

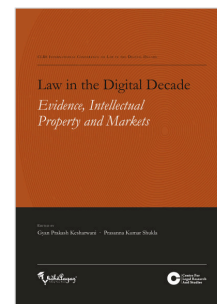
CHAPTER 2

The Certificate Trap: How India's Rule for Electronic Evidence Undermines Cybercrime Prosecutions

Vaishali Verma

in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 15–21

DOI <https://doi.org/10.63108/VAB.LDD.2.2>



CITATIONS

BLUEBOOK (21ST ED.)

Vaishali Verma, *The Certificate Trap: How India's Rule for Electronic Evidence Undermines Cybercrime Prosecutions*, in *LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS* 15 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Vaishali Verma, 'The Certificate Trap: How India's Rule for Electronic Evidence Undermines Cybercrime Prosecutions' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 15.

CHICAGO (17TH ED.)

Verma, Vaishali. "The Certificate Trap: How India's Rule for Electronic Evidence Undermines Cybercrime Prosecutions." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 15–21. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.2.2>.

APA (7TH ED.)

Verma, V. (2026). The certificate trap: How India's rule for electronic evidence undermines cybercrime prosecutions. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 15–21). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.2.2>

SOURCE

<https://doi.org/10.63108/VAB.LDD.2.2>

LICENCE

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

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

CHAPTER 2

The Certificate Trap: How India's Rule for Electronic Evidence Undermines Cybercrime Prosecutions

VAISHALI VERMA*

Cybercrime prosecutions depend on electronic evidence, yet before a court can weigh whether such evidence is convincing, it must decide whether the evidence can be looked at at all. This paper compares how India, the United Kingdom, and the United States answer that threshold question of admissibility, and argues that India has chosen the least workable of the three answers. India treats a signed certificate under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 as an absolute precondition to admitting any electronic record, so that genuine evidence can be excluded over paperwork errors unrelated to its reliability. The United Kingdom abandoned a similar certificate requirement in 1999 in favour of judicial discretion, while the United States treats certification as only one of several optional routes to authentication. Drawing on this comparison, the paper argues that India should convert its certificate from a gatekeeper into a factor courts weigh, and proposes concrete statutory and administrative reforms.

Keywords: Electronic Evidence, Cybercrime, Admissibility, Comparative Criminal Law, Digital Evidence Certification

1 INTRODUCTION

Cybercrime investigations run on digital proof. A hacking case rests on server logs. A phishing case rests on emails. An online fraud case rests on bank transaction records and chat histories. Take away the electronic record, and there is often no case left at all. Cybercrime offences in India, from unauthorised access to identity theft, are themselves defined by reference to computers and communication devices under the Information Technology Act, 2000, so the proof of these offences is almost always electronic by definition.¹ Yet before any court can decide whether such evidence is convincing, it must first decide whether the evidence can be looked at in the first place. This is the law of admissibility, and it sits quietly behind every cybercrime trial, deciding cases long before anyone gets to argue about guilt.

This paper compares how three countries, India, the United Kingdom, and the United States, answer one narrow but consequential question: what must a party show before a court will even look at an electronic record. It argues that India has chosen the least workable of the three answers. India insists on a specific signed certificate before any electronic record can be admitted, and treats the certificate as a condition precedent, meaning that without it, the evidence simply cannot be considered, no matter how obviously genuine it is.² The United Kingdom abandoned an almost identical certificate requirement decades ago and now lets judges assess reliability case by case.³ The United States never had a mandatory

* Research Scholar at Dr. Ram Manohar Lohiya National Law University, Lucknow, Uttar Pradesh, India.

¹ Information Technology Act, 2000.

² Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

³ Youth Justice and Criminal Evidence Act 1999, c. 23, § 60 (UK).

certificate rule; a certificate is available as a shortcut, but it is only one of several ways to get electronic evidence admitted.⁴ This comparison forms part of a broader study of how different legal systems weigh electronic evidence in cybercrime prosecutions, and the certificate question is where the three systems diverge most sharply.

The argument proceeds in six parts. Part 2 explains briefly why electronic evidence needs any special rule at all. Part 3 traces India's certificate requirement from its statutory origin through the Supreme Court's unsettled case law to its current form under the Bharatiya Sakshya Adhiniyam, 2023. Part 4 examines the United Kingdom's move away from certification toward judicial discretion. Part 5 examines the United States' multi-track system of authentication. Part 6 argues that India's all-or-nothing rule, designed to guarantee reliable evidence, has instead become a technical escape route in cybercrime prosecutions, so that genuine evidence gets thrown out over paperwork while prosecutions collapse on procedure rather than merit. Part 7 proposes that India convert the certificate from an absolute gatekeeper into a factor that courts weigh, drawing on the UK and US models, while preserving the certificate's genuine value as a safe harbour.

2 WHY ELECTRONIC EVIDENCE NEEDED A SPECIAL RULE IN THE FIRST PLACE

Paper records are hard to alter without leaving a trace. Electronic records are not. A file can be copied endlessly, edited without a mark, and stripped of the very metadata that would show where it came from or whether it has been touched. Cybercrime evidence is especially fragile in this sense: server logs are routinely overwritten within days, cloud data may sit on machines outside the country investigating the offence, and a single record often passes through several different systems, each capable of altering it, before it ever reaches a courtroom. Courts everywhere have recognised that ordinary rules built for paper do not translate neatly to computer output, and each of the three jurisdictions in this paper responded to that recognition by legislating some threshold check before such evidence reaches the fact-finder. Where they differ sharply is in how strict that threshold check is, and in what happens when it is not perfectly met.

3 INDIA: THE CERTIFICATE AS ABSOLUTE GATEKEEPER

3.1 Section 65B and Its Troubled History

India's rule began with Section 65B of the Indian Evidence Act, 1872, inserted in 2000 alongside the Information Technology Act.⁵ Section 65B(4) required a signed certificate, identifying the electronic record, describing how it was produced, and confirming the conditions of the computer that produced it, before any copy of an electronic record could be treated as proof of its contents.

The Supreme Court's early interpretation of this provision oscillated sharply. In *State (NCT of Delhi) v. Navjot Sandhu*, arising out of the 2001 Parliament attack case, the Court held that electronic records, including mobile telephone call records, could be proved through the ordinary rules on secondary evidence even without a Section 65B certificate.⁶ That relaxed position lasted nearly a decade, and was

⁴ Fed. R. Evid. 902(13)-(14).

⁵ Indian Evidence Act, 1872, § 65B (India) (inserted by Information Technology Act, No. 21 of 2000, § 92 & Sch. II, and repealed by the Bharatiya Sakshya Adhiniyam, No. 47 of 2023, with effect from July 1, 2024).

⁶ *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600, 600-05 (India).

followed as late as 2015 in *Tomaso Bruno v. State of Uttar Pradesh*, without reference to the intervening decision in *Anvar*.⁷ In *Anvar P.V. v. P.K. Basheer*, a three-judge bench held that Section 65B is a complete and exhaustive code for electronic evidence, so the certificate is mandatory and Navjot Sandhu's contrary approach was wrong.⁸ In 2018, a two-judge bench in *Shafhi Mohammad v. State of Himachal Pradesh* tried to soften this again, holding that the certificate requirement could be relaxed where the party seeking to rely on the record was not in control of the device that produced it.⁹

The pendulum finally stopped, at least for now, in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*.¹⁰ A three-judge bench reaffirmed *Anvar* and overruled *Shafhi Mohammad*, holding that the certificate is a condition precedent to admissibility, a requirement that cannot be dispensed with even where a party genuinely cannot obtain it. Tellingly, the facts of the case show exactly how this plays out in practice. Election-related compact discs had been produced without the required certificate, and both the trial court and the High Court found there was substantive compliance through oral evidence given in cross-examination. The Supreme Court held this was not enough: the certificate was indispensable regardless of what the oral evidence otherwise proved. The Court did soften the blow slightly by holding that a party can apply to the court for a direction compelling production of the certificate where the person or authority who should sign it refuses or fails to respond, and that the certificate could still be supplied at a later stage of the trial.¹¹ But the core rule survived intact: no certificate, no admission, whatever else the record might show.

3.2 The Certificate Gets Harder: Section 63 of the BSA, 2023

India replaced the Evidence Act with the *Bharatiya Sakshya Adhiniyam*, 2023, effective from 1 July 2024.¹² Section 63 is the direct successor to Section 65B and largely re-enacts the same scheme, but it goes further still. Section 63(4), read with the Schedule to the Adhiniyam, now requires a two-part certificate: Part A, filled in by the person in charge of the device, and Part B, filled in by an independent expert, disclosing the hash value of the record.¹³ Where Section 65B needed one signature, Section 63 needs two, from two different people, one of whom must be a forensic expert.

This change did not go unchallenged. The Pune Bar Association petitioned the Supreme Court, arguing that Section 63(4) imposes undue hardship on ordinary litigants by requiring a hash-value disclosure and an expert's signature as a precondition to admissibility, and that this made the provision arbitrary and unconstitutional.¹⁴ In 2026, the Supreme Court upheld the provision, reasoning that the risk of manipulation through artificial intelligence and deepfake technology gave the hash-value and expert-certification requirements a rational connection to the law's purpose.¹⁵ Whatever the merits of that reasoning, the practical result is that India's certificate requirement has become more demanding, not less, even as the comparators examined in this paper moved in the opposite direction.

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

⁸ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, 473-74 (India).

⁹ *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801 (India).

¹⁰ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, 1-4 (India).

¹¹ *Id.* at 4.

¹² *Bharatiya Sakshya Adhiniyam*, No. 47 of 2023, India Code (2023) (India) (brought into force July 1, 2024).

¹³ *Bharatiya Sakshya Adhiniyam*, No. 47 of 2023, § 63(4) & Sch. (India).

¹⁴ *Pune Bar Ass'n v. Union of India*, Writ Petition (S. Ct. India 2026), as discussed in SC Upholds Section 63(4) as Hash Value Requirement Ensures Authenticity of Electronic Evidence, TaxGuru (May 28, 2026), <https://taxguru.in/corporate-law/sc-upholds-section-634hash-requirement-ensures-authenticity-electronic-evidence.html>.

¹⁵ *Id.*

3.3 Why This Bites Especially Hard in Cybercrime Cases

Cybercrime prosecutions are where the certificate requirement causes the most damage, for three structural reasons. First, the person in charge of the relevant computer or communication device is often not a witness the investigating agency controls. It may be a foreign social media platform, a private telecom operator, or a bank's information-technology department, none of whom are eager to travel to an Indian trial court to sign a certificate. Second, cybercrime evidence typically passes through many hands: the victim's device, an internet service provider's server, a forensic laboratory, and the investigating officer, and Section 63(4) now asks for signatures from at least two of them in a specific format, raising the odds that at least one link in the chain is missing or defective. Third, investigating officers, who are usually not lawyers, may misunderstand or omit the certificate at the time of seizure, and by the time the omission is noticed, the original device or log may no longer be available to fix it.

4 THE UNITED KINGDOM: FROM CERTIFICATE TO JUDICIAL DISCRETION

The United Kingdom once had a rule strikingly similar to India's. Section 69 of the Police and Criminal Evidence Act 1984 provided that a statement in a document produced by a computer was inadmissible unless the party could show there were no reasonable grounds to believe the statement was inaccurate because of improper use of the computer, and that the computer was operating properly at the relevant time.¹⁶

Section 69 proved unworkable almost immediately. It produced technical litigation over trivial defects, most famously in *Director of Public Prosecutions v. McKeown*, where a defendant argued that a breathalyser's slow internal clock undermined the reliability of a reading, even though the clock error had nothing to do with the alcohol measurement itself. The House of Lords held that only malfunctions bearing on the accuracy of the document's contents mattered, not any and every defect in the machine.¹⁷ The Law Commission examined the provision and, in a 1997 report, recommended its outright repeal, concluding among other things that the section did not address the real causes of unreliable computer evidence and that parties relying on such evidence were often in no position to satisfy a court about the internal operation of a machine they had not built and did not control.¹⁸ Parliament agreed, and section 60 of the Youth Justice and Criminal Evidence Act 1999 abolished section 69 outright, with no replacement certificate scheme of any kind.¹⁹

Since 1999, computer evidence in the United Kingdom has been governed by an ordinary common law presumption: in the absence of evidence to the contrary, a court presumes that a mechanical or computer system was working properly at the relevant time.²⁰ If the opposing party puts forward some evidence that it may not have been working properly, the burden shifts to the party relying on the record to prove reliability. Any residual hearsay problem is handled through the ordinary hearsay provisions of the Criminal Justice Act 2003 rather than through any electronic-evidence-specific certificate.²¹ The result

¹⁶ Police and Criminal Evidence Act 1984, c. 60, § 69 (UK) (repealed 1999).

¹⁷ *Dir. of Pub. Prosecutions v. McKeown*, [1997] 1 W.L.R. 295 (H.L.) (appeal taken from Eng.).

¹⁸ Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics*, Law Com. No. 245, Cm. 3670 (1997) (UK).

¹⁹ Youth Justice and Criminal Evidence Act 1999, c. 23, § 60 (UK).

²⁰ Crown Prosecution Service, *Legal Guidance: Computer Records Evidence* (UK) (setting out the common law presumption of proper functioning following the repeal of section 69).

²¹ Criminal Justice Act 2003, c. 44, §§ 127, 129 (UK).

is that a genuine, reliable printout or log is not excluded merely because nobody signed a particular form. The record is treated like any other piece of evidence, admissible unless there is a real, evidenced reason to doubt it.

5 THE UNITED STATES: MANY ROADS TO AUTHENTICATION

The United States never adopted a certificate requirement at all. Federal Rule of Evidence 901(a) states the baseline: a proponent need only produce evidence sufficient to support a finding that the item is what it is claimed to be.²² That standard can be met by live testimony from someone with knowledge, by the distinctive characteristics of the record itself, by expert comparison, or by several other means the rule expressly lists as illustrative rather than exhaustive.²³

In 2017, the Federal Rules of Evidence were amended to add Rules 902(13) and 902(14), which allow electronic evidence to be self-authenticating, meaning admitted without live testimony, where a qualified person certifies that the record was generated by a reliable process, or that a copy was made using a verified method such as matching hash values.²⁴ Crucially, this certificate is optional. It is a convenience that spares a party the expense of calling a witness when authenticity is not seriously disputed, not a precondition without which the evidence cannot be admitted at all.²⁵ A party can always fall back on the ordinary, testimony-based routes under Rule 901 if no certificate is available.

The leading judicial explanation of how this plays out is *Lorraine v. Markel American Insurance Co.*, where a federal magistrate judge set out, in detail, the full menu of ways a party can authenticate electronically stored information, stressing that counsel must be prepared to use whichever route the facts of the case actually support.²⁶ The flexibility of the American approach does not mean anything goes. Courts still exclude evidence when no adequate authentication is offered by any route. In *United States v. Vayner*, a printout of a social media profile page was excluded because the prosecution offered no evidence, beyond the page itself containing the defendant's name and photograph, that the defendant had created or controlled it, and the Second Circuit held that a reasonable juror could not find the page was what the government claimed.²⁷ The American system, in other words, filters out weak evidence through a searching, fact-specific inquiry into actual reliability, rather than through a single missing signature on a form.

6 WHY INDIA'S MODEL IS THE LEAST WORKABLE OF THE THREE

The comparison exposes what is really wrong with India's approach: it conflates a genuinely useful evidentiary safeguard with an inflexible, form-driven precondition. All three countries want the same thing: assurance that an electronic record actually is what it claims to be. The United Kingdom and the United States pursue that assurance through open-ended inquiries into actual reliability, a presumption that can be rebutted by real evidence in the former, and a menu of authentication routes tested against the facts in the latter. India instead asks a single, narrow, procedural question, namely whether a specific certificate,

²² Fed. R. Evid. 901(a).

²³ Fed. R. Evid. 901(b).

²⁴ Fed. R. Evid. 902(13)-(14).

²⁵ Fed. R. Evid. 902(13)-(14) advisory committee's note to 2017 amendment.

²⁶ *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 538, 545-46 (D. Md. 2007).

²⁷ *United States v. Vayner*, 769 F.3d 125, 131-33 (2d Cir. 2014).

now in two parts, was properly executed, and makes the answer to that question dispositive, regardless of what other proof of reliability exists.

This produces exactly the outcome the Arjun Panditrao facts illustrate: a court can be entirely satisfied, from oral testimony given under cross-examination, that a record is genuine, and still be required to exclude it because a signature is missing.²⁸ In a cybercrime case, the record excluded this way is not a hypothetical. It might be the only chat log connecting an accused to a phishing scheme, or the only server log showing unauthorised access to a hospital's patient database. When that evidence is thrown out for a certification defect that has nothing to do with whether the log is genuine, the prosecution does not just lose a piece of evidence; it often loses the case, because electronic evidence is frequently all that exists in a cybercrime matter. The result is what this paper's title calls the certificate trap: a rule meant to keep out unreliable evidence ends up keeping out reliable evidence too, simply because reliability was demonstrated the wrong way.

The 2026 decision in *Pune Bar Association v. Union of India* forecloses a constitutional fix, since the Supreme Court has now held the two-signature version of the requirement to be a rational, permissible response to the risks of digital manipulation.²⁹ That may well be correct as a matter of constitutional law. Deepfakes and artificially generated media are real and growing threats to the authenticity of digital records, and a legislature is entitled to respond to them. But the fact that a rule survives a rationality challenge does not mean it is good policy. The United Kingdom and the United States show that it is possible to guard against manipulated evidence without making a single missing form fatal to an otherwise strong case. Reform, if it is to come, will have to come from Parliament rather than from the courts.

7 A WORKABLE PATH FORWARD

India does not need to give up on certification altogether. Hash values and expert sign-off are genuinely useful tools, especially given the real risk of manipulated digital media. What India should give up is treating the certificate as the only door into the courtroom. Three changes would bring India closer to the more workable models examined above, without abandoning the safeguards Parliament clearly still wants.

First, Section 63 should be amended so that the certificate operates as one recognised, convenient route to admission, as it does under Rules 902(13) and 902(14) in the United States, rather than as the exclusive route. Where a party can otherwise satisfy the court that a record is genuine, through witness testimony, forensic comparison, or independent corroboration, the absence of a certificate should go to weight, not admissibility.

Second, India could adopt something like the United Kingdom's rebuttable presumption for records generated by systems not reasonably in dispute, such as routine server logs and standard telecom call records, while reserving a stricter certification requirement for cases where the opposing party raises a genuine, evidenced objection to reliability. This would target the safeguard at cases that actually need it, instead of applying it uniformly regardless of whether anyone disputes the record's authenticity.

Third, the court-ordered production remedy recognised in Arjun Panditrao, currently limited to compelling an unwilling custodian to produce a certificate, should be broadened into a general judicial power

²⁸ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, 3-4 (India).

²⁹ Pune Bar Association v. Union of India, Writ Petition (Civil) No. 599 of 2026.

to accept alternative proof of authenticity, such as expert testimony on metadata or hash verification performed after the fact, whenever a certificate cannot reasonably be obtained, whether because a foreign platform will not cooperate or a custodian has died or disappeared. Investigating agencies should also be given clear, simple standard operating procedures, so that the two-part certificate is completed at the point of seizure rather than reconstructed, often unsuccessfully, months later at trial.

None of this requires India to copy the United Kingdom or the United States wholesale. It requires only that India stop treating a paperwork requirement as more important than the truth it was designed to protect.

8 CONCLUSION

Electronic evidence now decides most cybercrime cases before a single witness is cross-examined on the merits, because admissibility is judged first. India's certificate rule, tightened rather than loosened by the *Bharatiya Sakshya Adhiniyam*, 2023, and now upheld against constitutional challenge, continues to treat that certificate as an absolute gatekeeper: no certificate, no case, regardless of what else the record shows. The United Kingdom abandoned an almost identical rule in 1999 because it recognised that the rule did not track actual reliability. The United States never adopted such a rule at all, and instead built a flexible, multi-track system that still manages to exclude genuinely unauthenticated evidence when the facts warrant it. India can keep the parts of its certification scheme that guard against real risks like digital manipulation, while giving up the part that turns a missing signature into an automatic acquittal. Until it does, the certificate trap will keep swallowing genuine evidence, and with it, genuine prosecutions.

* * *