



TECHNOLOGY AND CRIMINAL LAW: HASH VALUE MANDATES AND FORENSIC VULNERABILITIES UNDER SECTION 63 OF THE BHARTIYA SAKSHYA ADHINIYAM, 2023

Shaurya Pratap Singh*

ABSTRACT

Every year, more crimes are solved or lost because of just one email, CCTV clip, WhatsApp chat, or recording. But no one ever thinks about how a judge knows that the proof in front of him in court is the same as the one being sent at the time the event happened and not something made later. This is where the Bharatiya Sakshya Adhiniyam's Section 63 comes into action. It was enforced on July 1 2024, and it replaced the Indian Evidence Act, 1872. It is India's new law about how electronic evidence should be used in court, and hash files are the tool used to determine whether it has been changed or if it is the original evidence. This paper tries to explain Section 63 of the Bharatiya Sakshya Adhiniyam. What is a hash value? Why does the law insist on it? Does the whole legal system still have some loopholes that a criminal or a lawyer can use in his or her favour? This journal aims to understand, in a way, how a student prepares for their presentation.

Keywords: Bharatiya Sakshya Adhiniyam 2023, Indian Evidence Act, Section 63, Section 65B, Hash Value.

INTRODUCTION

In today's world, technology has become one of the biggest pieces of evidence in crime cases. Now murder is not just about a person killing someone who is seen by someone; now he will come to the court stand in the witness box and point out the accused. Now it is about location, call details, phone records, deleted WhatsApp chats which will be recovered, CCTV footage of that area or even a fitness tracker which was tracking his body functions. All of these proofs are electronic, and the biggest problem with this electronic evidence is that it can be

*BBA LLB, FIRST YEAR, NATIONAL FORENSIC SCIENCES UNIVERSITY, GANDHINAGAR.

manipulated; it can be edited, copied or faked without any mark or change. A photograph can be morphed, a video can be edited or deepfaked, and an audio can be cut from anywhere in a recording, which is a real fear in the Indian Courts. So a law is required to find a way to deal with the situation before letting a digital file be used in the courtroom as evidence to provide justice to the needy, to find out if the proof is real or if someone has done something wrong with it. For a long period of time, India tried to answer this question using Section 65B of the Indian Evidence Act, 1872. This provision required a certificate but didn't provide the actual proof that a file is altered or not. On July 1 2024, the Indian Evidence Act was replaced by the Bhartiya Sakshya Adhiniyam 2023, and Section 63 of the Bhartiya Sakshya Adhiniyam is the new name of Section 65B of the Indian Evidence Act, with some new additions that it now expects the hash value of the electronic records to be mentioned in the certificate that goes along with the proof.

This journal is to explain the whole system and look into the weak points and forensic vulnerabilities that this hash value mandate has brought along with it. From Section 65B of the Indian Evidence Act to Section 63 of the Bharatiya Sakshya Adhiniyam, Section 65B was added to the Indian Evidence Act, 1872, in the year 2000 when the Information Technology Act came into force because the courts needed a way to deal with computer-generated proofs. In Section 65B, it is said that a computer-generated output will be considered as evidence if it meets certain conditions, and a certificate along with the responsible person had to be produced in the courtroom.

The problem was that in 2014, the Indian Courts were not able to decide how strict the law should be. In the case of *Anvar P.V. v. P.K. Basheer*, the Supreme Court said that the certificate under Section 65B of the Indian Evidence Act is mandatory and the electronic evidence is invalid no matter how genuine it looks. In 2017, a two-judge bench in the case of *Shafhi Mohammed v. State of Himachal Pradesh* relaxed this rule and said that if the party doesn't have control over the device from which the evidence is produced, they cannot be forced to produce the certificate. This created a contradiction in the Supreme Court itself because of having two different views on the same point, and finally, in the year 2020, a Supreme Court three-judge bench settled the matter in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* and once again said the certificate is mandatory, overruling the 2017 rule. The 2020 judgment is still treated as a guiding light for how electronic evidence should be treated, even under the Bhartiya Sakshya Adhiniyam 2023.

When the Parliament sat down to draft the Bhartiya Sakshya Adhiniyam, it was clear that there should be no change to the certificate requirements. But the lawmakers made it stricter. That is why Section 63 of the Bhartiya Sakshya Adhiniyam doesn't only ask for the certificate describing the device and its owner, similar to Section 65B of the Indian Evidence Act; it also expects the hash value to be stated and, in many situations, a second certificate from a technical expert in addition to the certificate from the person producing the record. This process is called dual certification, and it was never a part of the old Section 65B of the Indian Evidence Act.

WHAT IS SECTION 63 OF BHARTIYA SAKSHYA ADHINIYAM 2023?

Its bare act says that the admissibility of electronic records as documents without original production is allowed, outlining conditions for regular usage, handling of multiple devices, and evidentiary certificates.

Detailed Explanation: It says that any information stored, printed or copied from a mobile, computer, server or any other electronic device or communication device can be treated as proof as long as some specific conditions are satisfied. It is important because normally a digital file technically does not have a single physical original as a paper letter does, and the evidence laws ask for the original document. Section 63 of the Bhartiya Sakshya Adhiniyam solves this problem by saying that a properly certified electronic record will be treated as if it were the original.

Section 63 lays down conditions for when this computer output can be trusted, and these conditions are:

- The device must have been used regularly to create, store, or process information for ordinary activities by the person who had lawful control over it at that time.
- The information contained in the electronic record must have been regularly and ordinarily fed into the device during the normal course of those daily or business activities.
- Throughout the material period, the device must have been operating properly. If it was out of order at any point, the defect must not have been something that altered the electronic record or affected the accuracy of its contents.
- The output must exactly reproduce or be derived from the original data that was fed into the device.

Something that made Section 63 of the Bharatiya Sakshya Adhiniyam 2023 more effective than Section 65B of the Indian Evidence Act 1872 is Subsection 4, which states that the certificate must go with the electronic evidence every time it is submitted. This certificate has to identify the record, describe how it was produced, give all the details of the device involved in the incident and confirm that the conditions are satisfied. The certificate should be signed by the owner of the device and also by an expert in the given case. The point that it was signed by an expert in the case is the biggest change in section 65B of the Indian Evidence Act, 1872, done in section 63 of Bhartiya Sakshya Adhiniyam, 2023.

The schedule attached to the Bhartiya Sakshya Adhiniyam, 2023 gives us a proper format of the certificate. It is divided into two parts, which are Part A and Part B, respectively. Part A consists of the details that should be filled by the owner of the device, and Part B consist of details that should be filled by a technical expert, and this is the part where the hash value comes into action.

WHAT IS HASH VALUE?

A hash value is basically a fingerprint of a digital file, just like we humans have a unique fingerprint that is different from others even though we have the same number of fingers; in the same way, a digital file, irrespective of its size, either big or small, has a unique string of letters that can only be generated from it using a hash function. It is also known as a hash algorithm. MD5 and SHA-256 are the two most common functions mentioned in Bhartiya Sakshya Adhiniyam 2023. When you take a screenshot, WhatsApp chat, audio, video, a photograph or call record and run it through the hash function, it generates a set of random-looking strings of numbers or letters, which is used to check whether the proof is right or wrong. If only one letter, number or even a single full stop is added or removed, it shows that the evidence is altered because if a single change is made to the evidence, the hash value will be different from the original. This means if police seize a laptop from someone and calculate its hash value on the same day, and then again calculate its hash value on the day of the hearing in the courtroom, irrespective of how much time has passed between the first day of calculation and the second day of calculation, the hash value will be the same without even a single change of any number, letter or even a full stop; it shows that the proof is not changed in between, and the data of the device can be used as proof in the courtroom.

This is why a hash value is also called a digital fingerprint or electronic fingerprint. Supreme Court, in its latest 2026 landmark judgment in Pune Bar Association v. Union of India, signified the importance of hash value under Section 63 of the Bhartiya Sakshya Adhiniyam 2023.

THE CERTIFICATE REQUIREMENTS

We can understand the certificate properly by analysing the schedule of the Bhartiya Sakshya Adhiniyam 2023 because it gives us a proper format of the certificate and both of its parts.

Part A of the certificate describes the person who is the owner or in charge of the device, or the person who is managing the activities on that particular device that produced the electronic records. The device could be a CCTV camera in someone's house recording a theft or a company's IT server holding emails of all employees of the company, which is relevant to a specific case. This part of the certificate talks about the device, when the record was created and how the device was used.

Part B of the certificate talks about the technical part. Here, a person who is considered to be an expert has to state the hash value of the electronic record and tick which hash value is used to generate it. This part is important to prove that the evidence is not altered and that the evidence shown in the courtroom is the same as what was seized from the event in a technological way.

This requirement of two separate certificates, one about the device and the other about the technical integrity of the data, is called the dual certification system. This dual certification system works as a safety net, but it has also raised questions that reached the Supreme Court about who will be the expert body for Part B of the certificate. Madras High Court, in the case of R v. B (2024), gave the authority to sign a valid Part B certificate only to the Examiners of Electronic Evidence notified under Section 79A of the Information Technology Act, 2000, but this means only a handful of government employees will have the authority to sign a valid Part B certificate, which is very few in number if we compare it to the number of civil and criminal cases that require a hash value certificate.

The Pune Bar Association challenged Section 63(4) of the Bhartiya Sakshya Adhiniyam in front of the Supreme Court, arguing that this placed a heavy burden on regular litigants who cannot always find an expert. In May 2026, a three-judge Supreme Court bench led by the Chief Justice himself upheld that a hash value is the electronic fingerprint of a device, and it

gives courts a dependable way to check whether a file is original or altered. At the same time, the bench also held that not only those notified in Section 79A of the Information Technology Act are able to sign a valid Part B, but other qualified persons can also act as experts. However, it is not yet decided who those qualified persons will be. Case Laws that shape this area: Case laws are the primary reason behind Section 63 of the Bharatiya Sakshya Adhiniyam because most story of electronic evidence in India comes from courtrooms rather than from Parliament, at least until the Bharatiya Sakshya Adhiniyam 2023 came and fixed the statute.

It starts from *Anvar P.V. v. P.K. Basheer* (2014), in which a certificate under section 65B of the Indian Evidence Act, 1872 was mandatory, overruling earlier looser practice where secondary electronic evidence was something let in through oral testimony alone.

Shafhi Mohammed v. State of Himachal Pradesh (2018), where the rules were relaxed for people who genuinely could not get a certificate because they were not the in-charge of the device. This event created confusion because different benches were following different standards.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020): In this case, a three-judge bench restored the mandatory nature of the certificate and also described that if the device is not in the possession of the party, the court has the power to direct the production of the certificate from the in-charge of the device.

Pune Bar Association v. Union of India (2026) is the newest and the most important landmark case for Section 63 of the Bharatiya Sakshya Adhiniyam, 2023; the constitutional validity and the schedule of 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 were directly challenged before the Supreme Court for being arbitrary and difficult to satisfy. The Supreme Court upheld the hash value and the certificate requirement while also opening up who can be an expert as a likely reference point for how Section 63 gets interpreted in the years ahead.

There were also decisions from High Courts, such as one from the Delhi High Court, holding that a plain screenshot without an accompanying Section 63-style certificate cannot be accepted as proof. This shows how strictly our courts are now applying the certificate rule even to everyday digital communication, not just to big corporate data or forensic images of hard disks.

FORENSIC VULNERABILITIES: WHERE SYSTEMS CAN STILL BREAK

This part is the heart of the matter because this particle surrounds most of the journal talk about. Making hash value mandatory sounds like a clean, mathematical solution to a messy human problem of evidence altering. But in practice, the system has some soft spots a clever lawyer can point out.

Hash Value Collision: No hash function is immune to collisions, which means two different files sometimes accidentally generate the same hash value. MD5, which is still allowed in the Bhartiya Sakshya Adhiniyam certificate format, is considered weak by computer scientists today because researchers have already shown ways to create the same hash value of different files using MD5 on purpose. SHA-256 hasn't shown such a problem until now; that is why it is considered stronger, but the fact is that Bhartiya Sakshya Adhiniyam 2023 still allows MD5 to be used for generating hash values. A determined and technologically skilled person can exploit MD5 for himself or herself.

That Hash Value only Prove that the Copy Matches, not that the Original was Genuine:

The hash value of the file only proves that the electronic evidence shown in the courtroom is byte by byte identical to the electronic evidence collected from the place. However, it does not tell whether the electronic evidence collected from the place was right or not; there is a possibility that the electronic evidence is already altered, changed, misplaced, or unlawfully obtained. If someone altered the electronic evidence before its hash value is generated, then it is of no use. **Chain of Custody Gap:** There must be a clear, unbroken record of who handled the device or file, when and why, right from the moment of seizure to the moment its hash value is generated. In India, in smaller police stations and rural courts, the chain of Custody documentation is very weak, delayed or done very casually. If the police seize electronic evidence and put it in the store room of that respective police station for two or three weeks without generating its hash value, in those two or three weeks, if anyone sneaks into the store room, he or she can alter the proof, which cannot be determined because the original hash value was still not generated.

Shortage of Training Experts: The whole idea of part B assumes that a qualified expert is available to generate the hash value correctly and will be able to explain it if cross-examined in court. But India doesn't have enough digital forensics experts to match the number of cases involving cyber fraud, matrimonial disputes, or defamation cases on social media. When the

Supreme Court, in the Pune Bar Association v. Union of India case, notified who can sign Part B of the certificate beyond Section 79A of the Information Technology Act, 2000, it solved the problem of very few experts to some extent, but it also created the problem of who will be a qualified expert because now the expert tag can be claimed by people of different skill sets in the technical field, and it is possible that they would generate a wrong hash value, and a wrong hash value is worse than no hash value because this gives false confidence.

Free and Unregulated Hashing Tools: Many of the guides nowadays available to lawyers suggest downloading some unethical free software like WinMD5 to generate hash values themselves. While these free software tools are not unsafe, our government doesn't have a standard forcing every expert to use open-source, audited and valid software. A person can potentially use a fake or modified version of such hashing tools that always show a match in the hash value.

Deepfake and AI-Generated Content: The Bhartiya Sakshya Adhiniyam's mandate is very good at proving whether electronic evidence is altered or not after it was hashed. But since AI has arrived, individuals can create completely fake images, audio, videos, and voice recordings, and these are software-generated, not taken by any camera or phone or any other electronic device, but still pass the requirements of section 63(4) of the Bhartiya Sakshya Adhiniyam because it only checks for alteration. This is exactly the deepfake anxiety that commentators pointed to as the real reason the Supreme Court took the Pune Bar Association case seriously in 2026, even though the certificate requirement itself looked like a purely technical, almost boring, procedural rule.

Burden Falls Unevenly on Ordinary Litigants: A large company facing a commercial dispute can easily hire a high-tech firm to issue a well-defined Part A and Part B of the certificate, but a small litigant in a small town trying to generate a hash value related to a property or matrimonial dispute may struggle a lot. This was also mentioned in the Pune Bar Association v. Union of India (2026) case; however, the Supreme Court rejected the argument by saying this makes the law unconstitutional.

Multiple Certificate Requirements at Every Stage: Section 63(4) requires the certificate to be submitted at each instance the electronic record is produced for admission. This repeated requirement, while meant to ensure continuous verification, can also become a procedural trap. If a party successfully proves a hash value once at the trial stage but the case goes into appeal,

and the record needs to be referred to again, unclear practice on whether a fresh certificate is again technically required can create delay and confusion, which defence lawyers can use to stall proceedings.

GROUND REALITY: HOW IS THIS PRACTICED IN INDIA

It is one thing to read Section 63 in the bare act and quite another to see how it actually works in the courtroom in a district. In India, many police stations still don't have a dedicated cyber cell with trained staff to understand things like hashing. Investigating officers still prefer traditional eyewitnesses, statements, or physical exhibits rather than digital forensics. This means that in a good number of cases, hash values are either not generated at the time of seizure at all, or are generated much later, which weakens their evidentiary strength even if they are technically present in the certificate.

The infrastructure of courts is also uneven. A commercial court in places like Delhi, Mumbai or Bangalore that is dealing with Intellectual Property rights or banking fraud is likely to settle the case in a very good manner because they are dealing with such cases regularly, but a session court in a small town is not likely to settle the case in the same manner.

There is also the question of cost. Digital forensic labs, whether government-run or private, are not evenly spread across the country. A litigant in a far part of India may have to send a device hundreds of kilometres away to get a hash value certified by someone the court is likely to accept as a genuine expert, adding both time and expense to a case that may already be dragging on for years.

What can be done?

Just talking about the problem in the system is not the right way to solve the problem; we also have to give some suggestions in order to improve the system.

The law should remove all the weak algorithms such as MD5 and should only allow strong algorithms like SHA-256 or something even more advanced for hashing tools to avoid all the errors, and there should not be an optional algorithm for hashing; there should be a mandatory algorithm.

India needs a greater number of trained digital forensics experts spread across the state and should not be concentrated only in metro cities like Delhi, Mumbai or Bangalore, along with a

clarified list to distinguish who will qualify as an expert for Part B of the certificate because the Supreme Court has widened the scope of experts, saying not only those mentioned in Section 79A of the Information Technology Act, 2000. Training programmes should be conducted in smaller towns on how to properly seize a device and immediately generate a hash value after the device is seized in order to avoid any mishap.

Courts and investigating agencies should be encouraged to use government-approved software rather than any software for hashing so that there will be a baseline level of trust. Some kind of low-cost hashing and certification facility should be set up for ordinary litigants attached to district courts themselves, so that access to justice is not decided by who can afford a private forensic firm and who cannot.

We know that a hash value alone cannot catch a deepfake or a file that was altered before it was ever hashed; courts may need to develop separate standards, alongside the hash value requirement, for checking the authenticity of the content itself, especially for AI-generated media, and not just its integrity after the fact.

CONCLUSION

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 is a genuine attempt to bring Indian evidence law into the digital era, and the hash value mandate at its centre is a smart, scientific idea. It gives courts a reliable way to check whether a digital file has been secretly altered, something that was almost impossible to prove under the old law. The Supreme Court's decision in the Pune Bar Association case in 2026 has now placed this system on solid constitutional ground, and rightly called the hash value an electronic fingerprint that deserves the court's trust.

At the same time, no law is perfect the moment it is written, and Section 63 is no exception. The forensic vulnerabilities discussed in this journal, like weak algorithms still being allowed, chain of custody gaps, a shortage of qualified experts, the uneven burden on poor litigants, and the simple fact that a hash value cannot catch a fake that existed before the very first hash was taken, all show that the job of protecting digital evidence in Indian courtrooms is far from finished. A hash value is a strong lock, but like any lock, it has no value if the door is in a weak condition, and right now, several of those doors are in weak condition, from small police stations to under-resourced forensic labs, and still need real strengthening. Fixing these gaps is not just a technical matter for computer scientists; it is a matter of making sure that justice, in

a world increasingly run on data, remains fair for everyone, not just for those who can afford the best digital forensic experts.

REFERENCES

1. Bharatiya Sakshya Adhiniyam 2023, Section 63 and its schedule
2. Indian Evidence Act, 1872, Section 65B
3. Anvar P.V. v. P.K. Basheer case, 2014
4. Shafhi Mohammed v. State of Himachal Pradesh case, 2018
5. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal case, 2020
6. Pune Bar Association v. Union of India
7. Information Technology Act, 2000, Section 79A
8. Dell International Services Private Limited v. Adeel Faroze and others. (Delhi High Court case)