EVOLUTION AND LEGAL CHALLENGES IN DIGITAL EVIDENCE AND E-FIR SYSTEMS

Asif Khan*

ABSTRACT

Generally, in this paper, I explore how India's criminal justice system is changing due to new technology development like digital evidence and online police reports (e-FIRs). I will look at how our laws have evolved, from old rules to new laws like the Bharatiya Sakshya Adhiniyam, 2023. Besides this, I will also get into the problems of using complicated digital data in courts, adding strict legal procedures with real-world practice. I will also examine important court decisions, especially the cases of Anvar P.V. v. P.K. Basheer.[1] and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.[2] These cases show how judges are trying to figure it out, the right way to handle digital evidence, like making sure it is real and deciding if it can be used in court, and also knowing when to seek help from experts. I am looking at both digital evidence and e-FIRs to see how we can really use technology to make things faster and more accessible than usual, while still protecting people's privacy and ensuring a fair trial. Besides this, I will also discuss the problems that police face, such as a lack of proper tools, not enough training, and issues with cybersecurity. My paper will conclude with suggestions for the future, such as building better forensic labs, training more people, working with other countries, and creating a more transparent system that serves the public at best. By looking at two real-life case studies, an explanation will also be given on how all of these play out in court. Ultimately, I argue that India needs a legal system that's strong, flexible, and protects people's rights in our rapidly changing, digital world.

Keywords: Digital Evidence, e-FIR, Indian Criminal Justice, Bharatiya Sakshya Adhiniyam 2023, Judicial Interpretation, Privacy Rights, Forensic Challenges.

*BA LLB, THIRD YEAR, JYOTIRMOY SCHOOL OF LAW.

[1] Anvar P.V v P.K Basheer (2014) 10 SCC 473.

[2] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2019) 2 SCC 44.

INTRODUCTION

As our world is rapidly going digital, the legal and justice systems are facing new challenges and opportunities every day. India, undergoing an immense digital shift, is dealing with challenging legal, technological, and procedural changes, especially in handling digital evidence and e-FIRs in criminal investigations. The evolution of digital evidence laws and the use of e-FIRs show how modern law enforcement is trying to adapt to new technology, while protecting justice and civil liberties.

Digital evidence has become an important part of solving and prosecuting crimes in the digital age. From emails and texts to blockchain, records and AI-created content, digital tracks often form the support for modern criminal cases. Moving from traditional paper evidence to electronic records requires big legal reforms to ensure this evidence can be accepted, proven authentic, and kept secure in court.

Similarly, the e-FIR system was introduced to allow victims and witnesses to report certain crimes electronically, making the process more accessible and effective. However, the use of technology in police work brings up key concerns about being fair, keeping private information safe, protecting data, and training police on how to handle digital evidence in order to protect from illegal use.

This journal looks at how Indian laws about digital evidence and e-FIRs have changed. It covers new laws, key court cases, and the practical challenges that judges and police face. Furthermore, it discusses big legal arguments regarding evidence rules, finding a balance between privacy and government needs, the difficulties of law enforcement across different areas, and new electronic threats like deepfakes and encrypted information.

BACKGROUND: THE EVOLVEMENT OF DIGITAL EVIDENCE

Digital evidence is simply information stored digitally that's used in court to prove or disprove a case. The massive increase in our use of devices, the internet, and social media has made this evidence more common and complex than ever. For a long time, Indian law didn't officially recognise electronic records as primary evidence. While the Indian Evidence Act of 1872 was essential, it wasn't built for the digital world. As time passed, Courts and laws started to accept digital evidence, which completely changed how legal cases are handled.

Early on, the Information Technology Act, 2000, recognised digital documents, but it had its limitations. Courts often had to depend upon Section 65 (B) of the Indian Evidence Act, which requires a certificate to permit electronic evidence in the court. This rule caused frequent irritating delays and ongoing legal disputes. To fix these issues, India came up with three new criminal laws in 2023: The Bharatiya Nyaya Sanhita (BNS), The Bharatiya Nagarik Suraksha Sanhita (BNSS), and The Bharatiya Sakshya Adhiniyam (BSA). The BSA plays an important role, because it replaces some parts of the old Evidence Act, making it easier to accept digital evidence, by relaxing certification rules and also strengthening protections against fakes.

DEVELOPMENT OF E-FIR SYSTEM

As laws around evidence change, the e-FIR system is becoming a popular, digital way to report crimes. The goal of e-FIRs is to make things simpler, prevent police from delaying or neglecting cases, and make the whole process more open and fairer. Now, many states have special websites where people can file reports for certain crimes online and get a digital confirmation.

However, though the idea is very great, the e-FIR system has its own tricky legal issues arising. We have to figure out how to confirm that a complaint is real, stop people from misusing the system or filing fake reports, and make sure personal information stays private and confidential. The online platforms themselves also need to be strong enough to withstand cyberattacks. Courts have had to fight with big questions, like whether an e-FIR is just as valid as a traditional paper one and what rights people have when they submit a report online.

LEGISLATIVE REFORMS AND KEY LEGAL PROVISIONS: ANALYTICAL PERSPECTIVES

The laws around the digital evidence and e-FIR systems in India have changed completely with the new Bharatiya Sakshya Adhiniyam (BSA), 2023, and the related Bharatiya Nyaya Sanhita (BNS) and the Bharatiya Nagarik Suraksha Sanhita (BNSS). These new laws show a deliberate, widespread effort to bring old legal rules up to date with modern technology. A closer look at these changes reveals the struggles and compromises that are at the heart of today's evidence laws and investigation procedures.

STRIKING A BALANCE: MAKING DIGITAL EVIDENCE MUCH EASIER TO USE, BUT ALSO SCRUTINIZING IT

One major reason for the new BSA, 2023, is to make it simpler to use electronic evidence in court. This moves us away from the strict and often complicated rules of the old Section 65B of the Indian Evidence Act. Before, the law required very formal certificates for digital records, which often caused big delays in getting justice, and sometimes valued technical rules more than finding the truth. If we look a little closely, then the BSA changes the definition of electronic evidence and relaxes the certification rules. This is a move to align the legal process with our digital world. By focusing on whether the evidence is real and trustworthy instead of just on a formal certificate, the BSA creates a more practical system that could reduce legal costs and delays.

However, with these ease rules, there's a bigger responsibility for judges to carefully and thoroughly check the quality and origin of digital evidence. The job of sorting out fake or tampered with electronic records now falls more on the courts and forensic experts. This means we need to improve how our judges are trained, establish standard forensic procedures, and increase technical expertise in areas that have traditionally been weaker in India's justice system.

E-FIR SYSTEMS: PROCEDURAL INNOVATION VS DUE PROCESS COMPLEXITIES

The new laws supporting e-FIR systems are a big, innovative step toward making crime reporting digital. By letting people file a report from anywhere, at any time, e-FIRs make the initial reporting process more accessible and faster for everyone. However, the real challenge is making sure that the system is fair and doesn't get misused. Unlike a paper FIR filed in person, where police can immediately check who the person is and what happened, e-FIRs have to deal with the challenge of proving that a complaint is real and has not been faked. To tackle this, the new laws have put in place verification rules and only allow e-FIRs for certain, less serious crimes.

But this raises a big question! "If e-FIRs are a genuine way to get legal help for minor crimes, why can't they be used for more serious ones that often require urgent attention?" Limiting them like this might create rigid, old-fashioned rules that may go against the very idea of using technology to make things easier and compatible.

BALANCING PRIVACY AND EVIDENTIARY NECESSITY

In our digital world, digital evidence and the e-FIRs contain a huge amount of personal and sensitive information. With India's new Digital Personal Data Protection Act, 2023, there is a delicate balance to strike; the government needs to investigate crimes, but at the same time, it also has to respect a person's right to privacy.

These new laws have set up rules for how to handle this data. They say the government should only use data for a specific reason and for a limited time, and they must keep electronic records safe. But in practice, there are still conflicts. Law enforcement often wants broad access to our digital lives, but at the same time, this can go against privacy protections. This overreach could even make people afraid to communicate freely online. So, when we look at these new laws, we have to understand that they are a battleground where privacy, transparency, efficiency, and justice are all competing interests. This is where courts come in. They have to act as the final judge, deciding exactly where the line should be drawn for police investigations.

THE PROBLEM WITH SEPARATE RULES: AGENCIES NOT WORKING TOGETHER

Right now, the different rules for collecting digital evidence, running forensic tests, and handling FIRs can cause problems because they don't always line up. Various groups, like cybercrime units, forensic experts, state police, and judges, all follow different procedures and have different skill sets. While our new laws talk a lot about the need for everyone to work together, in reality, there are big gaps. Ultimately, everyone isn't following the same standards across the country. This can mess up the integrity of evidence and make legal processes inconsistent. To fix this, we urgently need to create a single, unified set of rules and training for digital forensics that everyone can follow.

JUDICIAL INTERPRETATION: DOCTRINAL CHALLENGES IN DIGITAL EVIDENCE AND E-FIR REGIMES

The court system's role has always been crucial in deciding how digital evidence can be used and whether e-FIRs are legitimate in India. While new laws create the basic framework, it is the specific court cases and legal precedents that really shape the practical rules and solve the problems that come with the digital age.

JUDICIAL APPROACH TO DIGITAL EVIDENCE ADMISSIBILITY

Courts, including the Supreme Court and High Courts, have historically been very cautious about electronic evidence. They often insisted on strict rules, especially the certificate requirement under the old Section 65 (B) of the Indian Evidence Act. A key case, Anvar P.V. v. P.K. Basheer, where certificate wads were made mandatory, leading to concerns that legal formalities were getting in the way of finding the truth.[3]

Later, another important case came, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, where they eased this rigidity. The Supreme Court said that while the certificate was important, courts could also look at the facts and other evidence to decide if electronic proof was real and reliable.[4] This gave courts more flexibility to evaluate digital evidence based on the situation and not just on a technical rule.

Now, with the new Bharatiya Sakshya Adhiniyam (BSA), 2023, judges have new challenges. This new law is more relaxed about the formal requirements for electronic evidence. Because of this, courts have to develop new legal principles that not only protect the fairness of a trial but also understand the complexities of digital evidence, like checking metadata and cyber forensic audit trails.

CHALLENGES IN JUDICIAL CAPACITY: EXPERT RELIANCE

Now, this is a big concern about whether judges are ready to handle the technical side of digital evidence. Evaluating digital evidence requires a special set of skills, like data hashing, forensic imaging, and properly documenting the chain of custody, that aren't typically part of a judge's training.

Because of this, courts often have to rely heavily upon expert witnesses to explain the evidence. But this creates its own problems. It can lead to heated arguments between opposing experts, making it harder for the judge to figure out the facts. This can sometimes turn into an "expert war," where both sides bring in their own specialists to argue their case. The lack of standard forensic rules and official accreditation can also make it hard to trust these experts' opinions.

[3] Anvar P.V v P.K Basheer (2014) 10 SCC 473.
[4] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2019) 2 SCC 44.

Ultimately, this can make digital evidence feel like a "black box" to the court, something powerful and important, but whose inner workings will be a mystery.[5]

JUDICIAL EVALUATION OF E-FIR LEGITIMACY

When judges deal with e-FIRs, there are some questions that they mostly encounter, about the reports' status, validity, and legal consequences. The courts have consistently allowed people to file reports electronically, but they've also stressed that this doesn't reduce the police's duty to investigate thoroughly.[6] Because e-FIRs are filed digitally, proving a complaint is authentic is a major concern. Courts have had to step in when people file false or misleading reports, which can lead to unnecessary lawsuits or harassment. To stop this misuse, judges will have to actively create and enforce rules always, to verify who is filing a complaint.

ANALYTICAL REFLECTIONS ON JUDICIAL BALANCING ACTS

Courts, when at a critical point, try to balance two opposing ideas, making sure the justice system is accessible and efficient, while also ensuring it's accurate and fair. In other words, it can be said that, on one hand, making the evidence rules more flexible lets us use more digital information, but if judges aren't careful, there's a risk that faulty evidence could lead to an unfair outcome. At the same time, on the other hand, being too strict with what evidence is allowed can prevent legitimate, powerful digital evidence from being considered.

The solution is to have a continuous conversation within the legal system, which should bring together new technology with traditional rules of evidence. Judges need to create standards that are both scientifically sound and realistic about how digital evidence and e-FIRs are actually created and used in the real world.

OPERATIONAL, TECHNOLOGICAL, AND POLICY CHALLENGES IN IMPLEMENTING DIGITAL EVIDENCE AND E-FIR SYSTEMS

The success of India's new laws on digital evidence and e-FIRs really depends on whether police or other agencies can actually put them into practice. Right now, there are many real-world and technical problems stopping these new legal frameworks from being used smoothly

[5] See discussion on expert evidence reliability in digital forensics: S. Sridharan, 'Challenges in Judicial Assessment of Digital Evidence' (2024) 12 Indian Journal of Law and Technology 101.
[6] Anvar P.V v P.K Basheer (2014) 10 SCC 473, High Court judgment on admissibility of e-FIRs.

in everyday criminal investigations. This section will look at these challenges and what they mean for future policy.

Complexity and Volume of Digital Evidence: The amount of data created on digital platforms is growing rapidly, making it a huge and complex pile of digital evidence. This includes everything from social media posts and emails to encrypted messages and files saved in the cloud. It's a real challenge to collect, save, and analyse all this diverse data with our current forensic tools.[7] Police departments often hit roadblocks, trying to figure out what's important within this massive amount of data. This can affect how trustworthy and reliable their investigations are/can be.

Inadequate Forensic Tools and Resource Constraints: Doing digital forensics requires specialised, high-tech tools that can create exact copies of data, recover deleted files, analyse metadata, and decrypt secure files. Unfortunately, many studies have shown that our current forensic labs aren't up to the task. They often have outdated technology or don't have enough funding, especially in smaller states and rural areas.[8] This technological gap directly affects the quality of digital evidence and can make it less likely to be accepted in court.

Expertise and Training Deficiencies: Experts agree that the judges, lawyers, and police officers often don't have enough training in the complex details of digital forensics and handling electronic evidence.[9] This knowledge gap causes problems like evidence being collected incorrectly, poor storage methods, and weaknesses in a case during a trial.

To fix this, several efforts have been made to improve training, but they have often been disorganised and have not been good enough. This makes the risk of mishandling or having evidence thrown out even worse. This shows that there's an urgent need for full, standardised training programs that are updated as technology changes.[10]

Cross-Border Jurisdictional and Legal Complexities: Generally, Cybercrimes don't respect borders, which creates tricky problems with jurisdiction and international teamwork. Indian agencies often have a tough time getting digital data stored on servers in other countries. This

[7] Legal Challenges, Digital Evidence, and New Criminal Laws (IJFMR, 2025) 5-7.
[8] A Singh, 'Digital Evidence Management in India: Technological and Resource Constraints' (2024) Indian Journal of Cyber Law 112.
[9] S Sridharan, 'Challenges in Judicial Assessment of Digital Evidence' (2024) 12 Indian Journal of Law and Technology 101.
[10] 'Capacity Building for Cybercrime Investigation' Ministry of Home Affairs Report (2024).

is just because treaties meant to help with the Mutual Legal Assistance Treaties (MLATs) are slow, and different countries have different rules about protecting data.[11] The fact that global cyber laws aren't all the same is what makes it difficult to maintain a clean chain of evidence and can lead to long delays in bringing people to court. This, in turn, weakens the effect of punishments.

Privacy Concerns and Data Protection: Handling digital evidence means dealing with a lot of personal and sensitive information. Because of this, it has to follow privacy laws like India's new Digital Personal Data Protection Act, 2023. There's a constant struggle to balance the need to get evidence quickly and efficiently with the need to collect only the data necessary and keep it confidential. If digital evidence is mishandled or if the investigators overstep their boundaries, it could violate a person's basic rights. This is why strict oversight and clear legal protections are so important.[12]

Technical Vulnerabilities and Cyber Threats: The digital world is so sensitive in Nature that it can be tampered with, infected with malware, deepfakes, and easily encrypted, which makes it hard to trust digital evidence. Things like "anti-forensic" techniques, where people intentionally hide or delete data, can create serious challenges for investigators and judges trying to find the truth.[13] To deal with these threats, we need to constantly update our technology and use specialised investigation methods.

e-FIR System Challenges: While e-FIRs make things more accessible, in this situation, they can come up with their own set of procedural and technical problems. Verifying who is filing a complaint from a distance creates the risk of false or pointless reports, which wastes both police resources and court time.[14] However, there is another fact, and that is, different states use different rules for e-FIRs, and this is what creates confusion and can also make the public lose faith in the system. Making sure that the e-FIR websites have strong cybersecurity is absolutely necessary to prevent hacking, data breaches, and attacks that could shut down the portals.[15]

[11] Jurisdictional Issues in Cybercrime' (iPleaders, 2024) <https://blog.ipleaders.in/all-about-digital-evidence> accessed 3 September 2025.
[12] Digital Personal Data Protection Act, 2023 (India).
[13] R Kumar, 'Anti-forensic Techniques and Challenges' (2024) Journal of Digital Forensics 48.
[14] 'Challenges and Legal Issues in e-FIR Registration' (Law Journals.org, 2025) 29.
[15] Merit Y, 'Guidelines for Securing e-FIR Portals' (2023).

Policy Implications: To overcome these challenges, we will need a multi-pronged approach:

- We need to fund modern forensic tools and create a single, nationwide standard for how digital evidence is handled.
- We have to create official training programs for police, judges, and prosecutors so they know how to properly handle digital evidence.
- We need to make it easier to work with other countries to quickly share data and investigate cybercrimes that cross borders.
- We have to find a better balance between protecting people's data and the needs of the justice system, making sure everything is done with transparency and accountability.
- We should build a single, secure, nationwide e-FIR system with consistent rules and a way to quickly verify reports.

EMERGING TECHNOLOGICAL TRENDS AND FUTURE-PROOFING DIGITAL EVIDENCE SYSTEMS

Overcoming all these challenges requires a smart and well-thought-out plan, and in my reference, the steps are:

Firstly, we need to invest a huge amount of money in modern forensic technology all over the country. This means giving our labs, police, and cybercrime units the best tools to get, analyse, and save digital evidence. At the same time, we have to create a single, nationwide standard for handling digital evidence. By having a single set of consistent rules, from the crime scene to the courtroom, we can actually fix the current problem where things are getting messy and don't match up. This would ensure that the evidence collected in one state is just as good in another, creating a stronger, more reliable legal system.[16]

Secondly, a big priority has to be creating official, high-quality training programs where everyone can get involved. The training should go beyond the basics and get into the nitty-gritty details of digital forensics, managing electronic evidence, and the legal issues with new tech. We need to teach police how to properly handle digital files from the very beginning, train prosecutors on how to use digital evidence to build a case, and give judges the knowledge

[16] Investment in modern forensic technology and need for unified standards in India: Deloitte India and Data Security Council of India, 'Indian Digital Forensic Market Report 2025' (Deloitte India, 5 June 2025) <https://www.deloitte.com/in/en/about/press-room/india-must-fast-track-indigenous-r-d.html>accessed 3 September 2025.

to carefully evaluate what experts tell them. This is crucial for filling the knowledge gap that's in our justice system today.[17]

Thirdly, it's really important to improve how we work with other countries. Cybercrime doesn't stop at the border, and neither should our ability to investigate it. We need to make it easier to use things just like the Mutual Legal Assistance Treaties (MLATs) and create better ways to share data across borders. This would help Indian agencies quickly get data from foreign servers, speed up investigations, and ensure that people who commit cybercrimes internationally can be held responsible more effectively.[18]

And fourthly, we have to strengthen our laws to find a better balance between protecting data and catching criminals. These new data protection laws need clear, detailed rules for law enforcement. These rules should focus on data minimisation, taking only what's absolutely needed, or proportionality, making sure the invasion of privacy is justified by the seriousness of the crime. This would make the whole investigation process more transparent and accountable, helping to build public trust while still allowing the police to do their job well.[19]

Finally, a key step is to create a single, secure, nationwide e-FIR system. This would replace the current messy, state-by-state approach with one united system. This platform should have consistent rules for filing a report and a quick way to verify them to stop fake complaints from the very beginning. A centralised system would not only be more efficient and easier for the public to use, but would also ensure that every citizen has a consistent right to file a complaint, no matter where they are.[20]

Similarly, Blockchain Technology has the potential to completely change how we handle evidence by making it impossible to tamper with and creating clear, transparent records. By

[17] Official training programs and curriculum in digital forensics:
SGT University, 'M.Sc. Digital Forensics and Information Security' (SGT University, 2024) <https://sgtuniversity.ac.in/science/programmes/msc-digital-forensics> accessed 3 September 2025.
[18] Improving international cooperation in cybercrime investigations:
Ministry of External Affairs, India, 'India and US sign MoU on Cybercrime Investigations' (17 January 2025) https://www.mea.gov.in/press-releases.htm?dtl%2F38924%2FIndia_and_US_sign_MoU_on_Cybercrime_Investigations accessed 3 September 2025.
[19] Strengthening data protection laws with law enforcement guidelines under DPDP Act 2023:
CookieYes, 'India's Digital Personal Data Protection Act (DPDP Act) Explained' (16 June 2025) https://www.cookieyes.com/blog/india-digital-personal-data-protection-act-dpdpa/ accessed 3 September 2025.
[20] Creation of a single secure nationwide e-FIR system under BNSS 2023:
Bharatiya Nagarik Suraksha Sanhita, 'Standard Operating Procedure (SOP): Zero FIR & e-FIR' (2023) https://bprd.nic.in/uploads/pdf/SOP_on_Zero_FIR%20&%20eFIR%20-%20NCL%202023.pdf accessed 3 September 2025.

putting a timestamp on digital evidence in a localised ledger, blockchain can make the chain of custody stronger and also reduce the risk of tampering. To add these new tools to our current legal systems, technologists, lawmakers, and judges will need to work together to create rules that keep our evidence standards high while embracing new technology.[21]

ETHICAL AND HUMAN RIGHTS DIMENSIONS IN DIGITAL EVIDENCE AND E-FIR PRACTICES

As technology evolves rapidly than usual, our criminal justice system has no choice but to keep up. It needs to look ahead, embracing new tools and methods to build a legal framework for such digital evidence that will never become outdated.

A major game-changer on the horizon is the use of Artificial Intelligence (AI) and Machine Learning (ML) in digital forensics, and that's where the world is actually racing. Think of it like a superhero for investigators. These technologies can do the tedious work of sifting through massive amounts of data within a small portion of the time that a human takes naturally. They're amazing at spotting hidden patterns and identifying the subtle signs of tampering, like a flawless deepfake or a piece of evidence that has been secretly altered. This doesn't just speed up investigations, but it can also uncover crucial clues that would have remained completely hidden using old-school methods.

However, bringing AI into the courtroom isn't as simple as just plugging it in. Well! It brings a host of new legal headaches. The biggest one is the issue of explainability. When a human expert gives testimony, a prosecutor can ask, "How did you reach that conclusion?" and the expert can explain their reasoning step-by-step. An AI, on the other hand, often works like a "black box." It answers, but its internal decision-making process can be a complete mystery.

This lack of transparency raises a fundamental question about fairness in justice. "How can a defendant challenge evidence if no one, or not even the people who created the AI, can fully explain how it works?" This could put a defendant's right to a fair trial in jeopardy.

To solve this, courts will have to step up. They'll need to create entirely new legal standards for judging the reliability of AI-generated evidence. However, this means that the judges and lawyers will have to get much more comfortable with the basics of AI. They'll need to

[21] S. Sridharan, 'Artificial Intelligence in Digital Forensics: Opportunities and Challenges' (2025) Indian Journal of Law and Technology 115.

understand not only "what these technologies can do" but also their limitations and, crucially, their potential for hidden biases that could unfairly target certain groups of people. It's a huge task, but it's one that we can't afford to ignore if we want our justice system to remain fair and effective in the digital age.

Privacy as a Constitutional Imperative: The Supreme Court of India made a landmark decision in the case of Justice K.S. Puttaswamy (Retd.) v Union of India (2017), by recognising that privacy is a fundamental right under Article 21 of the Constitution. This was a huge deal, and it created a critical legal foundation for how digital forensic practices are now judged.[22] The problem is that gathering digital evidence can be very invasive in nature. It often involves collecting massive amounts of data, harvesting metadata (data about data), or even continuous surveillance. These practices pose a serious risk to the very right to privacy that the Supreme Court just recognised.

In digital investigations, the police must strictly follow court rules that require data collection to be necessary, proportional, and for a legitimate purpose. Collecting data without good reason or in an overly broad way does not just violate people's constitutional rights, but it also makes the public lose trust in law enforcement.[23] In simple terms, for digital forensic investigations to be effective and lawful, they must be operated under a strict judicial oversight, and this oversight ensures three key things: necessity, proportionality and legitimate purpose.

For instance, an investigator cannot simply demand all of a suspect's digital data just because a small part of it might be relevant. The request must be limited to what's necessary; a judge might approve access to a specific email account, from a certain time frame, but not their entire cloud history. When police conduct arbitrary or overly broad searches, it's not just a legal violation, but it also deeply harms public trust. People become more hesitant to cooperate with law enforcement, which can hinder future investigations and damage the relationship between the community and the police.

This is where the new Digital Personal Data Protection Act, 2023 (DPDPA) comes in. It is the most powerful new law that takes these judicial principles and puts them into clear legal duties for forensic examiners. The Act requires them to operate with both fairness and transparency, which means that they must be open about what data they are collecting and why. It also

[22] Justice K.S. Puttaswamy (Retd.) & Anr v Union of India (2017) 10 SCC 1.
[23] Sanchit Mathur et al, 'The Growing Field of Digital Forensics: Ethical Challenges in India's Digital Landscape' (2025) Vellore Institute of Technology Bhopal.

enforces purpose limitation, ensuring the data they collect is used only for the specific investigation and not for other purposes. Essentially, the DPDPA acts as a legal guidebook, telling investigators that they must handle data responsibly and make every effort to minimise privacy intrusions while doing their job. It not only strengthens the constitutional right to privacy but also provides clear rules, creating a system that is both more secure for citizens and more accountable for law enforcement.[24]

Ethical Challenges in Digital Forensics: Currently, India does not have a set of clear, mandatory ethical rules just for digital forensic professionals. Unfortunately, this lack of regulation creates a lot of uncertainty and opens the door for potential misconduct, like making up evidence, holding back certain data, or showing bias in how they interpret their findings.[25] Experts believe that there should be a strong code of conduct that focuses on forensic integrity, keeping a strict chain of custody, and having tough rules to prevent conflicts of interest. This would protect both the fairness of the legal system and the reliability of scientific evidence.[26]

Ethical challenges are getting more serious day by day, with new technologies like AI-powered forensic tools. These tools bring up questions about how transparent and explainable the algorithms are, and whether their potential biases could unfairly affect the rights of people who are accused of crimes.[27] Also, forensic practices have to find a balance between both the urgent needs of an investigation and the sensitive nature of digital data. This is particularly true for private communications, data belonging to minors, and information related to marginalised groups, all of which just require stronger protections.[28]

Transparency, Accountability, and Oversight: In order to make sure that forensic practices are ethical and to prevent misuse, we need to have clear rules and independent oversight. The recent changes in the Bharatiya Nagarik Suraksha Sanhita, 2023, are a step in the right direction. This is what they now require: that police and other agencies record, search and seizure operations, and forensic sample collection, which makes the whole process more transparent.[29] However, there are still gaps in how these rules can actually be put into practice.

[24] Digital Personal Data Protection Act, 2023 (India).
[25] Deepali and Radhika Dev Verma, 'Role of Digital Forensics and Criminal Investigation in India' (2025) International Journal of Research Publication and Reviews.
[26] 'Guidelines on Ethical Use of Digital Forensics', Ministry of Home Affairs Report (2025).
[27] A. Nayak, 'Algorithmic Transparency and Fairness in Forensic AI Evidence' (2025) 15 Journal of Law and Technology 78.
[28] ibid
[29] Bharatiya Nagarik Suraksha Sanhita, 2023 (India), ss 105, 349.

So, the most important thing is that we need to strengthen our institutions and get civil society involved to actively monitor both forensic processes and e-FIR operations.

Thus, to deal with these issues now, we could make some key policy changes. For example, we could create a forensic audit committee, set up regular reviews, and protect the whistle-blowers who report the problems with the forensic integrity. Taking these few steps would help in bringing India's forensic practices up to the level of the best international standards, such as those set by the International Organisation on Digital Evidence and the International Organisation for Standardisation (ISO) or the International Electrotechnical Commission (IEC).[30]

Balancing Law Enforcement and Civil Liberties: The ability of digital evidence to speed up and improve criminal investigations is a powerful tool, but it also comes with the risk of police overreach. In India and elsewhere, there have been several cases of misuse, such as manipulating digital evidence, violating people's privacy, or using surveillance for political reasons. This highlights the urgent need for strong legal protections.[31] Judges are increasingly focusing on the right to a fair trial, which directly means courts have to carefully examine how digital evidence is collected. They're also looking at whether the evidence is truly relevant to the case, especially when it affects someone's privacy.[32] To ensure procedural fairness, it's also very important to have effective ways for people to get a legal remedy if their rights are violated by digital forensic activities.

RECOMMENDATIONS AND FUTURE PERSPECTIVES FOR DIGITAL EVIDENCE AND E-FIR LEGAL FRAMEWORK

The legal reforms in India regarding digital evidence and the new e-FIR systems are a fantastic step forward, showing a real commitment to bringing the criminal justice system into the 21st century. However, these changes are truly appreciated, but they are not without their growing pains. These ongoing problems are very significant, spanning everything from legal ambiguities to the need for updated laws and the technical infrastructure required to handle vast amounts of digital data. We also have to consider the operational challenges, such as the

[30] International Organization on Digital Evidence, 'Standards and Best Practices for Digital Forensics' (2018); ISO/IEC 27037 and 27041.
[31] S. Sridharan, 'Challenges in Judicial Assessment of Digital Evidence' (2024) 12 Indian Journal of Law and Technology 101.
[32] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2019) 2 SCC 44.

training of personnel, the similarity of procedures, and ensuring that every police station can implement these systems effectively. Moving next, it's going to take some focused, creative solutions and a clear vision from policymakers to make sure that these promising initiatives deliver on their full potential and truly transform the system for the better.

Establishing Strong Forensic Infrastructure and Accreditation: Now, think of it this way, our forensic laboratories need serious maintenance to keep up with the digital world. To make sure that we can stand by the authenticity of every digital evidence in court, these labs need to be modernised, adopt universal protocols, and earn international accreditation. An important part of this is investing in cutting-edge technology that tackles modern problems. We should be looking at tools like blockchain to make sure that evidence storage is tamper-proof, using automated systems for metadata validation, and even using AI to detect deepfakes.[33] Creating a national board to set these forensic standards would be a game-changer, ensuring that all states and agencies handle evidence with the same level of care and precision.

Exhaustive Capacity Building and Judicial Training: Making just laws is not enough; we need people who can actually use them. We should set up a thorough, multi-level training program for everyone who's involved, police investigators, lawyers, forensic experts, and judges, so that they can all keep up with the fast-changing world of digital forensics. Offering specialised cyber forensic certification courses and requiring ongoing legal education will really help in improving the quality and consistency of how these cases are handled.[34]

Enhancing Data Protection and Privacy Safeguards: While implementing a new digital evidence structure, we have to be very careful about privacy. And the new policies should follow the rules of India's Digital Personal Data Protection Act, 2023. This means that we have to set clear limits on how much data can be collected and put in place strong, transparent oversight to prevent the government from overreaching with digital surveillance and evidence collection in future.[35] It's a good idea to create new technical standards for tools that can extract the evidence while still protecting a person's privacy.

Streamlining Cross-Border Cooperation: As we all know, cybercrime is a global issue, so India cannot tackle this alone. That's why it is very crucial for us to focus on working with

[33] Anju Gandhi et al, 'Electronic evidence changes will modernise banking practices' (Law.asia, 5 November 2024) <https://law.asia/electronic-evidence-indian-law> accessed 3 September 2025.
[34] Ministry of Home Affairs Report, 'Capacity Building for Cybercrime Investigation' (2024).
[35] Digital Personal Data Protection Act, 2023.

other countries and making it a bit faster to share digital evidence across borders. Let's think of it like this: a lot of the time, the evidence for a crime committed in India might be sitting on a server in another country. And to get that evidence, our laws and standards need to match up with international ones. By getting in relation with the models from places like the EU and the UK, we can ensure smoother judicial cooperation and more effective results.[36]

Upgrading e-FIR Systems for Security and Usability: We need to always make sure that our online police report (e-FIR) portals are extremely secure. They have to be protected from multiple things, like hacking, denial-of-service attacks, and data breaches. To make sure that the person filing the report is who they say they are, we should also add features like fingerprint scans or multi-factor authentication. And to keep things consistent and smooth across the country, we should create a single set of national rules for e-FIRs, along with clear technical and procedural guidelines.[37]

Fostering Judicial Technological Literacy: Judges will always need to keep updating their procedural rules to handle the digital evidence and virtual hearings, much like the Delhi High Court's new rules, on both electronic evidence and video conferencing. These changes help in making the legal system more accessible and smoother, while still protecting everyone's rights. We could also help this along by appointing more judges who have a background in technology.[38]

Promoting Public Awareness and Transparent Governance: To help people trust more and use these new digital justice systems, we need to educate them regarding as much information as possible. We have to teach citizens about their rights regarding the digital evidence, and also how to use e-FIR (online police reports), and what their privacy protections are. And when people understand how digital evidence is handled and what safeguards are in place, they will have more confidence in the system, which is crucial for these new tools to succeed.

[36] 'Cross-Border Electronic Evidence Frameworks – EU vs. India' (NJCSL, 2025) <https://lawjournals.celnet.in/index.php/njcsl/article/view/1884> accessed 3 September 2025.
[37] MeitY, 'Guidelines for Securing e-FIR Portals' (2023).
[38] Delhi High Court, 'Electronic Evidence and Video Conferencing Rules, 2025' (2025) <https://www.scconline.com/blog/post/2025/07/11/delhi-high-court-electronic-evidence-video-conferencing-rules-2025 >accessed 3 September 2025.

2 PRINCIPAL CASE STUDIES

Case Study 1: Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473: This landmark Supreme Court case totally changed how courts in India handle digital evidence. Basically, in this case, there was a person who challenged the use of some electronic evidence in an election dispute. The main issue was that the evidence didn't have a special certificate that was required by a specific law (Section 65B(4) of the Indian Evidence Act). The Court agreed with the person's challenge. It ruled that for electronic records to be used as evidence; they must have this certificate to prove that they are authentic. Without this, the evidence cannot be used in court.

This decision was a big deal because it put strict rules directly in place. Previous court decisions had been a bit more relaxed, but this ruling highlighted that because digital data is so easy to manipulate, we need formal safeguards. The case highlighted a key problem: how do you balance the strict rules of court procedure with the reality that digital evidence can be easily tampered with? This decision basically presumed some key points, and that is, to maintain trust, you need to rely on certificates, expert opinions, and a clear record of who was handling the evidence.

However, some people have also argued that this strictness can be a problem. They say it might prevent genuine evidence from being used just because of a technicality, which could get in the way of finding the truth. This case created a strong legal foundation for how judges would handle digital evidence in the future, trying to find a balance between being flexible and ensuring the evidence is reliable.

Case Study 2: Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2019) 2 SCC 44: The main point of this new ruling was a key distinction, where, if the electronic evidence is an original (for example, the actual phone or computer), then, in this case, it doesn't need the special certificate mentioned in the previous case. However, if it's a copy of original electronic evidence, then it still needs that certificate to be used in court.

The Court also stated that the judges should look at the bigger picture, especially when they are evaluating the digital evidence, considering things like how trustworthy it is and the context in which it was found. This ruling was a step forward because it showed how the court was adapting to the real world. It recognised that it is not always practical to bring an original digital device to court. And this is what gave judges more flexibility to use their own judgment and prevent a case from failing just because of a technicality.

However, this new flexibility and changes also apply more pressure on the judges. They now need to be more tech-savvy and will have to understand forensic science to make good decisions. Highlighting the need for the court system to improve its own digital skills. So, in the end, the Khotkar case shows how the legal system is trying to find a balance between the demands of modern technology and the fundamental right to a fair trial.

CONCLUSION

India's legal and criminal justice system is currently going through a massive technology upgrade, and it is a really big deal. New laws, like the Bharatiya Sakshya Adhiniyam, 2023, are the game-changers. They now treat digital files and records as a primary form of evidence, which makes it much easier to use them in court and also in cutting down on a lot of the old paperwork and rules. This is a smart move, because our world is becoming more digital, and also the crimes are in the same way. But this big change comes with its own set of challenges.[39]

Courts are right in the middle of this. Where on the one hand, they want to be open to using digital evidence, but at the same time, on the other hand, they have to be very careful because it's so easy to tamper with. Landmark Supreme Court cases such as Anvar P.V. v P.K. Basheer and Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal have shown how judges have gone back and forth on this sometimes, being very strict with rules and other times being more flexible also. This struggle shows that our judges need to become more tech-savvy. They need to understand how forensic science can make good decisions, and we need better, more consistent standards for forensics across the country.[40]

Our law enforcement agencies are also facing the same big hurdles. Many of our forensic labs don't even have enough resources; the tools are outdated, and training is often inconsistent. This is what messes up the evidence, and as a result, can slow down cases, creating loopholes that can be exploited in court.[41] While online police reports (e-FIRs) are a revolutionary step forward, they also bring up new problems, like making sure the person filing the report is real and that everyone's data is kept secure.

[39] Jayaditya Sharma, 'Reforming Cybercrime Investigation In India: A Forensic and Legal Framework Approach' (2025) 12 Indian Journal of Law and Legal Research 101.
[40] Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2019) 2 SCC 44.
[41] Harshit Gupta, Monika Rastogi, and Ruchi Kaushik, 'The Intersection of Digital Forensics and Criminal Investigation in India: Legal and Procedural Dimensions of Evidentiary Standard' (2025) 4 International Journal of Human Rights Law Review 128.

Then also comes the big question of privacy. Where the Supreme Court confirmed that privacy is a fundamental right, and with this new Digital Personal Data Protection Act, 2023, the government can't just collect whatever data it wants. Here, we need to strike the tricky balance; we need to allow for effective investigations while making sure that individual rights aren't trampled. The people want clear rules and transparent oversight to prevent the government from overreaching with digital surveillance.[42]

To truly succeed, we cannot just throw technology at the problem; instead, we will need a comprehensive plan. Which means not only investing in advanced tech like AI-assisted tools and blockchain for evidence is enough, but also getting everyone on the same page is necessary. This includes better training for both police and judges, and creating consistent rules for how things are done. Since cybercrime doesn't respect borders, we will have to improve our ability to work with other countries to share evidence seamlessly.

India is at a critical point. The new technology and laws are just exciting, but ever thought that they can also be risky, being the "hollow victories" if we don't address the underlying problems like a lack of resources, legal ambiguities, and human rights concerns. However, if India tackles these challenges with smart policies, forward-thinking judges, and a clear vision, then there's a high chance that it could create a world-class model for a fair and effective digital justice system.

[42] Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1; Digital Personal Data Protection Act, 2023.