INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITALIZATION OF EVIDENCE AND COURT RECORDS: PROCEDURAL AND EVIDENTIARY CHALLENGES IN THE INDIAN LEGAL SYSTEM

AUTHORED BY - PRAGATI TRIPATHI
Student / Researcher, Amity Law School
Amity University Uttar Pradesh, Lucknow Campus, Uttar Pradesh, India

CO-AUTHOR - DR. AXITA SRIVASTAVA
Assistant Professor, Amity Law School
Amity University Uttar Pradesh, Lucknow Campus, Uttar Pradesh, India

Abstract

Mortgage lending is going through a massive change right now. With technology taking over almost every aspect of our lives, the way people get home loans is also transforming completely. Banks and housing finance companies that once relied on stacks of paper forms, manual verification, and weeks of processing are now turning to algorithms and automated systems. Artificial intelligence decides who gets a loan and at what interest rate. Automated valuation models estimate property prices without anyone ever visiting the site. Blockchain and smart contracts are being tested to speed up conveyancing and reduce fraud. Digital signatures let borrowers close loans from their phones without ever meeting a banker. Sounds great on paper efficiency, lower costs, faster approvals, all that.

But when you look closer, there are real legal problems that nobody seems to be talking about enough. This paper looks at the RBI's Digital Lending Directions, 2025 which came into effect on 8th May 2025 and represent the most comprehensive attempt yet to regulate this space. The Directions ask for strict data localization meaning all borrower data must stay in India and be deleted from foreign servers within 24 hours. They require Lending Service Providers to be tightly regulated with regulated entities remaining fully accountable for their actions. They mandate a cooling-off period of at least one day so borrowers can exit loans without penalty. They prohibit LSPs from collecting fees directly from borrowers. All of this is progressive and necessary.

ISSN: 2582-6433

But questions remain. How do we ensure that AI algorithms used for credit underwriting do not discriminate against certain communities or perpetuate historical biases? What happens when a borrower is denied a loan and the lender cannot explain why because the algorithm's decision is a black box? Who is liable when multiple lenders share a platform and something goes wrong the lead lender, all lenders, or the platform itself? Can global cloud providers like Amazon Web Services or Google Cloud technically comply with India's 24-hour data deletion rule? Are smart contracts even enforceable under the Indian Contract Act, 1872 which was written long before anyone imagined self-executing code? How do blockchain-based property transfers interact with state-level stamp duty and registration laws that vary across the country? These are not small questions. They go to the heart of whether digital transformation in mortgage lending will actually benefit borrowers or simply create new risks and uncertainties. After studying all this in detail and comparing how the United States, United Kingdom, and European Union are handling similar challenges, I argue that if we don't fix these legal gaps digital transformation might end up creating more problems for borrowers than it solves. The technology is moving fast. The law needs to catch up.

Keywords: Digital Lending, Mortgage, Artificial Intelligence, RBI Digital Lending Directions 2025, Algorithmic Bias, Data Localization, Lending Service Providers, Smart Contracts, Consumer Protection, Fair Lending, Automated Valuation Models, Blockchain, Conveyancing.

1. Introduction

Something big is happening in mortgage lending. For the first time in history, we are seeing a real shift from paper files and manual processes to fully digital systems that operate at speeds nobody thought possible even a decade ago. AI algorithms now approve loans in minutes instead of weeks. Automated valuation models estimate property prices using data analytics instead of physical inspections. Blockchain technology is being tested for conveyancing to reduce fraud and eliminate middlemen. Borrowers sign documents from their phones and close loans without ever visiting a bank branch.

All this is happening because lenders are under pressure. Courts are drowning in cases. Borrowers expect instant approvals like they get from other digital services. Competition from fintech companies is forcing traditional banks to modernize or become irrelevant. The numbers tell the story clearly. AI adoption in mortgage lending jumped from 15% in 2023 to 38% in

ISSN: 2582-6433

2024. That is not a slow gradual change. That is a rapid transformation that is reshaping an entire industry.

Then came the RBI's Digital Lending Directions, 2025. This framework completely changed how digital lending operates in India. Before these Directions, the regulatory landscape was fragmented and confusing. Different guidelines applied to different types of lenders. There were the 2022 Guidelines on Digital Lending, the 2023 and 2024 Default Loss Guarantee frameworks, the 2024 Key Facts Statement Circular, and various outsourcing and fair practices circulars going back years. Lenders struggled to keep track. Borrowers had no clear understanding of their rights.

The 2025 Directions changed all that. They consolidate everything into one unified code covering all regulated entities including commercial banks, cooperative banks, NBFCs, housing finance companies, and All-India Financial Institutions. They apply to all digital lending defined as a remote and automated process that leverages digital technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery, and related services. This is comprehensive coverage that leaves little room for regulatory arbitrage.

But here is where it gets complicated. The Directions introduce requirements that are strict and far-reaching. All borrower data must be stored within India. If any data is processed overseas for legitimate reasons, it must be deleted from foreign servers and transferred back to India within 24 hours no exceptions. Lending Service Providers who run the apps and acquire customers cannot collect any fees directly from borrowers all fees must be paid by the regulated entity. Every borrower must get a Key Facts Statement in simple language explaining all loan terms. There is a mandatory cooling-off period of at least one day during which borrowers can exit loans without paying any penalty. All Digital Lending Apps must be reported to the RBI through the Centralised Information Management System with compliance certified by a board-approved chief compliance officer.

Lawyers and lenders are already worried about how this will work in practice. Will global cloud platforms like Amazon Web Services, Microsoft Azure, or Google Cloud be able to guarantee that data is deleted from all their servers within 24 hours? Their infrastructure is complex and distributed across multiple regions. Ensuring deletion within such a tight timeframe may be technically impossible. What happens if data remains on some backup server somewhere does

ISSN: 2582-6433

that mean the lender has violated the law?

In multi-lender arrangements where one platform partners with multiple banks and NBFCs, who is liable when something goes wrong? The Directions say regulated entities remain fully accountable for their LSPs, but if a platform misleads a borrower about loan terms, does every lender on that platform face liability? Does the lead lender bear primary responsibility? Can borrowers sue the platform directly or only the lenders? These questions are not answered clearly.

Then there is the question of smart contracts. The UK government is reviewing how blockchain and smart contracts could speed up property transactions and reduce fall-throughs. Singapore has already given legislative recognition to electronic transactions including smart contracts. In India, we have nothing. Are smart contracts enforceable under the Contract Act, 1872 which requires offer, acceptance, and consideration? Does code constitute valid acceptance? Which court has jurisdiction when a smart contract executes automatically across borders? How do we handle stamp duty on tokenised property transfers when state laws require physical or electronic stamping? The Registration Act, 1908 requires registration of most property transactions, but blockchain records are not legally recognized. These are not small questions.

Automated valuation models raise another set of concerns. In the United States, the Government Accountability Office's September 2025 report warns that AVMs may systematically disadvantage certain communities by producing less accurate valuations where data is sparse. In India, property records are often incomplete. Many transactions are under-reported for stamp duty purposes. Official values may not reflect market reality. An AVM trained on this data may be completely unreliable. Yet lenders are adopting these models because they are faster and cheaper than physical inspections. Who is liable when an AVM undervalues a property and the borrower gets a smaller loan? The lender? The AVM provider? Both?

Algorithmic bias is perhaps the most troubling issue. AI models are trained on historical data. If that data reflects past discrimination think redlined neighborhoods where loans were systematically denied the algorithm learns those patterns. It becomes a tool for perpetuating inequality, not solving it. The black box problem means even the creators of these algorithms sometimes cannot explain why a particular decision was made. When a borrower is denied a loan and asks why, what does the lender say? "The algorithm decided"? That is not an acceptable answer under any fair lending framework.

ISSN: 2582-6433

The EU's AI Act classifies credit scoring algorithms as high-risk systems requiring stringent transparency, documentation, and human oversight. The US CFPB has issued guidance requiring lenders to provide specific explanations for adverse actions regardless of whether the decision was made by algorithm or human. The UK's FCA principles require AI systems to deliver fair outcomes for consumers. In India, the 2025 Directions are silent on algorithmic transparency. They require audit trails but not explanations. They mandate data collection but not disparate impact testing. This is a gap that needs filling.

This paper tries to understand whether these digital reforms actually make sense on the ground or if we are creating new legal problems while trying to solve old inefficiencies. Through detailed analysis of the technological landscape, the regulatory framework, and comparative approaches from other jurisdictions, it identifies where the law needs to catch up with technology. The goal is not to stop innovation but to ensure that as mortgage lending transforms, it does so in a way that protects borrowers, ensures fairness, and maintains trust in the financial system.

2. Objectives of the Study

- To trace how electronic evidence law has evolved in India from the Evidence Act of 1872 to the BSA, 2023.
- To carefully examine Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 and what the dual-certification requirement really means for regular litigants.
- To assess whether our Forensic Science Laboratories have the capacity to handle the increased workload that this new law creates.
- To look at the ground reality of e-filing and digital infrastructure in district courts beyond the big high courts.
- To compare India's digital evidence framework with what the United States, United Kingdom, and Singapore are doing.
- To suggest practical changes that might actually work given our institutional realities.

3. Methodology

This is mostly a doctrinal study which means I spent time reading and analyzing legal texts rather than doing surveys or interviews. The primary materials I relied on include the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the old Indian

ISSN: 2582-6433

Evidence Act, 1872, and relevant constitutional provisions. I also went through important Supreme Court judgments like Anvar, Arjun Panditrao, Navjot Sandhu, Maneka Gandhi, and Puttaswamy because judicial interpretation has shaped this field more than anything else.

For secondary sources, I looked at articles written by legal scholars, reports from various law commissions, and policy documents related to the e-Courts project. To make the analysis richer, I also did a comparative study looking at how four different jurisdictions handle digital evidence. The idea was to see what works elsewhere and whether any of those solutions could work in India.

4. Literature Review

Scholars have been writing about electronic evidence for quite some time now, and the debate has shifted significantly with each major court judgment. Before 2014, there was genuine confusion about whether the certificate under Section 65B of the Evidence Act was mandatory or just one of the ways to prove electronic records. The Parliament Attack case, *State v. Navjot Sandhu* (2005), had created some flexibility by holding that electronic evidence could be led through secondary evidence under Sections 63 and 65 even without compliance with Section 65B. But this view was not consistently followed by courts, and litigants never knew which standard would apply.

Then came *Anvar P.V. v. P.K. Basheer* in 2014. A Constitution Bench of the Supreme Court clearly held that the certificate under Section 65B (4) was mandatory and no other method could be used to admit electronic evidence. The Court ruled that Sections 63 and 65 of the Evidence Act had no application to electronic records, and that the non-obstante clause in Section 65B made it a complete code for admissibility. This judgment settled the law in principle but also created practical difficulties because many litigants and even investigating agencies were either unaware of this requirement or could not produce the certificate on time.
The confusion returned with *Shafhi Mohammad v. State of Himachal Pradesh* in 2018, where a Division Bench held that the requirement of a certificate could be relaxed in the interest of justice, particularly where the party was not in possession of the device. This directly contradicted the larger bench judgment in *Anvar*, and for two years, the law was in a state of uncertainty.

ISSN: 2582-6433

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal in 2020 clarified things finally. A three-judge bench overruled *Shafhi Mohammad* and reaffirmed that the certificate under Section 65B(4) is a condition precedent to admissibility . The Court went further and clarified that the certificate must be obtained at the time the evidence is first presented and cannot be procured later to fill gaps, though it acknowledged that in cases where a party has applied for the certificate and been refused, the court can summon the person to give it . The Court also made an important clarification: if the original electronic device itself is produced in court—like a mobile phone or laptop—and the owner steps into the witness box to prove it, no certificate is needed because that is primary evidence . This made the requirement stricter but also more precise.

With the Bharatiya Sakshya Adhiniyam, 2023, the conversation has moved to Section 63 and what some scholars are calling the dual-certification requirement. Under the new law, the certificate must now be signed not only by the person responsible for the device but also by an expert, and it must include technical details like the hash value of the electronic record. The hash function is essentially a digital fingerprint that ensures the record has not been tampered with. Some scholars argue that this will overwhelm our forensic infrastructure. India has very few digital forensic experts, and our Forensic Science Laboratories are already understaffed and overburdened. Extracting, compiling, and verifying hash values for hundreds of documents in a single case is a monumental task, and outside metropolitan areas, the infrastructure to do this is often limited.

Others point to comparative models like the United States, where Rule 902 of the Federal Rules of Evidence allows self-authentication through hash values and digital signatures, which is much faster and does not depend on human availability. Under Rule 902(13) and (14), data copied from electronic devices can be authenticated by a certification from a qualified person without the need for live testimony, provided the certification explains the process of digital identification used. This shifts the burden to the opposing party to challenge authenticity, rather than requiring the proponent to produce a witness. Some scholars suggest India could learn from this approach, though others worry about the lack of clarity on who qualifies as an "expert" under Section 63 and whether court authorization is needed.

What I noticed while reading this literature is that most scholarship focuses on Supreme Court judgments and what the law should ideally be. There is less writing about what actually happens

ISSN: 2582-6433

in district courts and how lawyers and litigants on the ground are coping with these requirements. How does a small-town litigant, with limited resources, go about finding an expert to certify a hash value? What happens when the police seize a device but do not extract the hash value at the time, and the evidence is later deleted? These are the questions that do not get asked in the law journals. This paper tries to fill that gap a little by connecting the legal framework with the institutional realities that exist outside the high courts. Because the law on paper is one thing, but what matters in the end is whether it works for ordinary people trying to prove their case.

5. The Legal Framework in India

5.1 How It Worked Before 2023

Under the Indian Evidence Act, 1872, electronic evidence was governed by Sections 65A and 65B. The basic idea seemed straightforward enough: if you wanted to admit something that came from a computer—a printout, a CD, a hard drive—you needed a certificate under Section 65B(4) saying that the computer was working properly when the record was created, that it was regularly used in that way, and that nothing had gone wrong with it. The person giving the certificate had to be someone in a position to know these things, usually the person in charge of the computer.

But courts kept fighting over this. In the Parliament Attack case, *State v. Navjot Sandhu* (2005), the Supreme Court suggested that maybe the certificate was not the only way. The Court said that if the original electronic record was not available, secondary evidence could be led under Sections 63 and 65 even without the certificate. This created flexibility, but it also created confusion. Different High Courts took different views, and litigants never knew which standard would apply.

Then came *Anvar P.V. v. P.K. Basheer* in 2014. A Constitution Bench of the Supreme Court looked at the issue and said no, the certificate is mandatory. Sections 63 and 65 have nothing to do with electronic records. Section 65B is a complete code, and its non-obstante clause means it overrides everything else. No certificate, no admission. This settled the law in principle, but it created enormous practical difficulties. Investigating agencies did not know about the requirement. Litigants could not produce the certificate on time. And courts were stuck dismissing evidence that was perfectly reliable simply because of a procedural gap.

ISSN: 2582-6433

The confusion returned briefly with *Shafhi Mohammad v. State of Himachal Pradesh* in 2018, where a Division Bench tried to relax the requirement in the interest of justice. But *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* in 2020 put an end to that. A three-judge bench overruled *Shafhi Mohammad* and reaffirmed that the certificate is a condition precedent. The Court also clarified that the certificate must be obtained when the evidence is first presented, not later to fill gaps. There was one important exception: if the original electronic device itself is produced in court—the mobile phone, the laptop—and the owner steps into the witness box to prove it, no certificate is needed. That is primary evidence, and primary evidence does not need certification.

5.2 What the BSA, 2023 Says Now

The Bharatiya Sakshya Adhiniyam, 2023 makes some significant changes to this framework. Three changes in particular stand out.

First, Section 57 says that electronic records are documents. This might sound like a small thing, but it is actually a huge shift. Under the old law, electronic records were always treated as secondary evidence. You could never produce the electronic record itself; you always had to produce a printout or a copy, and that copy needed a certificate. Now, because an electronic record is a document, it becomes primary evidence. If you have the original file on a phone or a computer, and you bring that device to court, you are bringing primary evidence. No certificate is needed for that.

Second, Section 61 says that courts cannot refuse to admit something just because it is electronic. This is aimed at the old practice where judges would sometimes say, "This is just a printout, it cannot be admitted." That objection is now gone. If something is otherwise admissible, the fact that it exists in electronic form is not a reason to keep it out.

Third, Section 63 deals with the certificate again, but this is where things get complicated. The new provision seems to require two certificates: one from the person in charge of the computer, and another from an expert. The certificate must also include technical details like the hash value of the electronic record, which is essentially a digital fingerprint that ensures the record has not been tampered with.

This is where the real problems start. India has very few digital forensic experts. Our Forensic

ISSN: 2582-6433

Science Laboratories are already understaffed and overburdened. In a single case, there could be hundreds of electronic records—WhatsApp messages, call logs, emails, CCTV footage—and each one needs its hash value extracted, compiled, and verified. Outside the big cities, the infrastructure to do this simply does not exist. Lawyers in small towns have no idea where to find an expert. Litigants with limited resources cannot afford to pay for one.

There is also a deeper question: what happens when the police seize a device but do not extract the hash value at the time? If the device is later returned or tampered with, there is no way to prove what was on it originally. The evidence could be lost forever, not because it is unreliable, but because someone forgot to press the right button.

The intention behind Section 63 is understandable. The law wants to ensure that electronic evidence is authentic and has not been tampered with. But the effect may be to make electronic evidence so difficult to admit that ordinary litigants simply give up. That cannot be what the law intended.

6. Problems with Admissibility and Digital Court Processes

6.1 Why Dual Certification Is So Difficult

Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 says you need certification from the person who manages the computer system and also from an expert. Now think about what this means in practice, away from the law books and in the real world where cases are actually fought.

We already have very few forensic experts in India. This is not speculation; it is a documented fact. Our Forensic Science Laboratories are understaffed and overworked. The vacancies for digital forensic experts have been lying unfilled for years in many states. If every single electronic record now needs two certificates—one from the system administrator and one from an expert—cases will simply sit around waiting for experts to find time in their schedules.

For someone in jail waiting for trial, this could mean many more months, even years, behind bars. Speedy trial is not just a nice idea; it is a constitutional right under Article 21. But when the law creates procedural requirements that cannot be met because the infrastructure does not exist, that right becomes meaningless.

ISSN: 2582-6433

And for poor litigants, the situation is even worse. Paying one expert is expensive enough. Paying two experts, and possibly covering their travel and court appearance costs, might be simply impossible. What happens then? Does their evidence get excluded entirely, even if it is reliable and true? The law does not provide an answer, and the courts will have to figure this out case by case, which is expensive and uncertain for everyone.

6.2 Our Forensic Labs Are Just Not Ready

This is the real crisis that nobody talks about enough in the law journals. Our Forensic Science Laboratories are struggling on multiple fronts, and the new law does nothing to address this.

First, there are not enough people. Across the country, posts for digital forensic experts remain vacant for years. The pay is not competitive with the private sector, and the work is demanding. Young graduates with skills in cybersecurity and digital forensics can make much more money working for corporations than they can in government service. So they do, and the labs are left with empty chairs.

Second, the equipment is old. Technology changes every year, sometimes faster. New devices, new software, new ways of hiding or tampering with data. But our labs do not get updated that often. Budget cycles are slow, procurement is bureaucratic, and by the time new equipment arrives, it is often already outdated.

Third, the workload is overwhelming. As everything goes digital, more and more evidence needs forensic analysis. Every phone, every laptop, every CCTV recording from every case ends up in the labs. The labs cannot keep up. Backlogs stretch for months, sometimes years.
When the law asks for expert certification but there are no experts available to provide it, something has to give. Either cases proceed without the evidence, which means guilty people might walk free, or cases get delayed indefinitely, which means innocent people stay in jail. Neither outcome is acceptable. A law that cannot be implemented fairly is not a good law, no matter how well-intentioned it might be.

6.3 E-Filing Is Still a Struggle in Regular Courts

The e-Courts project has been going on for years, and crores of rupees have been spent on it. But go to any district court in the country, and you will still see the same problems.

ISSN: 2582-6433

Many court complexes have just one or two e-filing kiosks for hundreds of lawyers. If you are not there early, you wait in line. If the kiosk breaks down, you wait until someone comes to fix it, which could be days. The promise of digital convenience evaporates when the infrastructure cannot support the demand.

The internet is slow and keeps disconnecting. Virtual hearings, which became common during the pandemic, are constantly disrupted by connectivity issues. Judges spend valuable time saying "you are frozen" and "can you hear me now" instead of deciding cases. What was supposed to make things faster is actually creating new delays.

Young lawyers and lawyers from rural areas often do not have their own laptops or good internet at home. They depend on cyber cafes or the court kiosks. When those options are limited, they cannot file documents on time. They cannot appear virtually. They are at a disadvantage compared to lawyers from big cities with good equipment and fast connections.
And then there is the human element. Judges, many of whom grew up in a paper world, now have to figure out software while managing their dockets. Clerks who used to file physical papers now have to learn digital systems with minimal training. The transition is messy, and the people caught in the middle are the litigants whose cases get delayed.

Digitalization was supposed to make justice faster and more accessible. In theory, it should. In practice, without the supporting infrastructure, it often just adds another layer of complexity to an already complicated system.

7. CONSTITUTIONAL QUESTIONS: FAIR TRIAL AND DUE PROCESS

Article 21 of the Constitution says that no person shall be deprived of their life or personal liberty except according to procedure established by law. In the famous case of *Maneka Gandhi v. Union of India*, the Supreme Court explained that this procedure cannot be just any procedure. It has to be fair, just, and reasonable. It cannot be arbitrary or oppressive.

When we talk about digital evidence, this principle becomes very important. The rules we create for admitting electronic records are not just technical details. They affect the fairness of the entire trial.

Consider the right to cross-examine. This is a fundamental part of a fair trial. The accused must

ISSN: 2582-6433

be able to challenge the evidence against them. But how do you cross-examine digital evidence? If the prosecution brings in a certificate with technical jargon and complex hash values, and the accused does not have an expert of their own, what can they really ask? "I put it to you that this hash value is wrong" is not a meaningful question if you do not understand what a hash value is. The right to cross-examine becomes formal rather than real.

Then there is the presumption of innocence. The prosecution always has to prove its case beyond reasonable doubt. The accused does not have to prove anything. But if the rules make it too difficult for the accused to show that digital evidence has been tampered with, this balance gets disturbed. Imagine a case where the only evidence is a WhatsApp message. The accused says the message is fake, that someone else sent it from their phone. But to prove that, they would need an expert to examine the phone, extract metadata, and explain the technical details. If they cannot afford that expert, they cannot raise a reasonable doubt. The burden has effectively shifted to them, even though the law says it should not.

Article 20(3) protects against self-incrimination. No person accused of an offence shall be compelled to be a witness against themselves. But when the police take your phone and extract data from it, does that count as compelling you to be a witness against yourself? The phone contains your messages, your photos, your location history. Extracting that data reveals things about you that you might not have chosen to reveal. The courts have not fully answered this question yet, and the new law does not address it.

After the *Puttaswamy* judgment, we also know that privacy is a fundamental right. The Supreme Court held that the right to privacy is protected under Article 21. Digital court records contain all kinds of personal information—financial details, medical records, private communications, intimate photographs. What safeguards do we have to prevent data leaks or misuse? Who can access these records? For how long are they stored? Can they be deleted? The current framework is silent on most of these questions.

All of this matters because the law is not just about winning and losing cases. It is about whether the system treats people fairly. If digital evidence rules make it harder for the accused to defend themselves, or if they create new ways for the state to intrude into private lives without safeguards, then we have to ask whether we are really moving toward justice or away from it.

ISSN: 2582-6433

8. How Other Countries Handle This

When you look at how different countries deal with digital evidence, some interesting patterns emerge. The United States follows the Federal Rules of Evidence, particularly Rule 902, and what is striking about their approach is that they allow electronic evidence to essentially authenticate itself. Instead of relying on human certificates and expert opinions, they use hash values and digital signatures. If a document's hash value matches what it is supposed to be, that is usually enough for the court. This makes things much faster because you are not waiting around for someone to write a certificate.

The United Kingdom takes a different route under the Police and Criminal Evidence Act. Their entire focus is on maintaining proper audit trails from the very moment evidence is seized. They are extremely strict about documenting who handled the evidence, when, and what was done to it. If the audit trail shows any gaps, the evidence becomes suspect. So their emphasis is on process rather than just technical authentication.

Singapore sits somewhere in between. Their Evidence Act provides for a certification process but it is much simpler than what India has introduced. They have managed to balance evidentiary integrity with practical efficiency, which means fewer delays in court proceedings while still ensuring that electronic records are reasonably reliable.

India under the BSA, 2023 Section 63 has chosen a more demanding path. We ask for two certificates one from the person in charge of the computer system and another from an expert. On paper this looks thorough and careful. But the problem is we simply do not have the institutional capacity to support this requirement. Our forensic laboratories are understaffed, our experts are overworked, and there is no streamlined process for routine electronic records. So while other countries have designed systems that work within their institutional realities, India has created a strict framework without building the infrastructure to match. The result is likely to be delays, increased costs for litigants, and frustration all around.

What stands out is that India has chosen one of the strictest approaches but without building the infrastructure to support it. Other countries manage to balance authenticity with practicality. We haven't figured that balance yet.

ISSN: 2582-6433

9. What Needs to Change

The first and most urgent change is to define what an expert actually is, because right now anyone can call themselves one and the law offers no clear guidance on qualifications, which means we need a proper definition with specific credentials and a code of conduct so courts and litigants know who to trust. At the same time, we have to make the process simpler for routine documents like bank statements or phone records from licensed companies, because it makes no sense to treat them the same way as disputed evidence—a simpler process would free up our overburdened forensic labs to focus on cases where evidence is actually contested. And those labs themselves need urgent attention, not just incremental budget increases but a national mission mode project to fix the infrastructure, because if the labs cannot handle the work with enough people and modern equipment, the whole system collapses and people stay in jail waiting for certificates that never come. A national digital evidence registry would help tremendously, where every piece of evidence gets a unique hash value at seizure and courts can check it later to confirm nothing has been tampered with, making the entire process more reliable and reducing the burden on experts. Beyond these immediate fixes, we also need to make rules for artificial intelligence before it becomes a problem, because AI is already being used in courts for translation and research, and we need clear rules about transparency, bias checking, and most importantly, keeping humans in charge so that the final decision always rests with a judge, not an algorithm. And finally, we have to help poor litigants by amending the Legal Services Authorities Act to cover forensic experts under legal aid, because if the other side has money to hire experts and you do not, that is not a fair trial, and all the procedural safeguards in the world mean nothing if only the rich can afford to use them.

10. Conclusion

There is no doubt that Indian courts need to change. The old paper-based system, with its files stacked to the ceiling and its decades-old procedures, simply cannot handle the caseload anymore. Every year, more cases are filed, more evidence is generated, and more people wait for their turn at justice. Digitalization is not just a convenience; it is a necessity. The Bharatiya Sakshya Adhiniyam, 2023 takes an important step in the right direction by treating electronic records as primary evidence, removing the old confusion about whether a printout is admissible, and recognising that in the modern world, the most important records exist not on paper but on screens and servers.

ISSN: 2582-6433

But laws alone do not deliver justice. They are words on paper, and words on paper do not hire experts, do not fix broken equipment, and do not pay for lawyers. If we ask for dual certification without having enough trained experts to provide it, we are not safeguarding evidence; we are creating a bottleneck that will keep cases pending for years. If we push e-filing without fixing the internet connections in district courts, without ensuring that every lawyer has access to a functioning kiosk, without training the clerks and judges who have to use these systems, then digitalization becomes just another hurdle for litigants to cross. If we collect vast amounts of digital evidence without clear privacy safeguards, without rules about who can access it and how long it can be stored, then we are creating new ways for the state to intrude into private lives without the accountability that a democracy requires.

Think about what this means for an ordinary person walking into a district court today. They have heard that things are going digital, that justice will be faster now. But when they get there, they find that the e-filing kiosk is broken, that the internet is too slow to upload their documents, that the court clerk is confused about the new procedures, that the expert they need to certify their evidence charges more than they can afford. They wait months for their case to be heard, and when it finally is, they discover that the electronic evidence they relied on has been excluded because the certificate was not signed properly. This is not justice. This is a system that promises reform but delivers only frustration.

The goal should be a system that is both efficient and fair. Technology can help achieve that goal, but only if we build the institutions to support it. We need forensic laboratories that are adequately staffed and equipped, not just in the big cities but across the country. We need clear standards for who qualifies as an expert, so that litigants know who to turn to and courts know who to trust. We need legal aid that covers forensic assistance, so that poor litigants are not at a disadvantage simply because they cannot afford an expert. We need privacy safeguards that recognise the fundamental right recognised in *Puttaswamy* and ensure that digital court records are protected from misuse. We need rules for artificial intelligence that keep humans in charge and ensure that algorithms do not silently shape judicial outcomes.

None of this is impossible. Other countries have figured out ways to make digital evidence work without overwhelming their forensic labs or excluding litigants who cannot afford experts. The United States allows self-authentication for certain types of electronic records. The United Kingdom has developed protocols for digital disclosure that balance efficiency with

ISSN: 2582-6433

fairness. The European Union has built privacy protections into the fabric of its digital infrastructure. India can learn from these examples, adapt them to our context, and build a system that actually works for the people who need it.

But if we do not do this work, if we pass laws and then walk away without building the institutions to implement them, the gap between what the law promises and what actually happens in courts will keep growing. And in that gap, ordinary people seeking justice will be the ones who suffer. The accused who cannot afford an expert to certify the evidence that would prove their innocence. The plaintiff whose case gets delayed because the e-filing system does not work. The litigant whose private information gets leaked because there are no safeguards. These are not hypotheticals. They are happening now, in courts across the country, every day. The Bharatiya Sakshya Adhiniyam, 2023 is not the end of the journey. It is the beginning. The question is whether we will take the next steps, or whether we will leave people waiting at the starting line while the world moves on.

References

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1
3. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801
4. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600
5. R.K. Dewan & Associates, "Electronic Records Now Governed by Section 63 of the Bhartiya Sakshya Adhiniyam, 2023" (2025)
6. American Bar Association, "New Rules for Self-Authenticating Electronic Evidence" (2018)

Statutes

- Bharatiya Sakshya Adhiniyam, 2023
- Bharatiya Nagarik Suraksha Sanhita, 2023
- Indian Evidence Act, 1872
- Constitution of India, 1950

Cases

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

ISSN: 2582-6433

- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1
- *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600
- *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248
- *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1