

The Law's Invisible Witnesses: Digital Evidence and the New Inequality of Proof in India

*Rinshu Kumari*¹

ABSTRACT

Every legal system rests on a quiet assumption that a person who has something true to say will, generally, be able to say it in a way the law can hear. This article asks what happens to that assumption when “saying it” increasingly means producing a certified electronic record, and when the capacity to produce one is not evenly spread across a population. India is presently rewriting both halves of its evidentiary story at once. On one side, the Bharatiya Sakshya Adhiniyam, 2023 has replaced the long-litigated Section 65B of the Indian Evidence Act, 1972 with a new statutory framework governing the admissibility of electronic records, while the judiciary itself is being rebuilt as a digital institution through the e-Courts project, video-conferencing, e-filing, and the National Judicial Data Grid. On the other side, India's own telecom regulator and national statistical office continue to record a country whose access to devices, connectivity, and digital skills remains deeply uneven by geography, gender, and generation. This article brings these two stories into the same frame. It argues, through close reading of the law alongside recent official data, that India risks quietly building a two-tier system of proof: one in which litigants who are digitally equipped possess a greater practical capacity to produce legally usable evidence, while those who are not may become evidentially invisible. The article traces why this matters, what is driving it, and what a more equal law of evidence would need to look like.

KEYWORDS

Digital evidence, Bharatiya Sakshya Adhiniyam, electronic evidence, e-Courts, digital divide, access to justice.

¹ Student, Banaras Hindu University, Varanasi, Uttar Pradesh.

INTRODUCTION: WHY THIS QUESTION NEEDS ASKING NOW

The question at the heart of this research emerged from an ordinary encounter with a digital requirement. At an Aadhaar correction centre, people who had travelled considerable distances and waited in long queues were unexpectedly required to produce an appointment letter generated through an online platform. When some were unable to produce it, they were unable to proceed with the documentation process despite having physically reached the centre and otherwise being ready to complete the required formalities. The episode appeared, at first, to be merely an inconvenience created by digitisation. On closer examination, however, it raised a more fundamental question: what happens when access to an institution increasingly depends not merely upon having access to technology, but upon knowing how to navigate it? That question becomes particularly significant when transposed into the legal sphere. If an increasingly digital legal system requires individuals to locate, preserve, retrieve, authenticate, and present information in digitally usable forms, does the ability to do so become an additional condition of effective access to justice? And if that ability is unevenly distributed, can formally equal evidentiary rules produce unequal practical opportunities to prove one's case? There is a comfortable story that Indian policymakers like to tell about technology and justice. It goes roughly like this: courts were slow, paper-bound, and inaccessible; digitisation has made them faster, more transparent, and more accessible; therefore, digitisation is unambiguously good for access to justice. This polished perception is highly plausible because every part of the story is defensible on its own terms. Digitisation genuinely has reduced some delays, has made cause lists and case status visible to litigants who would otherwise have had to travel to a court to learn them, and has allowed undertrial prisoners to be produced before a magistrate by video link rather than in a police van. None of this is being denied here.

What this article resists is the second, quieter half of the story, the assumption that because digitisation is good for the system, it must also be good, or at least neutral, for every person who has to pass through that system. That assumption deserves scrutiny precisely because Indian evidence law has, since 1 July 2024, operated under a new statutory framework for electronic records. The Bharatiya Sakshya Adhiniyam, 2023 ('BSA') contains specific provisions governing the admissibility of electronic records, including a certificate-based mechanism under Section 63.² This is not a small procedural footnote. In a country where digital communications, recordings, photographs, transaction logs, and other electronic records

² Bharatiya Sakshya Adhiniyam, 2023, §§ 61–63.

increasingly form part of everyday disputes, the ability to preserve, obtain, authenticate, and present such material may influence whether an underlying fact can be proved at all. The question this article asks, then, is simple to state and uncomfortable to answer. Who in today's India can actually meet the new evidentiary requirements, and who cannot. not because their story is false, but because of where they live, what they own, or what they have been taught to do with a phone. Answering that question requires reading two very different kinds of government documents side by side: the law itself, and the practical numbers that describe the country the law is meant to serve. This article therefore reads the BSA and the jurisprudence surrounding electronic evidence alongside recent data from the Telecom Regulatory Authority of India ('TRAI'), the Ministry of Statistics and Programme Implementation ('MoSPI'), and the government's reporting on the e-Courts project.³

None of these sources was written specifically with the problem of evidentiary inequality in mind. Read together, however, they reveal a question that conventional discussions of electronic evidence tend to leave in the background. What happens when a formally equal evidentiary rule encounters profoundly unequal digital capabilities? The need for this inquiry is, in one sense, structural where any legal system that changes its rules of proof should ask who can meet the new rules before and not after those rules start deciding outcomes. But the need is also distributive. The people most likely to rely on a single WhatsApp message, recorded call, photograph, or other digital record as important corroborative evidence, may not be the same people who possess the knowledge and resources necessary to preserve and authenticate it properly. If that overlap exists, a rule designed to protect the integrity of evidence may produce an unintended distributional consequence: those who can satisfy the technological requirements of proof may possess a practical advantage over those who cannot.

SETTING THE SCENE: WHAT THE EXISTING SCHOLARSHIP SAYS, AND WHERE IT STOPS

It would be inaccurate to suggest that the relationship between technology, inequality, and law has received no scholarly attention. Scholarship on digital inequality has increasingly moved beyond the simplistic question of whether individuals possess devices or internet connections.

³ TELECOM REGUL. AUTH. OF INDIA, TELECOM SUBSCRIPTION DATA AS ON DEC. 31, 2025 (Feb. 10, 2026); MINISTRY OF STATISTICS & PROGRAMME IMPLEMENTATION, COMPREHENSIVE MODULAR SURVEY: TELECOM, 2025 (NSS 80th Round, Jan.–Mar. 2025); PRESS INFO. BUREAU, MINISTRY OF LAW & JUSTICE, eCourts Project: Key Initiatives and Achievements (Feb. 2026).

Research on India, for example, has demonstrated that Information and Communication Technology (ICT) ownership and use are associated with existing social inequalities, including education, occupation, and caste.⁴ Scholarship on e-justice has similarly examined how the introduction of ICT into India's judicial system affects transparency, governance, efficiency, and access to justice.⁵ The electronic-evidence literature, meanwhile, has largely concentrated on questions of authenticity, admissibility, certification, reliability, and the judicial interpretation of Section 65B of the Indian Evidence Act, 1872 ('IEA'), followed by the new statutory framework under the BSA. These conversations are important. But they largely proceed along separate tracks.

What remains is the question of the ability of an ordinary person not merely to possess a digital device, but to acquire, preserve, authenticate, and successfully use digital information as evidence. The distinction matters because the digital divide is no longer adequately described by asking who has a smartphone or an internet connection. Contemporary digital inequality increasingly concerns what a person is capable of doing with the technology available to them. Research on digital skills has similarly distinguished between access to technology and the skills required to derive meaningful benefits from it.⁶ Two individuals may both own smartphones and use WhatsApp, email, cloud storage, or social-media platforms every day, yet possess radically different abilities to preserve information in a form that can later be relied upon in a legal proceeding. One may know how to preserve original files, identify relevant metadata, retain device information, export conversations, or seek appropriate technical assistance. Another may simply take a screenshot, forward a message, change devices, delete the original conversation, or rely upon a photograph of a screen without appreciating the evidentiary consequences. This distinction is crucial because digital participation does not necessarily translate into digital evidentiary capability. The relevant question is therefore no longer simply: Who has access to digital technology? It is: Who has the knowledge, skills, resources, and assistance necessary to turn digital information into usable evidence?

A. The Acquisition Problem

⁴ Rakesh Kumar et al., Social Inequalities, Fundamental Inequities, and Recurring of the Digital Divide: Insights from India, 61 TECH. SOC'Y 101251 (2020).

⁵ D. Ravindra Satish Babu, e-Justice in India: A Conceptual Framework, 71(2) INDIAN J. PUB. ADMIN. 328 (2025).

⁶ JAN VAN DIJK & ALEXANDER J.A. VAN DEURSEN, DIGITAL SKILLS: UNLOCKING THE INFORMATION SOCIETY (Palgrave Macmillan 2014).

The first inequality may arise even before admissibility is considered. Digital evidence is often transient, platform-dependent, device-dependent, or technically difficult to preserve. A person may encounter a threatening message, receive an important WhatsApp communication, record an incident, possess relevant CCTV footage, or receive an email containing crucial information. Yet possessing that information at one moment does not guarantee that it will remain available, authentic, identifiable, or usable when litigation begins months or years later. The ability to acquire and preserve digital evidence can therefore depend upon technological literacy and access to appropriate tools. This creates an important distinction between having evidence and knowing how to secure evidence. A digitally confident litigant may instinctively preserve relevant material in multiple forms and seek technical assistance when necessary. A less digitally capable litigant may unknowingly destroy, alter, lose, or improperly preserve the same material. The resulting disadvantage is not necessarily caused by the absence of technology. It may arise from an unequal capacity to use technology effectively.

B. The Bharatiya Sakshya Adhiniyam as the Legal Framework

This problem acquires particular significance under India's present evidentiary framework, the BSA. The BSA recognises electronic and digital records within the law of evidence and lays down requirements concerning their admissibility and authentication. Section 63 specifically addresses the admissibility of electronic records and permits certain computer outputs to be treated as documents where the statutory conditions are satisfied.⁷ The statutory framework also includes a certificate mechanism. The Schedule to the BSA contains a certificate divided into Part A, to be completed by the party, and Part B, to be completed by the expert, and requires details concerning the electronic record and device or source, together with the relevant hash value and accompanying hash report.⁸ The purpose of this article, however, is not to undertake a comprehensive doctrinal analysis of Section 63 or to argue that its safeguards are unnecessary. Questions of authenticity, integrity, and reliability are indispensable when dealing with digital material that can be easily copied, altered, or manipulated.

Rather, the BSA provides the legal setting in which the digital divide may acquire an evidentiary consequence. The critical question becomes whether every litigant has a reasonably equal practical capacity to satisfy the requirements imposed upon digital evidence. If the answer is no, then technological inequality may influence not merely how people

⁷ *Supra* note 2, § 63.

⁸ *Supra* note 2, sched., §§ 63(4)(c), 63(5).

communicate, work, or access public services, but also what evidence they are capable of placing before a court. The question, therefore, is no longer simply who has digital evidence. It is who is capable of making digital evidence usable? And, ultimately what happens to those who are not?

C. The Gap This Article Fills

The existing literature therefore gives us important pieces of the problem, but they have not been sufficiently connected. Scholarship on the digital divide tells us that access to technology does not automatically produce equal technological capability. Scholarship on electronic evidence explains the legal requirements governing the use of digital material in court. Scholarship on e-justice examines the digital transformation of courts and its implications for access to justice.⁹ What remains insufficiently examined is the intersection between them. The central inquiry of this article is consequently not whether India has entered a digital age. It plainly has. The more difficult question is whether India's transition to digital evidence has created a new layer of inequality between those who are capable of acquiring and preserving digital evidence and those who are not. The problem can be expressed simply:

Digital access → digital capability → evidentiary capability.

A person may possess the first without possessing the second and may therefore be unable to achieve the third. This article argues that the digital divide should consequently be examined not only as a question of connectivity or technological participation, but also as a question of evidentiary capacity. In an increasingly digital courtroom, the ability to acquire, preserve, understand, and present digital information may itself become a litigation resource. The resulting inequality is subtle. The law may provide the same evidentiary rules to every litigant, yet litigants may enter the evidentiary process with profoundly unequal capacities to use those rules.

MAKING SENSE OF THE PROBLEM: INEQUALITY OF PROOF

To analyse this problem properly, it helps to give it a name of its own. This article uses the phrase 'inequality of proof' to describe a situation in which two litigants may possess equally credible claims yet face unequal practical chances of successfully proving those claims because

⁹ *Supra* note 5, at 328–341; *Supra* note 4.

one possesses a greater capacity to produce legally usable electronic evidence. This is distinct from the older and more familiar idea of inequality of arms. First, it can exist even where representation is equal. A litigant can have a capable legal-aid lawyer and still encounter difficulty because the underlying WhatsApp screenshot, recording, or other electronic record was not preserved in a form capable of satisfying the applicable evidentiary requirements. The problem therefore sits upstream of the lawyer's advocacy, in the litigant's earlier interaction with the technology. Second, it rewards a very specific and unevenly distributed skill, not wealth or education but something closer to digital fluency. Knowing how a record should be preserved, understanding that a screenshot may not be equivalent to preserving the underlying record, recognising the significance of device information or metadata, and knowing when technical assistance may be required. A wealthy but digitally unfamiliar litigant may therefore face difficulties that a poorer but digitally confident litigant may avoid. Third, and perhaps the most important is that the inequality can remain hidden. When a legal-aid case is lost because the litigant had no lawyer, the source of the disadvantage is visible. But when a case is lost because a genuine electronic record could not be properly proved, the judgment may simply record a failure of proof. Part of what this article tries to do is make that invisible category visible.

HOW THIS ARTICLE APPROACHES THE PROBLEM

It is important to distinguish that this is a socio-legal piece and not an empirical one. The article reads the relevant law, principally Section 63 of the BSA, 2023, its predecessor Section 65B of the IEA, 1872 and the Supreme Court's leading decisions on electronic evidence against recent official data concerning connectivity, digital skills, and judicial digitisation. The principal official datasets are TRAI's telecom subscription figures as at 31 December 2025, MoSPI's Comprehensive Modular Survey: Telecom, 2025 ('CMS-T'), and the Government's reporting on the e-Courts project.¹⁰ No dataset currently establishes a direct relationship between an individual litigant's digital capability and the outcome of their case. That absence matters. The argument that follows should therefore be understood as identifying a plausible and evidence-based structural risk, using available proxy data, rather than claiming to demonstrate a precise causal relationship between digital disadvantage and judicial outcomes. That limitation is important. But the absence of perfect data should not prevent the legal system from asking whether its increasingly technical evidentiary requirements are being introduced against a

¹⁰ *Supra* note 3.

background of unequal capacity. Indeed, the absence of such data is itself a reason for further inquiry.

THE CHANGING FACE OF INDIAN EVIDENCE LAW

A. A Brief History, And Why It Matters

To understand why Section 63 BSA matters, it helps to remember what came before it, because the story is really one of law repeatedly trying to catch up with technology. When the IEA was drafted in 1872, its authors could not have imagined a phone that could record, photograph, store, and transmit information almost instantaneously. The law first attempted to respond to electronic records in 2000, when Sections 65A and 65B were inserted into the IEA following the Information Technology Act, 2000 ('IT Act'). Section 65B established a special regime for the admissibility of electronic records produced in the form of computer output.¹¹ The resulting provision generated extensive litigation. In *Anvar PV v. PK Basheer*, the Supreme Court treated the certificate contemplated by Section 65B(4) as a condition for the admissibility of secondary electronic evidence.¹² The decision subsequently generated further questions concerning the scope and operation of the certificate requirement. Those questions were addressed authoritatively by the Constitution Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, which reaffirmed the importance of the certificate requirement while also explaining the circumstances in which the original electronic record could be produced and the certificate requirement could be dealt with by the court.¹³ The significance of this history is not merely doctrinal. It demonstrates that electronic evidence has never been a technologically neutral addition to ordinary documentary proof. The law repeatedly had to construct procedural gateways through which digital material becomes legally cognisable. Section 63 of the BSA continues that architecture, while updating it for a technological environment in which smartphones, cloud systems, communication devices, and other digital sources are central to everyday life.¹⁴ The schedule expressly covers devices and sources including mobile phones, servers, cloud storage, flash drives, DVRs, and other digital sources, while also requiring information relating to the device or source and the hash value of the electronic record.¹⁵

¹¹ Information Technology Act, 2000, § 92, inserting §§ 65A–65B into the Indian Evidence Act, 1872.

¹² *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, ¶¶ 22–24.

¹³ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, ¶¶ 52–61.

¹⁴ *Supra* note 2, § 63.

¹⁵ *Supra* note 2, sched., §§ 63(4)(c), 63(5).

B. A Critical Look at the New Standard

It would be easy, and wrong, to treat this simply as a story of the law becoming stricter for no reason. There is a genuine and serious problem that Section 63 is attempting to address. Digital content can be altered, copied, manipulated, or fabricated. A screenshot can be doctored, a recording can be edited, a digital conversation can be presented without its surrounding context. A court that accepted every electronic representation at face value, without mechanisms for testing authenticity and integrity, would expose the adjudicatory process to a serious risk of manufactured evidence. The insistence upon technical verification is therefore understandable. But it is possible to accept that the goal is legitimate while still asking a harder question about who bears the practical cost of achieving it. A certificate regime, involving technical information, hash values, device details, and expert verification, creates points at which a litigant may require assistance beyond ordinary legal representation. The law may therefore solve one problem, the risk of manipulated evidence, while creating a second, quieter dependency on technological knowledge and technical assistance. The important socio-legal question is not whether authenticity should matter but rather who has a realistic opportunity to satisfy the conditions through which authenticity is demonstrated? That question becomes more pressing where access to technical expertise is geographically and economically uneven. The article therefore argues that authentication and equality must be considered together.

C. The Institution Around the Law: E-Courts

The new evidentiary standard does not operate on its own. It sits inside a judiciary that is itself being rebuilt as a digital institution. According to the Government's February 2026 account of the e-Courts project, more than 637.85 crore pages of court records had been digitised; video-conferencing facilities had been expanded across 3,240 court complexes and 1,272 jails and approximately 1.03 crore cases had been filed through the e-filing platform.¹⁶ These developments represent significant institutional gains. But they also change the stakes of digital inequality. The digital divide is no longer merely a barrier to obtaining or preserving evidence. It can increasingly affect filing, tracking, participation, communication with institutions, and the submission of material to the court. A litigant's position within India's digital divide

¹⁶ MINISTRY OF LAW & JUSTICE, GOV'T OF INDIA, eCourts Project: Key Initiatives and Achievements (Press Info. Bureau Feb. 2026).

therefore touches multiple stages of a case, not merely the moment at which a particular electronic record is tendered.

THE DIVIDE REVEALED BY THE DATA

A. A Country of Two Teledensities

It is tempting to think of India's connectivity story as essentially solved. TRAI's telecom data as of 31 December 2025 recorded more than 1.3 billion telephone subscriptions and an overall teledensity of 91.74 per cent.¹⁷ From this, one might conclude that the technical environment necessary for digital evidence is broadly in place. But after reading the rural-urban figures, however, the picture changes. TRAI recorded urban teledensity of 148.92 per cent against rural teledensity of 59.63 per cent.¹⁸ At the state level, the contrast is still sharper. Delhi recorded a teledensity of 359.50 per cent, while Bihar stood at 61.88 per cent.¹⁹ These figures should not be treated as direct measures of individual digital capability as teledensity measures subscriptions relative to population and can exceed 100 per cent where individuals hold multiple connections. But they are nevertheless significant indicators of unequal connectivity environments. The point is therefore not that a person in Bihar necessarily has less access to technology than a person in Delhi but that the technological infrastructure within which digital legal processes operate is not distributed evenly across space.

B. Ownership is not the same as Ability

A subtler and, for this article's purposes, more important gap emerges once one moves from TRAI's subscription counts, which measure connections rather than individual capability, to MoSPI's household survey, which measures individual usage and selected ICT skills. The CMS-T covered 34,950 households and 1,42,065 persons across India between January and March 2025.²⁰ Consider the specific skill most relevant to the broader argument here: the ability to send a message with an attached file. Among persons aged fifteen years and above, 67.2 per cent of rural men and 50.9 per cent of rural women reported having performed this activity

¹⁷ TELECOM REGUL. AUTH. OF INDIA, TELECOM SUBSCRIPTION DATA AS ON DEC. 31, 2025 (Feb. 10, 2026).

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ MINISTRY OF STATISTICS & PROGRAMME IMPLEMENTATION, COMPREHENSIVE MODULAR SURVEY: TELECOM, 2025, NSS REPORT NO. 593 (NSS 80th Round May 2025).

during the preceding three months. The corresponding figures were 79.1 per cent for urban men and 65.8 per cent for urban women.²¹

Mobile ownership shows a similarly uneven distribution:

INDICATOR	Owns a mobile phone (%)	Used internet, last 3 months (%)	Sent a file attachment, last 3 months (%)
Rural Men	80.7	72.1	67.2
Rural Women	48.4	57.6	50.9
Urban Men	90.0	85.5	79.1
Urban Women	71.8	74.0	65.8

Table: Gender and rural/urban gaps in ownership, internet use, and file-sharing capability.

Source: MoSPI, Comprehensive Modular Survey: Telecom, 2025.²²

²¹ *Id.*

²² *Id.*

The survey does not measure the ability to satisfy Section 63 BSA. Nor does sending a file attachment establish digital evidentiary competence. What it does demonstrate is that even a relatively ordinary digital task is performed at markedly different rates across demographic groups. That makes the assumption of uniform digital capability difficult to sustain. There is also a household-level illusion worth naming here. The CMS-T reported that 85.5 per cent of Indian households possessed at least one smartphone.²³ But household possession does not necessarily translate into equal individual capacity. A device may be shared, controlled by one household member, or unavailable to another member when needed. The distinction between household access and individual control therefore matters greatly when the law assumes that a particular individual can independently retrieve, preserve, transmit, or authenticate a digital record.

C. A Generation Catching Up, and a Generation being Left Behind

There is a genuinely hopeful part of this story too, and it would be unfair to leave it out. Among persons aged fifteen to twenty-nine, 94.3 per cent reported internet use during the three months preceding the CMS-T survey. Mobile phone usage among this age group was approximately 97.1 per cent.²⁴ The generational convergence is encouraging. But it also creates another question. Not every litigant belongs to the youngest and most digitally confident cohort. Property disputes, matrimonial disputes, succession disputes, employment disputes, and other forms of civil litigation can involve older individuals. The point is therefore not that older litigants are incapable of navigating digital systems. It is that age is one of the dimensions along which digital capability varies, and legal institutions should not quietly assume uniformity merely because national youth figures are improving.

WHERE THE LAW AND THE DIVIDE MEET: UNDERSTANDING THE REAL-WORLD IMPACT

Part V talked about the law and VI talked about the ground reality of India. This Part brings them together. It is only in that meeting point that the socio-legal significance of India's evidentiary digitisation becomes visible.

A. The Certificate That May Be Difficult To Obtain

²³ *Id.*

²⁴ *Id.*

Section 63's certification architecture introduces technical requirements that may require assistance beyond ordinary legal advocacy. In metropolitan legal markets, litigants may have comparatively greater access to lawyers, forensic professionals, cyber-law practitioners, and technological services. In less-resourced regions, that access cannot simply be assumed. The data discussed above does not itself establish the geographical distribution of forensic experts. Accordingly, the argument here should not be stated as though TRAI's teledensity figures prove a shortage of certifying experts but the data does establish a broader structural inequality in the technological environment. When that inequality is combined with a legal regime that requires technical information and certification, it raises a serious policy question: Is the technical assistance necessary for producing legally usable electronic evidence equally available to all litigants? At present, India does not appear to collect sufficient nationwide data to answer that question empirically. This is a limitation of the present inquiry but it is also a gap in the evidence base for policymaking.

B. When The Video Link Itself Becomes The Obstacle

Video-conferencing is often presented, rightly, as an access-to-justice success story. It has spared undertrial prisoners, witnesses, lawyers, and litigants significant travel and logistical burdens.²⁵ But video testimony is itself dependent upon digital infrastructure. The Government reports that video-conferencing facilities now extend across 3,240 court complexes and 1,272 jails, with more than 3.93 crore hearings conducted through video conferencing.²⁶ The achievement is substantial. Yet the existence of infrastructure does not eliminate the possibility of uneven experience. A witness connecting from an area with unstable connectivity may encounter interruptions, frozen video, or poor audio at precisely the moment when testimony matters. The resulting risk is subtle. A technological failure may be experienced not as an infrastructure problem but as an apparent problem with the witness's communication.²⁷ This is an example of a recurring phenomenon where technology can solve one access problem while creating another, less visible one. The appropriate response is therefore not to reject video-

²⁵ DEPARTMENT-RELATED PARLIAMENTARY STANDING COMMITTEE ON PERSONNEL, PUBLIC GRIEVANCES, LAW AND JUSTICE, RAJYA SABHA, ONE HUNDRED-THIRD REPORT ON FUNCTIONING OF VIRTUAL COURTS/COURT PROCEEDINGS THROUGH VIDEO CONFERENCING (INTERIM REPORT) (2020), <https://d2r2ijn7njrktv.cloudfront.net/IL/uploads/2020/09/11150617/103-Report-on-Virtual-Courts.pdf>.

²⁶ *Supra* Note 16.

²⁷ Elena Bild et al., Sound and Credibility in the Virtual Court: Low Audio Quality Leads to Less Favorable Evaluations of Witnesses and Lower Weighting of Evidence, 45 LAW & HUM. BEHAV. 481 (2021).

conferencing but to ensure that technological failure is not silently converted into an assessment of credibility.

C. The Litigant Who Cannot File Their Own Evidence

Approximately 1.03 crore cases had been filed through the e-filing platform as of 31 December 2025.²⁸ E-filing is therefore no longer a peripheral administrative convenience. It is an increasingly important gateway into the digital court system. But e-filing presumes a bundle of capacities like device access, internet access, file management, document transmission, authentication, and the ability to navigate a digital interface.

The Government has also reported the existence of e-Sewa Kendras intended to facilitate access to e-Courts services.²⁹ These centres can therefore play an important role in preventing digital exclusion. But facilitation should not become an afterthought. Where a litigant must repeatedly depend on a third party to perform basic digital functions, the system may technically remain accessible while becoming practically dependent. That is precisely the distinction this article seeks to draw.

D. The Cases Where This Matters Most

The population shown by the CMS-T to be less digitally equipped, particularly rural women, should not automatically be equated with victims of domestic violence, harassment, or abuse. Such a conclusion would go beyond the data. The more careful point is that some disputes disproportionately involve digital communications as corroborative material. A threatening message, recorded call, photograph, email, or other electronic record can sometimes provide important corroboration where disputes otherwise depend heavily upon competing accounts. Where a complainant has limited independent digital access or limited knowledge of preserving electronic records, the evidentiary value of such material may be affected by circumstances that have little to do with the truth of the underlying allegation. This is where inequality of proof becomes analytically useful. The concern is one of capacity, not credibility.

CASE CONTEXTS: WHERE THE PROBLEM BECOMES VISIBLE

The argument becomes clearer when placed against actual legal contexts.

²⁸ *Id.*

²⁹ *Id.*

A. Electronic Records And The Certificate Requirement

The trajectory from Anvar to Arjun Panditrao illustrates the legal system's attempt to balance reliability with practical usability. In Anvar, the Supreme Court treated the Section 65B certificate as a mandatory requirement for the admissibility of secondary electronic evidence.³⁰ In Arjun Panditrao, the Constitution Bench reaffirmed the centrality of the certificate while clarifying the statutory scheme and the circumstances in which production of the original electronic record could affect the need for certification.³¹

The doctrinal lesson is important for the present argument. The law is not concerned with the existence of the material but whether the material satisfies the conditions through which it can be treated as legally reliable evidence. That transformation, from digital existence to legal usability, is precisely where unequal digital capability becomes relevant.

Consider a complainant who possesses threatening messages or a recorded communication. The legal question is not merely whether the message existed. Questions of preservation, authenticity, source, production, and admissibility may arise. Where the complainant has limited digital literacy, limited independent access to a device, or no immediate access to technical assistance, the practical process of preserving and presenting that material can become more difficult. The point is not that the BSA makes such evidence impossible to use. It is that the capacity to use it successfully is not necessarily distributed equally. That distinction should form part of any socio-legal assessment of digital evidence.

Digital harassment and non-consensual sharing of intimate material create another setting in which preservation may matter. The Information Technology Act contains offences relating to privacy and publication or transmission of obscene or sexually explicit material, while the Bharatiya Nyaya Sanhita, 2023 ('BNS') contains relevant offences dealing with sexual and related conduct.³² In such cases, digital records may disappear, accounts may be deleted, devices may be replaced, and platforms may alter or restrict access to information. The problem is therefore not simply whether a victim possesses a screenshot. It is whether the victim can preserve sufficient material, identify its source, retain relevant information, and present it in a

³⁰ *Supra* note 12.

³¹ *Supra* note 13.

³² Information Technology Act, No. 21 of 2000, §§ 66E, 67, 67A (India); Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).

manner capable of satisfying the applicable evidentiary framework. Again, the concern is one of capacity, not credibility.

B. Undertrials And Video-Link Hearings

The same paradox appears in the context of video-linked proceedings. The Government's figures show that video-conferencing is now deeply embedded in the judicial infrastructure.³³ This can reduce transportation burdens and facilitate quicker production of undertrials. But if connectivity failures affect the quality of communication, the legal system needs safeguards ensuring that an infrastructural problem does not become a credibility problem. The answer is not to abandon virtual hearings. It is to recognise that digital access is itself part of the conditions under which procedural fairness is experienced.

WHAT WOULD A MORE EQUAL LAW OF EVIDENCE ACTUALLY REQUIRE?

None of the foregoing is an argument for abandoning Section 63's insistence on authenticity. That would simply be like trading one injustice of unequal ability to prove real facts for another of an open door to fabricated evidence. The more honest conclusion is that authenticity and equality both need to be actively engineered into the system, because neither arrives on its own. A few specific steps follow from the analysis above.

A. Turn E-Sewa Kendras Into Genuine Evidence-Support Centres

E-Sewa Kendras should not function only as filing counters. Where legally and technically appropriate, they could be equipped and staffed to assist litigants in preserving electronic records, understanding the certification process, and accessing appropriate technical assistance. Priority could be given to regions where connectivity and court burdens create particularly significant access problems.

B. Build Public Panels of Forensic Certifiers

State Legal Services Authorities could explore publicly accessible panels of qualified technical experts who can assist litigants who cannot privately obtain expert services. The objective

³³ *Supra* note 16.

would be analogous to legal aid's that technical assistance should not become an invisible price of entry into the evidentiary system.

C. Set An Honest Floor For Video Testimony

A minimum connection-quality protocol could be established below which a hearing is adjourned, repeated, or shifted to an alternative mode rather than allowing poor connectivity to affect the perceived reliability of the participant. A poor connection should be treated as an infrastructural failure, not silently read as a witness's unreliability.

D. Start Collecting The Data That Does Not Yet Exist

India currently lacks a dataset that systematically connects litigants' digital capabilities with their mode of evidence submission, technical objections to electronic evidence and eventual case outcomes. Without such data, the relationship proposed in this article will remain partly inferential. The National Judicial Data Grid and associated judicial data systems provide a potential institutional starting point for developing anonymised indicators capable of studying these relationships.

E. Treat Digital Literacy As An Access-To-Justice Measure

Digital literacy should not be treated merely as an economic or educational development objective. As courts increasingly rely on digital participation, the ability to engage with digital systems has become integral to effective participation in legal processes. Accordingly, digital literacy initiatives for groups facing persistent digital disadvantage, including rural women and older persons, should therefore be understood as part of the broader infrastructure of access to justice.

CONCLUSION

None of what this article has argued suggests that India's judiciary was wrong to modernise, or that Parliament was wrong to tighten the rules around electronic evidence. Both changes respond to real and serious problems- a slow, paper-heavy court system on the one hand, and the vulnerability of digital content to manipulation on the other. The argument here is narrower and, it is hoped, harder to dismiss. A legal system cannot responsibly raise the technical bar for being believed without first asking, honestly and with real data, who in the country it serves can actually clear that bar. India's own telecom and statistical data already demonstrate that

digital access and digital capability remain unevenly distributed. The CMS-T, for instance, shows substantial differences between rural and urban populations and between men and women in mobile ownership, internet use, and the ability to perform basic file-sharing tasks. TRAI's figures similarly reveal a pronounced rural-urban difference in teledensity. These figures do not prove that digitally disadvantaged litigants lose cases nor do they establish that Section 63 has already produced a measurable two-tier evidentiary system. What they do is make the assumption of universal digital capability difficult to sustain. That is the central concern of this article. The law may provide formally identical evidentiary rules to every litigant. But formal equality of rules does not necessarily produce substantive equality in the capacity to use those rules. The difference between the two may be where a new form of inequality of proof begins. The question, therefore, is not whether India should have digital evidence. It already does. The question is whether everyone who has a truthful story to tell has a reasonably equal opportunity to turn that story into evidence the law can hear. Until that question is taken seriously, India's newest and most technically sophisticated witnesses may remain its most invisible ones.

