

[61] Bharatiya SakshyaAdhiniyam 2023 (India), ss 39(2), 63(4)

Integrity poses the question whether the record has been materially changed since its creation. The risk is not a mere threat of blatant manipulation, but also of covert modifications; automatic modifications to time, thumbnails, video formats, etc. that digital systems can make without ill intent.

Attribution is an inquiry as to who the record can be attributed to legally - a human being, a machine, a bank account or bank. This often is the most difficult inquiry in criminal cases. A message will not demonstrate the writer of this message in an account. The ownership of a tool is not sufficient to prove authorship. An IP address does not specify an actor as a human being. Attribution is thus founded upon circumstantial evidence that is cumulatively built up: the usage patterns of the accounts accessed, the matching of the devices, audit trails, behaviour at the time and the context. This is especially critical with respect to cybercrime and conspiracy cases where attribution forms the biggest legal battleground[62]. Reliability is concerned with the trustworthiness of the record producing system. An automatically generated server log might be highly accurate in the usual running of a business system. A note created digitally to be used in litigation may not be as much so. Section 63 (2)[63] conceptualizes the concept of reliability by the idea of regular use: Was the system used regularly? Did information come into the limelight normally? Was the system functional as it was supposed to be? Were those regular-routine inputs the cause of the output? Regularity of the system is a statutory proxy to reliability.

The four concepts have a relationship. An authentic record can be unreliable as an object of evidence of authorship. It can be attributed to a device but been compromised in an integrity if the extraction is not documented. It could be faithful and false with lack of completeness. Courts ought not to demand of the inquiry one gate but a compilation and stratification of inquiry.

1.8 RELEVANCE, ADMISSIBILITY, WEIGHT, AND FAIRNESS

Common law evidence law draws the distinction between relevance, admissibility and

[62] Bharatiya Nyaya Sanhita 2023 (India)

[63]Ibid. pg.39

weight[64]. Such a difference is essential in the online world. Electronic evidence can be a piece of evidence that is logically related to a fact at issue but cannot be legally used due to statutory provisions of proof being violated[65]. Its weight may be diminished even in case it is admissible by questions on source, authorship, or completeness. This difference is important since digital records have aura of objectivity that could lead to fact-finders over-weighting them in comparison with their factual probative worth.

At each of the three levels, fairness is a factor to be considered. Criminal trials are not an adjudicative process organized around rights to contest and equal standing, criminal trials are not merely mechanisms of retrieving the truth[66]. The accused is entitled to examine, interrogate and put into context electronic evidence[67]. In a situation whereby a voluminous electronic record is created without proper notice or even a chance to look into it, formal admissibility of the evidence can be present with the violation of the right to a fair trial. The law of equity is a two-way street. The fact that a certificate of a third party is not readily available should not be enough to prevent a prosecution where it can be ordered to be produced by the court. Fairness safeguards the accused against surreptitious or unclear digital evidence; it also safeguards the prosecution against omissions due to adherence to procedural inflexibility that is not responsive to the truths of current evidence gathering.

1.9 ELECTRONIC EVIDENCE AND THE BURDEN OF PROOF IN CRIMINAL CASES

The prosecution has to demonstrate beyond reasonable doubt the guilt in the criminal law. Criminal case prosecutor should show that the electronic record is present, legally admissible, authentic, obtained in a lawful manner and together with other pieces of evidence should be sufficient to prove a verdict. High technology can never substitute good legal proof, but tends to increase the weight of evidence proof.

The fact that the burden of proof directly affects the inferences that should be made means that courts should be cautious in the interpretation of electronic evidence. Defendants can challenge the chain of custody, offer countering expert testimony and claim that holes in the

[64] Mason and Seng (n 17) 173.

[65] ibid 174.

[66] Constitution of India 1950, art 21

[67] Constitution of India 1950, art 21; Bharatiya Nagarik Suraksha Sanhita 2023 (India).

record impact the overall weight of the record. An example of this is the case of Sonu where a party that failed to object to the electronic evidence during the initial stages of the proceedings was found to be in the wrong in making an appeal against the objections during the appeal stage[68]. So, the burden and procedure are tightly connected in the cases of digital evidence[69].

1.10 DOCTRINAL LIMITATIONS OF A CERTIFICATE-CENTRIC APPROACH

Although the certificate is the key to access in the admissibility of electronic records in the BSA[70], the excessive focus on certification exposes severe limitations in the doctrine. A certificate is merely a reply to one question - how did this output come about?[71] It does not establish whether the output is complete, whether the author of the communication was the accused; whether the record has been selectively deleted out of a larger record set; whether the content has been altered prior to or subsequent to the exporting of the record; or whether the conversion of the record to a presentable form has destroyed any integrity of the context. All these substantive questions can remain open all together on a certificate which meets the formal requirements of Section 63(4)[72].

The over dependence on certificates is posing a threat of reducing evidence law to a regime of bureaucratic simplification. To the extent that courts permit certificates signed under the rules and procedures governing their form to end inquiry, then they will systematically ignore the larger doctrinal questions of authenticity, attribution, integrity and fairness that relate to whether a digital record can in fact carry the evidential burden that the prosecution is placing on it.

Just as bad is the other mistake, that is, suing without certificate as fatally without the coercive powers of the court to summon the custodian. The biggest quandary of the existing

[68] Sonu @ Amar v State of Haryana (2017) 8 SCC 570 (Supreme Court of India).

[69] Bharatiya SakshyaAdhiniyam 2023 (India), ss 61–63; Sonu @ Amar v State of Haryana (2017) 8 SCC 570 (Supreme Court of India);

[70] Bharatiya SakshyaAdhiniyam 2023 (India), s 63.

[71] Bharatiya SakshyaAdhiniyam 2023 (India), s 63(4)

[72] ibid, s 63(4).

framework is the tension between the statutory rigour and evidential reality. The BSA tries to deal with this via Section 63(3) which acknowledges distributed systems and the impossibility doctrine acknowledged in Arjun Panditrao[73]. The root problem is though that digital evidence is no longer produced as the result of mere linear chains of users, platforms, networks, backups, and processes. A statutory system based on single source computer output will need to be construed to accommodate that complexity. This is the challenge for the following chapters in the particular context of cloud computing, chain of custody, completeness and AI generated evidence.

CONCLUSION

The doctrinal analysis of electronic evidence in the Indian criminal law shows a structure which has been greatly modernised but still lacks structural completeness. The Bharatiya Sakshya Adhiniyam, 2023 is a welcome legislative improvement on its predecessor, rethinking the concept of primary evidence to embrace the idea of digital multiplicity, and introducing a form of certification requirement in Section 63(4). Judicial history since Navjot Sandhu to Anvar P.V. to Arjun Panditrao is an indication of the slow reorientation of the judiciary towards doctrinal uniformity, between statutory rigour and procedural realism.

The framework, however, has tensions inherent in it which cannot be overcome by certification. The certificate is concerned with the provenance of an output but does not say anything about completeness, attribution, selective deletion as well as post extraction tampering. Section 176(3) BNSS requires the mandatory forensic obligation which is procedurally progressive, but which leaves a quantifiable level of compliance gap between the forensic requirement and the evidence present on remote cloud infrastructure as opposed to the evidence being present on physical devices. The four pillars of authenticity, integrity, attribution and reliability require a layered judicial inquiry and not a bureaucratic gate keeping.

Finally, the legislation will have to be changed to a system that does not focus on certificates; instead, it will have to incorporate cloud environment forensics, expert witness organization, and chain of custody strength. The statutory architecture will otherwise be unable to rise above the procedural compliance but substantive insufficiency of a limitation with grave

[73] Bharatiya SakshyaAdhiniyam 2023 (India), s 63(3); Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (Supreme Court of India).

consequences in an age in which digital records are the main battleground of criminal evidence.