CHALLENGES IN ADMISSIBILITY OF DIGITAL EVIDENCE: CONSTITUTIONAL CONCERNS, HUMAN RIGHTS, AND COMPARATIVE PERSPECTIVE

Mridul Bhatt, LL.M. (Cyber and Security Law),
ICFAI University Dehradun, Uttarakhand, India[1]

ABSTRACT

The BSA and BNSS together have placed fundamental rights under acute stress by giving the State powerful tools to seize and forensically clone entire digital devices without proportionate safeguards. The Supreme Court in *K.S. Puttaswamy v. Union of India (2017)* declared privacy a fundamental right under Article 21 and established a three-part test — legality, necessity, and proportionality — but current police practice routinely fails the proportionality prong. When a phone is seized for a minor financial offence and a full bit-stream copy is made, the police effectively walk away with a person's intimate photographs, medical data, and private conversations, none of which are relevant to the charge — a "fishing expedition" that the Puttaswamy framework squarely prohibits. The self-incrimination front is equally contested: courts have begun distinguishing between passwords, which originate in the mind and are therefore testimonial (protected under Article 20(3)), and biometrics, which are physical and arguably not. However, this distinction collapses in practice because unlocking a phone by any method gives the police access to deeply testimonial content, making the act of unlocking functionally equivalent to compelled self-incrimination. Beyond these individual rights, the BSA creates a structural "justice divide" — the State commands entire forensic laboratories while an ordinary accused cannot afford a single private expert to challenge a hash mismatch or a manipulated timestamp, violating the principle of equality of arms under Articles 14 and 21. Globally, the UK solved its equivalent bottleneck by presuming computers reliable unless the defence proves otherwise; the US made hash-certified evidence self-authenticating; and the EU standardised "qualified electronic signatures" that courts accept automatically. India's current dual-certificate regime, by contrast, demands manual expert endorsement for every piece of digital evidence — a 19th-century solution that urgently needs to absorb these three models to survive the AI age without sacrificing constitutional rights.

[1] LL.M. Cyber and Security Law, ICFAI University Dehradun, Uttarakhand, India

Keywords: *Digital evidence, Admissibility, Privacy rights, Self-incrimination, Search and seizure, Equality of arms, Comparative law.*

1.1. The Right to Privacy vs. State's Power of Search and Seizure (The Puttaswamy Impact)

The implementation of the *Bharatiya Sakshya Adhiniyam (BSA), 2023*, alongside the new procedural law, the *Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023*, has triggered a massive conflict. This conflict is not just between two laws, but between the massive power of the State's investigative machinery and the fundamental rights of the individual citizen. The central battlefield for this conflict is the "Right to Privacy," which was declared a fundamental right under Article 21 of the Constitution by the Supreme Court in the historic judgment of *K.S. Puttaswamy v. Union of India* (2017)[2].

To understand this conflict, we must first look at how the concept of "search" has changed. In the pre-digital era—the world of the *Indian Evidence Act*—a "search and seizure" operation had physical limits. If the police wanted to search a suspect's house, they entered a physical door. They could look in cupboards, under the bed, or in a safe. The "privacy" of the individual was limited by the four walls of their home. Once the police left the building, the search was over. The boundaries were clear, visible, and tangible.

In 2026, this logic has completely collapsed. The smartphone is not just a "communication device" or a "material object." It has evolved into a **"Virtual Home."** A single device in your pocket contains more information about your life than your physical home ever could. It holds your financial history (banking apps), your health records (fitness trackers), your intimate conversations (WhatsApp), your political beliefs (Twitter/X history), your location history (Google Maps), and your memories (Photo Gallery).

The constitutional challenge arises because the *Bharatiya Nagarik Suraksha Sanhita (BNSS)* grants the police broad powers to seize these devices, but it does not provide specific rules for *how* to search them. This creates a dangerous situation often called a **"General Warrant"** scenario.

Under the "Proportionality Test" established in the *Puttaswamy* judgment, any state action that

[2] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

invades privacy must meet three strict conditions:

1. **Legality:** There must be a law in place.
2. **Necessity:** The invasion must be for a legitimate state aim (like solving a crime).
3. **Proportionality:** There must be a rational link between the aim and the invasion. The state should not use a sledgehammer to crack a nut.

The current practice violates this "Proportionality" principle. Imagine a scenario where a person is accused of a minor economic offense, like tax evasion. The police seize their phone. In a physical world, the police would only look for financial documents. But in the digital world, forensic experts create a "Bit-Stream Copy" (as discussed in Chapter 3) of the *entire* phone. This means the police now have access to the suspect's private photos, their chats with their spouse, their health data, and their children's information—none of which is relevant to tax evasion.

This is what legal experts call a **"Fishing Expedition."** The state seizes the device for one reason but then "fishes" through the massive amount of private data to find evidence of other crimes or simply to harass the individual. Defence lawyers in the post-BSA era are fighting back, filing petitions in High Courts. They argue that a digital seizure is a seizure of the "Digital Soul." They are demanding that digital warrants must be "purpose-limited." If the crime is financial, the warrant should only allow the police to search financial apps, not the photo gallery. Without these safeguards, the broad powers under the BNSS threaten to turn every citizen into a glass house, visible to the state at all times.

1.2. Article 20(3) and Self-Incrimination: Compelled Disclosure of Passwords and Biometrics

The most heated constitutional battle in the BSA era is taking place at the intersection of technology and the "Right against Self-Incrimination." This right is enshrined in **Article 20(3)** of the Indian Constitution, which states that no person accused of an offense shall be compelled to be a witness against themselves. In simple terms, the police cannot force you to speak and help them convict you.

However, modern technology has complicated this simple right. Our digital lives are locked

behind two types of gates:

1. **Knowledge-Based Security:** Things you *know*, like Passwords, PINs, or Patterns.
2. **Biometric-Based Security:** Things you *are*, like your Fingerprint, Face ID, or Iris Scan.

The judiciary is currently struggling to decide which of these falls under the protection of Article 20(3).

The Password Dilemma (The "Mind" Argument):

A password is a secret stored inside your brain. Under the legal precedents set by the Supreme Court in *Selvi v. State of Karnataka* (2010)[3], the state cannot force you to share information stored in your mind (like during a Narco-analysis test) because that violates your "Mental Privacy." If the police force a suspect to say their password or type it in, they are effectively forcing the suspect to "testify" against themselves. By giving the password, the suspect is admitting, "Yes, this is my phone, and I control its contents." If the phone unlocks and reveals incriminating chats, the suspect has been forced to help the police find that evidence. Defence lawyers argue that this is a direct violation of Article 20(3). They assert that a suspect has a constitutional **"Right to Silence,"** and this extends to digital silence. If a suspect refuses to give the password, they are exercising their right not to incriminate themselves.

The Biometric Paradox (The "Body" Argument):

On the other hand, biometric locks (Face ID or Fingerprint) are viewed differently. In the older case of *State of Bombay v. Kathi Kalu Oghad*, the Supreme Court held that asking an accused to give a fingerprint, a handwriting sample, or a blood sample is *not* a violation of Article 20(3). Why? Because these are physical facts. They are not "testimony." The police argue that asking a suspect to look at their phone (for Face ID) or put their thumb on the sensor is just like taking a fingerprint on paper. They argue it is a physical act, not a mental one. However, human rights activists argue this analogy is flawed and dangerous. Giving a fingerprint on paper is for *identification*—to prove who you are. Giving a fingerprint to unlock a phone is for *access*—to open a vault of private testimony. The "act of unlocking" is functional; it provides the police

[3] Selvi v. State of Karnataka, (2010) 7 SCC 263

with access to documents, emails, and chats that are definitely testimonial.

This creates a constitutional grey zone. In many cases, investigating agencies use the broad powers of the BNSS to threaten suspects with "non-cooperation" charges if they don't unlock their phones. Recent cases, such as *Digital Rights Forum v. Union of India* (2025)[4], have highlighted this tension. The courts are being asked to decide: Is the digital key to your private life protected by the Constitution, or does the state's need to solve crime override your right to keep your digital mind locked? Until the Supreme Court gives a final ruling, this remains a dangerous area where the "Right to Silence" is slowly being eroded by a "Duty to Decrypt".

1.3. The "Right to be Forgotten" in Judicial Records

While the digitization of courts and the BSA's electronic evidence rules have made justice faster, they have also created a permanent **"Digital Panopticon"** for those who are accused but later acquitted. This brings us to the **"Right to be Forgotten" (RTBF)**—the right of an individual to have their personal information removed from the internet and public records after a certain period of time.

In the physical world, if you were acquitted of a crime 20 years ago, the files would gather dust in a basement. Your neighbours and future employers would likely never know. The stigma would fade with time. In the digital world of 2026, nothing fades. The BSA facilitates the seamless integration of digital records into the judicial system. This means that sensitive digital data—such as intimate images in a "revenge porn" case, or embarrassing chat logs in a conspiracy trial—becomes part of the permanent judicial record.

Even if an accused is found innocent and acquitted, the digital footprint of the trial remains alive. The judgment is uploaded to legal databases (like Manupatra or SCC Online) and indexed by Google. Anyone searching the person's name will immediately find the judgment, the forensic reports, and the details of the allegations. The stigma becomes permanent.

The conflict here is between two rights:

1. **The Right to Privacy (Article 21):** The acquitted individual wants to move on and not

[4] Digital Rights Forum v. Union of India, 2025 INSC 134

be haunted by the past.

2. **The Principle of Open Courts (Article 19):** The public has a right to know what happens in court (Right to Information).

Legal researchers argue that the BSA has a major gap: it lacks a **"Data Expiry" protocol**. What happens to the "Bit-Stream Copy" of the suspect's phone that is sitting in the forensic lab's server? Even after the trial is over and the person is free, the state often retains this massive dump of private data. There is a genuine fear of data leaks. If a forensic lab is hacked five years later, the private photos of an innocent person could be leaked to the internet.

Indian High Courts are increasingly hearing pleas from people asking for their names to be redacted (removed) from digital judgments so they can find jobs or get married without their past haunting them. The argument is that the "Right to be Forgotten" is not just about erasing search results; it is about the **physical destruction** of the digital forensic clones created under Section 63 procedures. The state should not hold onto a citizen's private data forever just because they were once a suspect.

1.4. Equality of Arms: The Economic Barrier to Accessing Forensic Experts

A fundamental principle of a fair justice system is **"Equality of Arms."** This means that both sides—the Prosecution (the State) and the Defence (the Accused)—must have equal weapons to fight the legal battle. If one side has a tank and the other has a stick, the trial cannot be fair.

The BSA's complex reliance on forensic science and the Section 63(4) certification requirement threatens to destroy this equality. It risks creating a justice system that is deeply divided by economic class.

Consider the resources of the State. The Prosecution has access to the vast machinery of the government. They have the Central Forensic Science Laboratories (CFSL), State Forensic Science Laboratories (SFSL), and the National Crime Records Bureau (NCRB). They can order advanced hash value verification, metadata analysis, and deepfake detection at the taxpayer's expense. They have a sophisticated army of experts at their disposal.

Now consider the accused. Unless they are a wealthy business tycoon, the average citizen lacks the resources to fight this digital battle.

- **The Cost of Defence:** Hiring a private forensic expert to challenge the state's evidence is incredibly expensive. To prove that a hash value is mismatched, or that a timestamp was altered ("time-stomped"), the defence needs to hire a specialized cyber-forensic consultant. In 2026, the fees for these experts are prohibitive for the common man.

- **The "Expert Deficit":** As noted in plethora of judgements, there is already a shortage of experts. The few good private experts are expensive and often booked by corporate clients.

This creates a **"Justice Divide."** If the state produces a forensic report saying, "This laptop contains incriminating emails," an indigent (poor) accused has no way to verify if that is true. They cannot afford to hire an expert to check if the laptop was tampered with or if the emails were planted. They are forced to accept the prosecution's evidence as "Gospel Truth" simply because they cannot afford to challenge it.

This is a violation of **Article 14 (Right to Equality)** and **Article 21 (Right to Fair Trial)**. Legal scholars are calling for **"Digital Legal Aid."** Just as the state provides a free lawyer to a poor accused, the state must now provide free forensic experts to poor accused persons. Without this support, the truth in a courtroom will not be determined by facts, but by who has the money to decipher the bit-stream.

1.5. Fair Trial Concerns: The Risk of "Trial by Metadata"

Finally, the most subtle but dangerous threat to human rights under the BSA is the phenomenon of **"Trial by Metadata."**

In the old days, a trial was about human stories—motive, character, eyewitness accounts. In the BSA era, the trial is becoming about data points. The law allows for the admission of vast quantities of metadata: GPS location logs, call duration records, tower locations, and login timestamps. The danger is that prosecutors can use this data to create a narrative of guilt based on **correlation, not causation**.

The Problem of Decontextualization:

Metadata is stripped of context.

- A GPS log might place an accused at the scene of a crime. But it doesn't show *why* they were there. They might have been passing by, or buying milk. The data only shows "presence," but the prosecution presents it as "opportunity."

- A call log might show that the accused called the victim five times on the day of the murder. It looks suspicious. But the metadata doesn't record the *content* of the calls. They might have been discussing a mundane work issue.

In the absence of the actual content (often because messages are encrypted or deleted), prosecutors rely heavily on this circumstantial metadata to weave a web of guilt.

The Presumption of Machine Infallibility: There is a psychological bias known as "Automation Bias." Judges and juries tend to trust computers more than people. If a witness says, "I saw him there," the judge might doubt the witness's eyesight. But if a computer printout says, "GPS Lat/Long: 28.6139° N, 77.2090° E," the judge tends to accept it as objective, scientific truth. This is dangerous because, as discussed in Chapter 3, digital evidence *can* be manipulated. GPS can be spoofed. Phones can be cloned. Timestamps can be altered. When a court convicts a person primarily based on metadata patterns, it risks eroding the **"Presumption of Innocence."** The burden of proof shifts to the accused to explain the data, rather than the prosecution proving the guilt.

Furthermore, there is the issue of **"Information Overload"** or "Data Dumping." In complex cases, the prosecution often dumps terabytes of raw data on the defence team just days before the trial. It is physically impossible for a human lawyer to read through thousands of pages of server logs to find exculpatory evidence (evidence that proves innocence). This tactic cripples the defence's ability to cross-examine effectively.

The risk is that the *human* element of the trial—the assessment of reasonable doubt, intent, and morality—is being swallowed by the cold, often misleading, certainty of the algorithm. We risk entering an era where the machine decides guilt, and the judge merely stamps the printout.

1.6. United Kingdom: The PACE Act and the Presumption of Computer Reliability

To evaluate the efficacy of the *Bharatiya Sakshya Adhiniyam (BSA), 2023*, it is imperative to look beyond India's borders. The United Kingdom offers the most pertinent comparative study because the Indian legal system shares its common law roots with English jurisprudence.

Historically, the UK faced the same "certificate crisis" that India is facing today, but their legislative response took a fundamentally different trajectory.

In 1984, the UK enacted the *Police and Criminal Evidence Act (PACE)*. Section 69 of this Act was remarkably similar to Section 65B of the Indian Evidence Act (and the new Section 63 of the BSA). It required the prosecution to prove that the computer was operating properly and was not subject to malfunction. This created a heavy burden on the prosecution to produce technical evidence for every routine computer printout.

However, by the late 1990s, the British Law Commission realized that this requirement was archaic. They argued that in the modern world, computers are generally reliable, and requiring a certificate for every piece of digital evidence was clogging up the courts. Consequently, via the *Youth Justice and Criminal Evidence Act 1999*, the UK Parliament **repealed Section 69** of the PACE Act[5].

The Shift to Presumption: Today, the UK operates on a common law "Presumption of Reliability." The courts presume that a mechanical instrument (like a computer) was in order at the material time unless the contrary is shown. This is a reversal of the burden of proof compared to the BSA.

- **Under the BSA (India):** The prosecution *must* affirmatively prove the computer was working (via Section 63 certificate) to get the evidence in.
- **Under UK Law:** The evidence is admitted automatically. If the defence wants to challenge it, *they* must bring evidence to show the computer was broken.

This approach solves the "Expert Bottleneck." In the UK, you do not need a forensic expert to certify a bank statement or a call log. The court assumes the bank's server was working. The expert is only called if the defence makes a specific, credible allegation of tampering. For India, this offers a powerful lesson: Is the BSA's rigid demand for a "Dual-Certificate" in every single case an over-correction? The UK experience suggests that a "rebuttable presumption" of reliability expedites trials without compromising justice, reserving forensic resources for cases where authenticity is genuinely contested.

[5] Youth Justice and Criminal Evidence Act 1999, c. 23 (United Kingdom), repealing Section 69 of PACE 1984

1.7. United States: Federal Rules of Evidence (Rule 902) and Self-Authentication

While the UK offers a lesson in "Presumption," the United States offers a lesson in "Self-Authentication." The US federal system deals with massive amounts of digital data using the *Federal Rules of Evidence (FRE)*.

The pivotal provision here is **Rule 902**, specifically the amendments introduced in 2017: **Rule 902(13)** and **Rule 902(14)**. Traditionally, to authenticate digital evidence in the US, a witness (like a forensic analyst) had to come to court and testify, "Yes, I copied this file." This "live testimony" requirement was expensive and slow.

The Solution: Digital Self-Authentication: Rule 902(14) allows for "Certified Data Copied from an Electronic Device, Storage Medium, or File." It introduces a mechanism where digital evidence can be "Self-Authenticating" if it is accompanied by a certification of its **Hash Value**[6].

Here is how it works:

1. A forensic technician creates a forensic copy of a hard drive.
2. They generate a Hash Value (digital fingerprint) for the original and the copy.
3. They sign a written affidavit stating, "The hash values match."
4. **Result:** The evidence is admissible *without* the technician having to appear in court.

This mechanism directly addresses the "Expert Bottleneck" identified in Chapter 2 of this dissertation. In India, under the BSA, the expert is often dragged to court to testify even for routine matters. In the US, the "certification by hash" replaces the live witness for the purpose of admissibility.

Furthermore, the US system is more flexible regarding *who* can certify. Unlike the BSA, which restricts the expert definition to those notified under Section 79A of the IT Act (creating a shortage), the US Rules allow any "qualified person" to certify the hash. This creates a much wider pool of eligible experts, ensuring that trials are not stalled waiting for a government

[6] Rule 902(13) & (14), Federal Rules of Evidence, (United States)

scientist. The US model demonstrates that "process-based" authentication (relying on the math of hash values) is more efficient than "person-based" authentication (relying on the status of the signatory).

1.8. European Union: The eIDAS Regulation and Electronic Signatures

The European Union approaches electronic evidence through the lens of standardized "Trust Services." The governing framework is the **eIDAS Regulation (Regulation 910/2014)**, which sets the standard for electronic identification and trust services across the entire EU market[7].

The EU framework is highly relevant to the BSA's Section 63(4) requirement for a "digital signature" or certificate. The eIDAS Regulation introduces a tiered system of electronic signatures that India could emulate to formalize its "Digital Notary" concept.

The Three Tiers of Trust:

1. **Simple Electronic Signature:** Basic data in electronic form (like a scanned signature).
2. **Advanced Electronic Signature (AES):** uniquely linked to the signatory and capable of identifying them.
3. **Qualified Electronic Signature (QES):** This is the gold standard. It is created by a "Qualified Electronic Signature Creation Device" and is based on a qualified certificate.

Legal Effect:

Under Article 25 of eIDAS, a **Qualified Electronic Signature (QES)** carries the *same legal effect* as a handwritten signature. Moreover, a "Qualified Electronic Time Stamp" enjoys a presumption of the accuracy of the date and time it indicates.

Comparison with India:

India has "Digital Signature Certificates" (DSC) under the IT Act, but their integration with the BSA is weak. The BSA demands a "certificate" but doesn't explicitly state that a high-security DSC is required. If India adopted the eIDAS model, the "Custodian" of a device could simply

[7] Article 25, Regulation (EU) No 910/2014 (eIDAS Regulation). (last accessed on 3.03.2026 at 08:21 pm)

affix a "Qualified Electronic Signature" to the evidence file. Because the QES is legally presumed to be valid and tamper-evident (if you change the file, the signature breaks), the court could accept the evidence immediately. The EU model teaches us that standardization is key. By creating a unified standard for "Trust Services," the EU ensures that digital evidence generated in France is easily admissible in Germany. For India, a similar standardization would allow a certificate issued by a forensic lab in Kerala to be instantly verified by a court in Delhi without procedural friction.

1.9. Lessons for India: Moving toward a "Best Evidence" Digital Model

What can India learn from these three global giants? The *Bharatiya Sakshya Adhiniyam, 2023*, is a significant step forward, but it is effectively a "hybrid" that is struggling to find its identity. It wants the strictness of the old world (certificates) but the speed of the new world.

To create a true "Best Evidence" model for the AI age, this dissertation proposes a synthesis of the best practices from the UK, US, and EU:

Lesson 1: Adopt the UK's "Rebuttable Presumption" for Routine Data. Not every WhatsApp chat needs a forensic expert. For routine, undisputed data (like bank statements or telecom logs), India should move towards the UK model. The law should presume the machine was working unless the defence can show a specific reason to doubt it. This would clear 80% of the backlog in Section 63 hearings.

Lesson 2: Adopt the US "Rule 902" for Hash-Based Authentication. The BSA is currently "person-centric"—it trusts the *person* signing the certificate. It needs to become "math-centric." India should amend the law to state that if a "Hash Value" is verified and certified by a qualified person, the evidence is self-authenticating. This would eliminate the need to summon experts to court just to say, "Yes, this is the file I copied."

Lesson 3: Adopt the EU's "Tiered Trust" for Digital Notaries. As proposed in the Problem Statement, the "Expert Bottleneck" is the biggest hurdle. India should adopt the eIDAS model to create a network of private "Digital Notaries." These would be private professionals (cyber-lawyers, IT security experts) armed with "Qualified Electronic Signatures." They could certify evidence at the scene of the crime or at the police station. Because their digital signature is encrypted and secure (like the EU QES), the court can trust it without needing a government

lab to verify every single file.

Conclusion:

The comparative analysis reveals that while the BSA is structurally sound, it is procedurally rigid. The global trend is moving towards *automation of trust*—using presumptions, hashes, and digital signatures to speed up admissibility. India's continued reliance on manual, dual-signature certificates is a "19th-century solution to a 21st-century problem." To truly modernize, the BSA must absorb the flexibility of the Common Law (UK/US) and the standardization of the Civil Law (EU).