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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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

ARTIFICIAL INTELLIGENCE IN JUDICIAL DECISION MAKING AND THE RIGHT TO A FAIR TRIAL: AN ANALYSIS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

AUTHORED BY - SAMBHAV SINGH,
PRABHAT RANJAN & TANISHKA SINGH
Amity University Lucknow Campus

ABSTRACT

The inevitable integration of Artificial Intelligence (AI) into the judicial system represents a decisive turning point in legal history, fundamentally transforming the procedural dynamics of justice-delivery. While on one hand AI holds the promise of reducing the heavy burden borne by the Indian judiciary, on the other hand its use raises serious constitutional concerns regarding the sanctity of fair hearing. The opacity of algorithmic decision-making—often termed the "black box" phenomenon—presents a direct challenge to principles of transparency, reasoning, and opportunity to confront evidence, which are core features of Article 21. With the recent enactment of the Indian Evidence Act (BSA), 2023, India has attempted to modernize its evidence-related framework. However, a critical gap remains: while this new law recognizes digital records, it remains largely silent on the unique epistemological challenges posed by AI-generated evidence—such as 'deepfakes' and biased 'predictive analytics.' This research paper presents an in-depth theoretical analysis aimed at examining whether the existing legal framework is sufficiently robust to prevent "algorithmic injustice." It argues that without specific safeguards—such as mandatory explainability and independent algorithmic auditing—the use of AI in courts could inadvertently undermine the constitutional guarantee of 'due process,' potentially transforming the accused from 'subjects of rights' into mere 'objects of data processing.'

KEYWORDS

Artificial Intelligence, Fair Hearing, Article 21, Indian Evidence Act 2023, Algorithmic Bias, Digital Evidence, Judicial Accountability, Constitutional Rights, Black Box Algorithms

ISSN: 2582-6433

CHAPTER 1: INTRODUCTION

1.1 *Background and Significance*

India's history of judicial administration has largely been a narrative of human judgment, where the gavel of justice has been wielded by individuals who have interpreted laws through experience, reason, and the light of conscience. For centuries, the court remained a fundamentally human forum, largely untouched by major technological changes. However, we now stand on the threshold of a profound transformation that has the capacity to fundamentally rewrite the basic grammar of justice itself. The digital revolution, which began merely with computerization, has rapidly transformed into the age of Artificial Intelligence (AI)—a technology that not only collects information but processes it, predicts from it, and even creates it. In a country where the judicial system is burdened with over 4.5 crore pending cases, the allure of AI as a panacea for eliminating delays is certainly very seductive. Its promise is efficiency: machines that can read files faster than any clerk, algorithms that can predict outcomes based on decades of old precedents, and software that can translate decisions into local languages in mere seconds.

Yet, viewing this merely as an administrative reform would be a grave mistake. What stands out most is that, for the first time in history, we are entrusting the cognitive functions of decision-making (adjudication) to non-human entities. Unlike typewriters or databases, which are passive tools, AI systems are active participants in the information ecosystem. Initiatives like the Supreme Court's SUPACE (Supreme Court Portal for Assisting Court Efficiency) indicate that the Indian judiciary is no longer standing on the sidelines watching, but is actively embracing these technologies. However, as we embrace speed, we must also ask: at what cost? The importance of this moment cannot be overstated, as the rules we set now will define the relationship between citizen and state for the next century.

It is also worth noting that legal systems are by nature conservative, designed to maintain stability and uphold precedents. The sudden entry of probabilistic algorithms into a system built on binary certainties (guilty or innocent) creates a philosophical collision. AI works on correlations found in vast datasets, while justice is based on causation and individual culpability. When these two logic systems collide, the possibility of systemic injustice becomes real. We have already seen warning signs globally, where algorithmic tools used for sentencing have demonstrated racial and socioeconomic biases that no human judge would openly

ISSN: 2582-6433

acknowledge.

This research is extremely important because India currently stands at a legislative crossroads. The enactment of the Indian Evidence Act (BSA), 2023, represents a decisive break from the colonial past, replacing the 150-year-old Indian Evidence Act. However, a critical shortcoming remains: while the new law attempts to modernize evidence rules, it remains largely silent on the unique epistemological challenges posed by AI-generated evidence—such as 'deepfakes' and biased 'predictive analytics'. This research paper presents an in-depth theoretical analysis aimed at examining whether the existing legal framework is sufficiently robust to prevent "algorithmic injustice." It argues that in the absence of specific safeguards—such as mandatory explanations and independent algorithmic auditing—the use of AI in courts could inadvertently weaken the constitutional guarantee of 'due process,' potentially transforming the accused from 'subjects of rights' into mere 'objects of data processing.'

1.2 *AI as a Tool in Modern Justice Systems*

To understand AI's impact, it is first necessary to understand what it means in a legal context. Broadly speaking, AI in the judiciary can be divided into two categories: assistive and adjudicative. Assistive AI includes tools like SUVAS (Supreme Court Legal Translation Software), which translates decisions, and legal research algorithms that help judges find relevant precedents. These are relatively harmless and are widely welcomed. They reduce the drudgery of judicial work, allowing judges to focus on substantive arguments. For example, a judge can now use AI to summarize thousands of pages of evidence in minutes—a task that previously took weeks.

However, when we move to adjudicative or predictive AI, the landscape changes dramatically. These are systems designed to assist in making decisions themselves. Examples include facial recognition software used by police to identify suspects from CCTV footage, or risk assessment tools that estimate the likelihood of a prisoner reoffending. From a practical perspective, the boundary between "assisting" and "deciding" often becomes blurred. If a judge receives a report prepared by AI showing a bail applicant's score as "High Risk" (High Risk), there is tremendous psychological pressure to make a decision in accordance with that "objective" number. This phenomenon is known as "automation bias," resulting in judicial discretion being effectively handed over to the machine.

ISSN: 2582-6433

Of course, the real danger lies in the fallible nature of these systems. A poignant example emerged in 2020 when Delhi Police used facial recognition technology during the investigation of riots. Reports surfaced that in some circumstances, the software's accuracy rate was less than 80%, and it struggled to distinguish between individuals with similar facial features. If such flawed technology is used as primary evidence to refuse bail or to charge a person, the consequences could be disastrous. An innocent person could languish in jail simply because an algorithm made a probabilistic error.

Moreover, AI tools are often like "black boxes." They reach conclusions through complex, multi-layered neural networks—a process that even their creators often cannot fully explain. In court, this can prove fatal to justice. How will a defense lawyer cross-examine an algorithm? How will a judge write a reasoned order if the logic behind the evidence is beyond understanding? Traditional accountability mechanisms— reasoned orders, cross-examination, and appellate review—fail when confronted with technology whose mechanism is opaque.

In plain terms, while AI can process data, it cannot understand its meaning. It can calculate probabilities, but it cannot weigh values. Justice is not an 'optimization' problem; it is a moral process. When we use AI in the realm of justice, we are not merely changing its tools; we are changing its 'architect.' The question is whether our constitutional structure can withstand this fundamental change without collapsing.

1.3 *The Constitutional Guarantee of Fair Hearing*

India's Constitution is not a static document; it is a living entity that evolves to meet the challenges of time. At its core lies Article 21, which guarantees that no person shall be deprived of his life or personal liberty except by procedure established by law. In the early years of the Republic, in cases like A.K. Gopalan v. State of Madras, the Supreme Court adopted a narrow interpretation, holding that any law so made satisfies this requirement. However, a major shift came with Menaka Gandhi v. Union of India, where the Court established that the procedure must be "fair, just and reasonable," not arbitrary, fanciful, or oppressive.

This "fairness" is not an abstract concept. It has concrete components: the presumption of innocence, the right to know the case against you, the right to cross-examine witnesses, and the right to a reasoned decision. Interestingly, AI poses a challenge to each of these components. The presumption of innocence is weakened by predictive policing algorithms that view

ISSN: 2582-6433

individuals as "risks" based on statistical profiles rather than actual conduct. The right to know is denied by proprietary algorithms protected by trade secret laws. The right to cross-examination becomes meaningless when the accuser is a piece of code.

One cannot ignore the tension between the efficiency offered by AI and the fairness demanded by Article 21. Efficiency is a utilitarian goal—the greatest good for the greatest number. Fairness is a duty-based goal—protecting individual rights even if it costs the system. The Indian Constitution clearly favors the latter (fairness). As Justice Krishna Iyer famously remarked, "The process of justice must be as fair as its outcome." If the process is tainted by opaque and biased technology, then the outcome, however efficient, will be constitutionally invalid.

Moreover, fair hearing is inseparably linked to the concept of "equality of arms." The state has vast resources to acquire advanced AI tools for surveillance and prosecution. An ordinary accused—often poor and marginalized—lacks even the ability to understand this technology, let alone challenge it. This creates an imbalance of power that violates Article 14 (equality before law). If the rich can hire forensic data experts to debunk AI evidence while the poor cannot, then the trial is no longer fair.

Therefore, in the 21st century, "procedure established by law" should include safeguards against technological arbitrariness. It is not enough for law to merely permit digital evidence; it must actively regulate it to ensure that the human dignity of the accused is protected. The Constitution stands as a strong shield against state oppression, and now it must also stand as a strong shield against algorithmic oppression.

1.4 *Scope of the Research Problem*

This research is specifically focused on the intersection of AI and criminal justice within the Indian legal framework. While AI applications exist in civil disputes and contract analysis, the stakes in criminal law— life and liberty—are far higher, and therefore constitutional scrutiny must be far stricter. Its scope is determined by the coming into force of the Indian Evidence Act (BSA), 2023, which is the primary law governing evidence.

The main problem this paper addresses is "regulatory vacuum." Although BSA recognizes electronic records (Sections 57 and 61), it treats them the same way as ordinary computer

ISSN: 2582-6433

printouts. It does not account for the 'generative' nature of modern AI. For example, "deepfakes"—highly realistic AI-generated videos—can now be created by anyone using their smartphone. If such a video is presented as evidence, there is no specific standard in current law for verifying its authenticity beyond a general certificate. Applying 20th-century evidence rules to 21st-century problems is inherently problematic.

This research deeply explores the specific risks associated with "algorithmic bias"—where AI tools merely reproduce social prejudices—and "algorithmic opacity." It does not address the technical engineering aspects of AI but focuses entirely on its legal, ethical, and constitutional implications.

Ultimately, the scope of this research extends to assessing whether the Indian judiciary is institutionally prepared for this change. This is not merely a question of law but also of capacity. Do our judges understand 'probability'? Do our lawyers know how to challenge data provenance? Thus, this research problem is multidimensional, encompassing statutory interpretation, constitutional theory, and institutional capacity.

1.5 *Objectives of the Study*

The primary objective of this research is to conduct a critical analysis of the constitutional validity of integrating Artificial Intelligence into the Indian criminal justice system, specifically examining its evaluation against the standard of "fair, just, and reasonable" procedure established under Article 21. Its purpose is to determine whether the use of 'opaque algorithms' in the judicial decision-making process is compatible with the principles of 'natural justice' or not.

Second, this study aims to conduct an extensive textual and structural analysis of the Indian Evidence Act, 2023. Its purpose is to identify specific deficiencies, ambiguities, and omissions in the new legislation relating to AI-generated evidence, authentication verification, and the admissibility of algorithmic outputs.

Third, this research attempts to explore the impact of AI on human rights, with special attention to the right to privacy (Article 21), the right against self-incrimination (Article 20(3)), and the right to equality (Article 14). Its purpose is to document how data-driven policing and sentencing processes can disproportionately affect marginalized communities.

ISSN: 2582-6433

Fourth, this study presents a comparative perspective, examining how other major jurisdictions— particularly the European Union, the United States, and the United Kingdom— are facing similar challenges. Its purpose is to identify global best practices that can be adapted to the Indian context.

Finally, its objective is to present concrete and actionable recommendations for legal and institutional reforms. This paper aims to propose a "rights-based AI framework" for the Indian judiciary that can balance the necessity of modernization with the imperative of protecting fundamental freedoms.

1.6 *Research Questions*

The first and most fundamental question of this research is: What impact does the use of Artificial Intelligence (AI) in judicial decision-making and evidence evaluation have on the core components of the 'right to fair hearing' under Article 21 of India's Constitution? This question explores the collision between algorithmic efficiency and constitutional 'due process,' particularly examining issues related to transparency and accountability.

The second question focuses on law: Does the Indian Evidence Act, 2023, provide an adequate legal framework for addressing the unique challenges posed by AI-generated evidence (such as deepfakes, algorithmic bias, and "black-box" opacity)? Its purpose is to assess whether the legislative modernization intent has translated into effective legal safeguards.

The third question looks outward to external sources for solutions: What regulatory models and judicial standards can India adopt from international jurisdictions to ensure that the incorporation of AI into courts does not compromise human rights and the 'rule of law'? This question aims to bridge the gap between global developments and domestic requirements.

1.7 *Hypothesis*

This research is based on the hypothesis that the current legal framework—primarily the Indian Evidence Act, 2023—is structurally insufficient to protect the 'right to fair hearing' in the age of Artificial Intelligence. Although the Act represents an important step in recognizing digital evidence, it maintains a "hardware-centric" approach while failing to address the "software-centric" risks associated with AI (such as bias, hallucination, and opacity).

ISSN: 2582-6433

This hypothesis assumes that without specific legal amendments—such as mandatory 'explainability audits' and restrictions on 'black-box algorithms' in criminal trials—AI use will gradually erode the rights of 'due process,' creating a system where 'regularity presumption' (which courts currently apply to official actions) becomes dangerously applied to algorithmic outputs as well, resulting in a system where the machine's word is final.

Moreover, this hypothesis suggests that without legislative support, managing these risks through judicial interpretation alone (under Article 21) will be insufficient. While courts can strike down state arbitrariness, they cannot unilaterally create complex technical regulations from the bench. Thus, a vacuum exists that legislative inaction is deepening.

1.8 *Research Methodology*

This research paper employs a qualitative and theoretical legal research methodology. It relies primarily on intensive textual analysis of primary legal sources: the Constitution of India, the Indian Evidence Act 2023, the Information Technology Act 2000, and the now-repealed Indian Evidence Act 1872. Landmark decisions of India's Supreme Court form the backbone of constitutional analysis.

Secondary sources include academic journals, Law Commission reports (particularly the 269th Report), technical research papers on AI ethics, and international policy documents such as the EU AI Act. The research adopts an interdisciplinary approach, integrating insights from computer science (how AI works) with legal theory (how justice works).

A comparative methodology is employed to benchmark Indian laws against international standards. The analysis is explanatory and critical, aimed at exposing hidden assumptions underlying the law.

The limitation of this study is that, as BSA 2023 is new, there is little direct case law interpreting it specifically in the context of AI; therefore, this analysis is predictive and norm-setting in nature, based on established constitutional principles.

Given the preliminary stage of AI adoption in Indian courts, this research avoids empirical data collection (surveys) and instead focuses on theoretical legal arguments that will shape future litigation.

ISSN: 2582-6433

1.9 *Division of Chapters*

This study is organized into eleven coherent chapters. Following this 'Introduction,' Chapter 2 establishes the theoretical foundation by analyzing the 'right to fair hearing' under Article 21. Chapter 3 provides historical context, tracing the evolution of 'evidence law in India' from 1872 to 2023.

Chapter 4 demystifies technology and clarifies how 'Artificial Intelligence' operates in the justice system. Chapter 5 presents a critical statutory analysis of the Indian Evidence Act, 2023, focusing specifically on 'digital evidence.' Chapters 6 and 7 form the analytical heart of this study, exploring 'human rights impacts' and 'challenges in ensuring objectivity' respectively. Chapter 8 expands the study's horizon through 'comparative perspectives.' Chapter 9 synthesizes findings to evaluate BSA from a constitutional perspective. Chapter 10 outlines detailed recommendations, and Chapter 11 concludes with a vision for the future.

CHAPTER 2: THE RIGHT TO FAIR HEARING UNDER ARTICLE 21

2.1 *Meaning of Fair Hearing*

"Fair hearing" is the golden thread woven throughout the entire fabric of criminal jurisprudence. Philosophically, it expresses the state's moral commitment that even the most despised criminal will be treated with dignity and procedural justice. It is not merely technical compliance with rules but a concrete guarantee that justice will be delivered without fear or bias. In the 'adversarial system' adopted by India, fairness operates on the assumption that truth emerges best when two opposing parties present their respective positions before a neutral arbiter. However, this requires a 'level playing field.' If one party is equipped with opaque, high-tech tools that the other party cannot understand, the very foundation of this adversarial contest collapses.

Unlike civil suits, where money is usually at stake, criminal trials involve the loss of life and liberty. Therefore, the standard of fairness here is much higher. This parallels Article 14 of the International Covenant on Civil and Political Rights (ICCPR), to which India is a signatory. Fairness, a core element of which, has traditionally meant that a judge has no personal interest in the trial's outcome. However, in this age of AI, a new dimension of fairness has emerged: the fairness of the tools being used. If an algorithm used to assess evidence contains pre-existing bias against a particular community, that hearing cannot be deemed fair, even if the

ISSN: 2582-6433

human judge is personally impartial.

It must also be noted that fairness is both procedural and substantive. Procedural fairness demands that steps taken—such as arrest, bail, evidence gathering, and hearing—comply with law. Substantive fairness demands that the law itself be just. As we integrate AI into our systems, we must ask: Is it just to subject a person to a mathematical model that cannot understand empathy or context? Fairness in this age is expanding; it now includes the right that decisions be made by a human, that compassion be applied during hearing, and that individual justice be ensured rather than statistical profiling. In plain terms, a fair hearing is a shield against the state's monopoly on violence. It ensures that the overwhelming power of prosecution is checked by the rights of the accused. When AI enters the courtroom, it often—through surveillance and data mining—strengthens the state's hand, tilting justice's scales even further to one side. Therefore, redefining fair hearing in the algorithmic age is an urgent necessity.

Ultimately, the legitimacy of the justice system rests on public trust. If the public believes that trial outcomes are determined by secret code and incomprehensible machines, the moral authority of courts weakens. Fairness means not just reaching the right outcome but transparency in the entire process of reaching that outcome.

2.2 *Constitutional Foundation and Judicial Interpretation*

India's journey toward the right to fair hearing under Article 21 is a fascinating story of judicial development. In the early 1950s, in A.K. Gopalan v. State of Madras, the Supreme Court adopted a strict and positivist approach. The Court held that "procedure established by law" in Article 21 meant any law made by the legislature, however arbitrary. This meant the state had complete freedom to make unjust laws. For decades, this approach dominated, restricting judicial review of procedural laws.

A revolution came in 1978 with Menaka Gandhi v. Union of India. A seven-judge bench threw open the doors of Article 21, ruling that the procedure must be "fair, just, and reasonable." The Court also established the "Golden Triangle" rule, stating that Articles 14 (equality), 19 (liberties), and 21 (life and liberty) are not isolated rights but interconnected. Any law curtailing liberty must not only follow procedure (Article 21) but also be non-arbitrary (Article 14) and reasonable (Article 19). This decision transformed Article 21 into a source of "substantive due process."

ISSN: 2582-6433

Since then, the judiciary has adopted a "living constitution" approach, continuously reading new rights into Article 21. Legal aid rights, rights to speedy trial, rights against handcuffing, and privacy rights—all have emerged from this rich foundation. This expansive interpretation suggests that any new technology introduced into the justice system must meet the strict standard set by Menaka Gandhi. For BSA 2023, merely permitting AI evidence is not enough; the manner of its admission must also be fair and reasonable.

Notably, whenever technology has posed threats to rights, courts have intervened. In Selvi v. State of Karnataka, the Court invalidated narco-analysis (truth serum) without consent, ruling that scientific efficacy cannot override constitutional liberty. This precedent directly applies to AI. Just as the state cannot force anyone to take a truth serum, it cannot subject them to aggressive AI profiling that estimates behavior from data.

The constitutional foundation is thus strong. The challenge lies in applying these broad principles to the specific, subtle issues raised by AI.

2.3 *Components of Fair Hearing*

Fair hearing comprises several distinct but interconnected components. The first and most important is **presumption of innocence**. This fundamental principle is that an accused is innocent until proven guilty beyond reasonable doubt.

AI risk assessment tools, which predict future crime based on historical data, fundamentally weaken this principle. They label individuals as "high risk" or "dangerous" before trial's end, creating judicial prejudice. This indirectly shifts the burden of proof onto the accused to prove they are not a risk. The second component is **right of disclosure**. The prosecution is legally bound to share all evidence with the defense. However, in AI cases, companies often claim their algorithms are "trade secrets" and refuse source code disclosure. If the defense cannot see the evidence (algorithm) used against it, the right of disclosure is violated.

The third foundation is **right to cross-examination**. Cross-examination is considered the greatest tool ever devised for finding truth. However, a software program cannot be cross-examined. If an AI identifies a suspect from blurry video, the defense lawyer cannot ask the AI, "Are you certain? Was the lighting dim? Do you have bias regarding this skin tone?"

ISSN: 2582-6433

The fourth right is **reasoned decision-making**. Judges must explain their orders so higher courts can review them. If a judge relies on an AI score saying "70% probability of guilt" without explaining why the AI reached this conclusion, the decision is without reasoning. This breaks the chain of judicial accountability.

Finally comes **equality of arms** (equality of arms). This principle requires that the defense have procedurally equal opportunity to present its case. Given expensive and complex AI tools, the government usually has a huge advantage. Until the government funds the defense to hire its own AI experts to scrutinize prosecution tools, both sides' "weapons" remain unequal, and the trial unfair.

2.4 *Fair Hearing and Natural Justice*

Natural justice serves as the moral soul of law. Its first principle, *nemo judex in causa sua* (no one should be judge in their own case), ensures impartiality. While an AI algorithm has no personal agenda, it may contain "coded bias." If an algorithm is trained on police data that has historically targeted a particular minority community, it will learn and reproduce that same bias. Thus, it becomes a digitally-biased "judge." This bias is treacherously deceptive because it is hidden behind mathematical "impartiality."

The second principle, *audi alteram partem* (hear the other side), guarantees the right to hearing. But any hearing is meaningless unless it is effective. If an accused faces AI evidence they cannot understand or challenge, their hearing right becomes a joke. They are speaking to a system that is completely deaf to their specific circumstances or context.

Consider a real-world example: A person applying for bail is denied release because an AI tool rates them "flight risk" based on zip code and credit history. The applicant wants to explain that their poor credit resulted not from carelessness but from a medical emergency. But AI, a rigid mathematical model, may have no "medical emergency" variable. Human sensitivity and nuance are completely ignored. The "hearing" this person receives from the machine is incomplete and inadequate.

The real danger is the "technological veil" that AI casts over injustice. Because the output comes from a computer, we often assume it is perfectly fair and correct. This makes it even harder to argue that natural justice has been violated. This violation is completely silent,

ISSN: 2582-6433

invisible, and hidden within code.

2.5 *Judicial Expansion of Fair Hearing Rights*

The Indian Supreme Court has a glorious history of expanding human rights' scope. In Hussainara Khatoon v. Home Secretary, Bihar, the Court declared that "right to speedy trial" (not explicitly mentioned in the Constitution) is an integral part of Article 21. This precedent is often cited to justify using AI to speed court proceedings. However, the Court also warned that speed cannot come at justice's cost.

In D.K. Basu v. State of West Bengal, recognizing the accused's vulnerability in police custody, the Court set guidelines to prevent torture. Today, "digital custody"—where a person's data is seized and analyzed— poses similar vulnerability risks. D.K. Basu's principles on transparency and legal access must be adapted to digital inquiry.

In Tomaso Bruno v. State of Uttar Pradesh, the Court emphasized scientific evidence's importance but said its authenticity must be strictly proven. The judiciary has shown readiness for new challenges. In K.S. Puttaswamy v. Union of India, the Court recognized privacy as a fundamental right. This directly impacts AI, which depends on massive personal data collection. This expansionist vision suggests courts will eventually include "protection from algorithmic bias" within Article 21.

The direction is clear: courts see the Constitution as a shield for citizens. As government acquires new technological swords, courts expand that shield. The next logical step would be recognizing that no trial can be fair when evidence comes from an impenetrable "black box."

2.6 *Evidence's Role in Ensuring Fairness*

Evidence is the currency of courts. A trial's fairness entirely depends on this currency's integrity. If evidence is fake—manipulated, forged, or biased—the judgment is worthless. In the analog world, we had physical seals and locks to protect evidence. In the digital world, protecting evidence is far harder. Digital files can be altered without visible marks.

The Supreme Court acknowledged this weakness in Anwar P.V. v. P.K. Bashir, striking down loose standards from the earlier Navjot Sandhu case. The Court ruled that for electronic records to be admissible, they must carry a certificate under Section 65B (now BSA's Section 63) of

ISSN: 2582-6433

the Evidence Act, ensuring source authenticity.

However, with AI, the challenge's nature changes. The issue is not just whether the file was tampered with (integrity) but whether it was reliably created (validity). A deepfake video is a completely "intact" file, but its content is false. Now, chain of custody must extend to the algorithm itself: Who trained it? What data was used? Has it been audited?

Fairness demands that the defense have the right to examine this digital chain of custody. If the prosecution presents AI-enhanced video, they must not only prove where the file came from but explain precisely what AI did to it. Without this fine transparency, evidence becomes a weapon of deception rather than truth.

2.7 *Connection with Articles 14 and 20(3)*

Article 14 guarantees equality before law and equal protection of laws. It is the Constitution's enemy of arbitrariness. If AI systems are not carefully designed, they become machines promoting inequality. They often perform poorly on minority populations. For example, facial recognition systems have higher error rates for women and people with dark skin. Using such tools in court denies those groups equal protection, putting them at higher risk of wrongful conviction merely due to their identity. This is clear Article 14 violation.

Article 20(3) provides that no accused person can be forced to give evidence against themselves. This is the right against self-incrimination. In the physical world, we know what this means: you cannot beat someone into confessing. But in AI's digital world, these lines blur. AI tools analyzing micro-expressions, voice tremors, or gait to estimate 'guilt suspicion' are effectively extracting testimony from the accused's body without consent.

In Selvi, the Supreme Court held that 'mental privacy' is part of Article 20(3). AI tools attempting to "look into" someone's mind—estimating intent or deception—violate this 'mental sanctuary.' If the state uses AI analyzing my social media history to "estimate" my criminal mindset, it is extracting testimony from my own data in ways I never imagined.

This Articles' combination creates a 'multi-headed constitutional danger.' One AI tool can simultaneously violate privacy (Article 21), equality (Article 14), and self-incrimination rights (Article 20(3)). This is a 'multi-headed hydra' requiring multi-dimensional constitutional

ISSN: 2582-6433

response.

2.8 *Impact of Technical Intervention on Fair Hearing*

We are witnessing the birth of a new legal concept: "technological due process." This refers to specific rights citizens need to protect themselves from technology used by the state. Technology's intervention in hearing undermines fairness. It shifts power balance. The state has budgets to buy latest AI surveillance and forensics, while the accused usually doesn't. This technical inequality poses the danger of rendering the "presumption of innocence" obsolete. When a computer says someone is guilty, we instinctively believe it. This "automation bias" is powerful psychological force judges must actively resist. Otherwise, hearing becomes mere rubber-stamping.

Richard Susskind argues in "Online Courts and the Future of Justice" that we must distinguish between "automating" old processes and "transforming" them. If we merely automate old inefficiencies and biases, we get faster injustice. Our goal should be transformation—using technology not just to speed up but to enhance fairness.

Ultimately, technology makes justice less transparent. The principle of "open court"—that justice must appear to be done—is endangered when justice's logic moves from court's open environment into server's silicon chips. We must struggle to keep justice's reasoning human, visible, and accountable.

CHAPTER 3: EVOLUTION OF EVIDENCE LAW IN INDIA

3.1 *Colonial Origins: The Indian Evidence Act, 1872*

The 1872 Indian Evidence Act stands as a vast testament to Victorian legislative craftsmanship. Primarily drafted by Sir James Fitzjames Stephen, it was enacted when British Raj sought to codify the diverse and often chaotic evidence practices of colonial India. Stephen, a utilitarian philosopher and judge, attempted to create a system based on logic, precision, and prediction. The Act substantially embodied the essence of English common law evidence, adapted for Indian context.

The Act's merit lay in its definitions. It defined "fact," "relevant," and "proved" with mathematical precision. At its core was distrust of hearsay and priority for direct, primary

ISSN: 2582-6433

evidence. Legislative intent was to prevent juries (which existed in India until the Naniata case of 1959) from being swayed by unreliable gossip or prejudice. It was law designed for a world of paper documents, inked signatures, and eyewitnesses.

For over a century, this Act served India extraordinarily well. Its structure was flexible enough to accommodate telephone, photography, and tape recording. Judges used its principles to guide India's transition from feudal to democratic republic. However, the Act was fundamentally 'analog' (physical) in nature. It assumed a "document" was a physical object that could be brought to court, examined, and safeguarded.

The definition of "document" in Section 3 was broad—"anything expressed or described on any material"—but implicitly assumed a tangible (physical) base. The idea that information could exist in intangible form as 'bits and bytes' that could exist simultaneously in two different places was completely foreign to 19th-century thinking. This conceptual limitation ultimately became the Act's 'Achilles' heel' in the digital age. Yet, we must acknowledge that the 1872 Act established those fundamental principles— relevance, admissibility, burden of proof—that still form our system's foundation. We are not rejecting Stephen's reasoning; we struggle to apply it to a reality he could never have imagined.

3.2 *Structure and Philosophy of the 1872 Act*

The 1872 Act is structurally divided into three main parts: relevance of facts, evidence, and presentation and effect of evidence. This three-tier structure provides logical flowchart for any trial.

First, the court determines which facts are relevant (Part I). Then it asks how those facts should be proven (Part II). Finally, it decides who will prove them and how much importance to give them (Part III).

A key philosophical pillar was distinction between **primary evidence** (the document itself) and **secondary evidence** (copies, certified copies). Section 64 famously mandated that "documents shall be proved by primary evidence, except in cases hereinafter mentioned." This was safeguard against forgery. If you want to prove a contract, bring the original contract. Copies were viewed with suspicion.

ISSN: 2582-6433

Another pillar was **exclusion of hearsay evidence**. The Act generally barred reporting what someone else said, demanding that the original speaker be present in court. This ensured cross-examination. Some exceptions existed, such as dying declarations (Section 32), based on principle that *nemo moriturus praesumitur mentiri* (no one goes to their maker with lies on their lips).

Section 45 addressed **expert opinions**. It allowed courts to rely on persons skilled in foreign law, science, or art. This became the gateway for forensic science—fingerprints, ballistics, DNA. Yet, the Act viewed experts as human witnesses offering opinions, not machines merely giving outputs.

The limits of Victorian legal thinking were that it assumed truth was singular and discoverable through logical inquiry. It did not account for digital truth's mutability. Its philosophy was: "What you see is what is true." In this age of deepfakes, "what you see is true" no longer applies.

3.3 *Judicial Interpretation Over Decades*

As India modernized, courts had to expand the 1872 Act's scope to include new inventions. When tape recorders arrived, in R.M. Malkani v. State of Maharashtra (1973), the Supreme Court ruled that if voice could be identified and the tape was untampered, recordings could be accepted as "documents." This was practical expansion.

Courts also developed rich jurisprudence on circumstantial evidence. Where no eyewitness existed, in Sharad Birdichand Sarda v. State of Maharashtra, courts established the "chain of circumstances" principle: this chain must be so complete that no doubt remains. This logic is highly relevant to AI, which fundamentally generates circumstantial evidence from patterns.

On expert evidence, courts clarified that an expert's opinion is merely corroborative, not conclusive. Final decision-making rests with the judge. Today, this principle is crucial: a person should not be convicted solely on an AI report. It should be used only as supporting evidence.

A historic principle held that procedural rules are handmaidens of justice, not mistresses. If evidence was genuine, courts would overlook technical errors. Yet, this generous approach reversed for electronic records; because electronic records' authenticity depends on strict technical compliance.

ISSN: 2582-6433

3.4 *Digital Age Limitations*

By the late 1990s, the internet revolution made clear that the 1872 Act was inadequate. Emails, server logs, and digital chats became central to crime and commerce. In the digital context, the Act's emphasis on "primary evidence" seemed irrational. What is an email's "original"? The server copy? The sender's laptop copy? The recipient's phone copy?

To solve this, Parliament passed the "Information Technology Act, 2000," adding Sections 65A and 65B to the Evidence Act. Section 65B created a special procedure for electronic records, allowing "computer output" to be accepted as evidence without presenting the actual computer, provided an authenticity certificate was given.

However, confusion lasted a decade. In Navjot Sandhu (Parliament attack case), the Supreme Court ruled that even without certificate, electronic evidence could be accepted under secondary evidence rules. This loose approach was data integrity's disaster, allowing tampered printouts easy evidence acceptance.

Improvement came with Anwar P.V. v. P.K. Bashir (2014), where a three-judge bench overturned Navjot Sandhu. The bench stated Section 65B is complete in itself. Without certificate, electronic evidence is wholly inadmissible. This restored some order. Yet, even Anwar P.V. emphasized *file integrity* (tampering), not *content validity* (AI-generated content). An AI report might be untampered but false.

3.5 *Legislative Reform Efforts*

Debate on a new Evidence Act lasted years. India's Law Commission recommended modernizations in its 185th Report. Later, the 269th Report focused on DNA technology, emphasizing scientific standards. But suggestions came piecemeal.

Parliamentary debates repeatedly surfaced that old rules were causing criminal cases to fail. Conviction rates were falling. "Best evidence rule" became obstacle in a world where best evidence often sat in some "cloud." Strong demands also arose to "decolonize" the legal system. The 1872 Act was viewed as colonial relic. Government wanted laws reflecting Indian customs and modern realities. This political will, combined with technical need, paved the way for new Criminal Codes.

ISSN: 2582-6433

Thus, the Indian Evidence Act, 2023, resulted from decades of reform thinking.

3.6 *Introduction to the Indian Evidence Act, 2023*

The Indian Evidence Act (BSA) 2023 is not merely a name change; it is a reorganization. Although it retains the 1872 Act's core elements (relevance, evidence, burden), it broadly expands definitions. Section 2(1)(d)'s definition of "document" now explicitly includes "electronic and digital records." This small change represents major conceptual shift.

The Act grants electronic records primary evidence status in many cases. Section 57 states that where a digital file is stored, it is a document. This removes "proving the copy's" conceptual barrier. "Certificate requirement" under Section 63 (replacing old Section 65B) makes electronic evidence acceptance easier, reducing procedural barriers to genuine evidence.

Key new sections include Section 61 (electronic record acceptability) and Section 63 (acceptability conditions). Certificate requirement remains but is streamlined. Anwar P.V.'s strict reading likely persists. What remains unchanged is AI silence. BSA is great for internet-age issues (email, chat) but perhaps unprepared for AI-age issues (deepfakes, algorithms).

BSA provides strong platform but needs plugins. It gives legal framework but judiciary must breathe life into it to address AI's specific challenges.

3.7 *Summary Assessment*

The journey from 1872 to 2023 shows both progress and persistent gaps. The 1872 Act was entirely paper- based. The new BSA accepts digital records as normal rather than exceptional. This is legislative thinking's vast leap.

Yet, what changed is mostly formal. Evidence law's concepts—relevance, admissibility, weight—remain same. BSA asks same questions as 1872 Act, merely in digital form. It doesn't introduce new fundamentally needed epistemological categories like "algorithmic creation" or "synthetic evidence."

The 1872 Act had privilege of handling a world where forgery was physically visible. AI's world, deepfakes appear completely genuine. Thus law must be more intervening, more demanding of evidence, more skeptical of technology. BSA is less skeptical than 1872, having

ISSN: 2582-6433

relaxed admissibility processes. In AI context, this simplification is dangerous.

Ultimately, this comparison highlights a missed legislative opportunity. BSA could have introduced provisions that mandatory "algorithmic impact assessments" precede any AI tool use in evidence gathering. It could have created dedicated chapter on "synthetic and AI-generated evidence" with higher standards. It didn't. BSA shows best of what we knew in 2021, not best of what we need in 2023.

CHAPTER 4: ARTIFICIAL INTELLIGENCE IN THE JUSTICE SYSTEM

4.1 *What is Artificial Intelligence?*

For lawyers, Artificial Intelligence often seems like science fiction—machines that "think." However, if we remove the hype, AI is essentially advanced statistics used at scale. It is a branch of computer science focused on creating systems capable of performing tasks that normally require human intelligence. These tasks include speech recognition, decision-making, language translation, and pattern recognition. Most importantly, AI is not a single technology but a collection of diverse tools.

The most relevant form of AI for the legal field is **Machine Learning (ML)**. Unlike traditional software, where a human programmer writes explicit rules (if X happens, do Y), ML systems are given large amounts of data and "learn" rules themselves. They discover correlations that humans might miss. For example, an ML model can analyze thousands of bail orders and "learn" the reasons prisoners are released.

A sub-category of ML is **Deep Learning**, which uses "neural networks" inspired by the human brain. These are multiple layers of computational nodes. Facial recognition and natural language processing rely on deep learning. Deep learning has one problem: its opacity—even its creators often cannot fully explain how a neural network reached a specific conclusion. This is called the "black box" problem.

Another crucial concept is **Generative AI** (like ChatGPT or Deepfake tools). These systems can create new content—text, images, videos—that appear completely authentic. In court, this is dangerous because it challenges the basic assumption that evidence is a record of reality.

ISSN: 2582-6433

Why is this legally important? Because lawyers and judges cannot afford to be technologically illiterate anymore. If an algorithm is determining your client's future, you must understand how it works to defend them. AI is not merely a tool; it is new legal agency.

4.2 *Types of AI Tools Used in Legal and Judicial Contexts*

Rule-Based Expert Systems: These are simplest forms, working like decision trees. "If income is below X and crime is Y, then legal aid is available." These are transparent and easy to audit. Many e-filing systems use this logic. They are safe and helpful.

Predictive Analytics: These are ML tools predicting outcomes. Lawyers use these to estimate case- winning chances ("litigation analytics"). Some courts use them to estimate prisoner recidivism risk. These are riskier because they rely on potentially biased historical data.

Natural Language Processing (NLP): This allows computers to understand and generate human language. SUVAS translates decisions. Other tools use NLP for "technology-assisted review" (TAR) in discovery, helping lawyers search millions of emails for evidence. These can be both helpful and problematic.

Computer Vision: AI "sees" images. It is used in forensics to match fingerprints, analyze CCTV to identify faces, or read license plates. The risk here is error—mistaking shadow for weapon, or misidentifying faces.

The spectrum ranges from helpful (translation, search) to dangerous (sentencing algorithms, lie detection). The justice system should adopt former while strictly regulating latter.

4.3 *AI in Policing and Pre-Trial Stages*

AI's most aggressive use currently happens with police. **Facial Recognition Technology (FRT)** is deployed in Indian cities under 'Safe City' projects. During 2019-20 protests, Delhi Police faced controversy using FRT to identify demonstrators. Critics noted high error rates and argued it was suppressing dissent. This is pre-trial AI determining who gets arrested.

Predictive Policing is another emerging field. Police use historical crime data to predict where crimes will occur ("hotspot policing") or who will commit them ("person-based predictive policing"). In India, CCTNS (Crime and Criminal Tracking Network and System) creates

ISSN: 2582-6433

massive database potentially feeding such algorithms. The danger is a "feedback loop": if police historically patrol poor areas more, they find more crime there; then AI uses this data justifying more patrols in same areas.

Bail Risk Assessment: Pre-trial, judges decide bail. Tools like PSA (Public Safety Assessment) give "risk scores." While not formally used in India, pending case backlogs make such tools attractive. But imprisoning someone based merely on a "score" represents fundamental shift in due process.

These tools operate often without judicial oversight, under broad legal authority. They affect "privacy rights" before cases reach courts. AI has already shaped the entire narrative before formal proceedings.

4.4 *AI Within Courtroom Proceedings*

Inside Indian courtrooms, AI remains assistive, not adjudicative. The Supreme Court's **SUPACE** portal processes facts and makes them available to judges. It does not decide. The Chief Justice repeatedly clarified AI will not replace human judges.

SUVAS translates decisions into regional languages, empowering non-English speakers to understand why they won or lost. This is excellent AI use. **e-Courts** digitizes records, preparing data infrastructure for future AI. However, we also see "deepfake" evidence entering courts. In family courts, manipulated audio is common. Criminal trials face manipulated video threats.

Indian tools are mostly administrative. But the sector advances. Soon, AI might suggest draft orders or calculate maintenance amounts. "Judge's assistant" can silently become "judge's guide."

4.5 *AI for Sentencing and Risk Assessment*

AI's most controversial use is sentencing. **COMPAS** (Correctional Offender Management Profiling for Alternative Sanctions) is a proprietary algorithm giving 1-10 risk scores. ProPublica investigation found COMPAS was biased. It falsely identified Black defendants as future criminals at double the rate of White defendants with identical histories. Yet judges used these scores for sentencing. This is "algorithm-based discrimination."

ISSN: 2582-6433

In State v. Loomis, Wisconsin Supreme Court allowed COMPAS use but with warnings. Defendant Eric Loomis challenged it, saying he couldn't cross-examine an algorithm. The court rejected his plea but acknowledged tool limitations.

Legally, "predicting recidivism" is risky. It punishes someone not for what they did but what a computer thinks they *might* do. This violates fundamental retribution principle—punishment must match actual crime, not risk.

India should learn from Loomis. Before adopting such tools to solve jail overcrowding, we must rigorously test for bias. We cannot import America's prejudices; we have our own (caste, religion) that any Indian AI will certainly learn.

4.6 *Global Trends in AI-Assisted Justice*

China leads with "internet courts" in Hangzhou, Beijing, and Guangzhou. "AI judges" (avatars) handle business and copyright disputes, claiming high efficiency. Critics point to lack of due process and prioritizing social control over individual rights.

Estonia develops a "robot judge" for small claims under €7,000. This aims to clear backlog so human judges focus on complex cases. This is bureaucratic model of justice.

EU adopted rights-prioritizing approach. The EU AI Act restricts some "high-risk" AI uses and strictly regulates others. It emphasizes "human-in-the-loop"—AI decisions must be reviewable by humans.

India stands at crossroads. We can choose China's efficiency model or EU's rights-conscious model. Given constitutional values, choice should be clear. We need efficiency but not at our democratic soul's cost.

CHAPTER 5: INDIAN EVIDENCE ACT, 2023 – AI- GENERATED EVIDENCE AND DIGITAL PROOF

5.1 *Overview of BSA 2023*

The Indian Evidence Act (BSA), 2023, was drafted with goal of liberating India's criminal justice from colonial influence and modernizing it. It repeals the 1872 Act, a British Raj remnant. Legislative intent clearly was addressing the "technical gap" that had grown. The

ISSN: 2582-6433

Home Minister emphasized this would redefine electronic evidence for contemporary needs.

Structurally, BSA maintains familiar framework—definitions, relevance, evidence, burden. This continuity is double-edged sword. It provides professional stability but carries analog-era logic forward. Main changes are in definitions. "Document" and "evidence" now include electronic records as default category, not exception.

Policy objective was easing digital evidence acceptance. Under old law (Section 65B), procedural barriers often rejected genuine evidence. BSA aims to streamline this. However, it prioritizes "admissibility" over "reliability." It opens doors to digital evidence widely but doesn't install necessary filters for fake or AI- manipulated content.

In summary, BSA is "Digital 2.0" world's "Digital 1.0" law. It solves email-era problems (integrity, storage) but hardly addresses AI-era problems (creation, hallucination). Forward step, perhaps, but not large leap.

5.2 *Recognition of Electronic Records as Evidence*

BSA's Section 57 is this new framework's cornerstone. It explicitly states that "documents" include electronic records. This means digital files are no longer mere "copies" of reality; legally, they are reality themselves. Law acknowledges that many documents are "born digital"—they never existed on paper.

For "primary evidence," implications are profound. Traditionally, primary evidence was paper's physical form. Now, Section 57 means digital file on server or cloud is primary evidence. This aligns law with technology. It solves the "cloud problem"—if data is spread across ten servers, which is "original"? BSA says: the record itself is document.

The word "custodian" becomes crucial. Who possesses electronic record? Today, "Big Tech" companies (like Google, Meta). BSA grants courts power to summon these records. However, when servers are abroad, jurisdiction issues arise. BSA doesn't fully solve this.

Courts' likely approach will be positive but cautious. Courts have long wrestled with Section 65B's "certificate regime." BSA eases this but judges will be more cautious about records' *source*. Having AI process records is one thing; completely trusting results is another.

ISSN: 2582-6433

5.3 *Admissibility of AI-Generated Documents*

Here we encounter first major problem. "AI-generated document" is what? Could be speech-to-text transcript made by AI, video enhanced by AI, or entirely synthetic image (deepfake). Under Section 2(1)(t)'s broad "electronic record" definition and Section 61's admissibility, technically all qualify as evidence.

But problem is BSA treats these as "records" of facts. Generative AI does not merely *record*; it *creates*. A deepfake video of crime never occurring is "electronic record" of fictional event. If admitted without scrutiny under Section 61, an innocent person could be wrongly convicted. There is no law category for "synthetic media."

Present legal response relies on forensic experts challenging such evidence. But this is "cat and mouse game." AI generators outpace AI detectors. BSA places no extra burden on party presenting AI evidence to show it is trustworthy. It treats deepfake video like CCTV recording equally at procedural level.

Automated reports—like AI-generated forensic analysis—are also acceptable. But if software has bug, its "evidence" is flawed. BSA is silent on "algorithmic authorship." Who authored AI poetry or AI-written threat letter? The prompter? The coder? AI itself? Law is silent.

5.4 *Authentication Requirements Under BSA*

BSA's Section 63 is new avatar of notorious Section 65B. It sets conditions for evidence acceptability. It requires certificate from person in charge of computer system, confirming system worked properly and data reproduction is authentic.

This requirement was designed for deterministic systems—databases, email, accounting software. These follow principle: input 'A' always gives output 'B' if system works. If computer functions properly, output is reliable. But neural networks are *non-deterministic* (probabilistic). "High" risk score might be prediction, not fact. System working "properly" doesn't guarantee truthful output. It can "hallucinate" (generate false information). Certificate can certify *container* (computer works) but not *content* (AI's truthfulness).

AI evolves constantly. January's ML model differs from June's model after learning new data. Which version is certificate authenticating? "Evolving algorithms" problem makes simple

ISSN: 2582-6433

certificate obsolete.

For AI evidence, Section 63 needs amendment or special rule. There should be mandatory "algorithmic audit certificate"—certifying not just uptime but accuracy, error rates, and bias metrics.

5.5 *AI Evidence and Certificate Requirements*

The gap between hardware certification and software validity is where AI evidence cases get stuck. System administrator can honestly sign Section 63 certificate saying "server ran perfectly" while AI software on that server runs biased algorithm. This certificate falsely suggests AI output is trustworthy.

Who can certify AI honesty? Surely not ordinary IT officer at police station. It requires data scientist. But BSA doesn't require "expert certificate" for advanced algorithms. It accepts general certificate.

Additionally, "evolving algorithms" issue: January model trained on data differs from June model. Certificate certifies which version? "AI's moving target" nature makes static certification outdated.

For proper AI evidence handling, Section 63 needs amendment or specific rule. A "algorithmic audit certificate" should be mandatory—certifying not mere hardware working but accuracy, error rates, bias metrics.

5.6 *AI Evidence Deficiencies and Ambiguities in BSA*

BSA's largest deficiency is lack of "explainability requirement." When AI evidence is presented, prosecution has no pressure to explain how algorithm reached conclusion. Court can accept facial recognition match without knowing software has 15% error rate for South Asian faces. Present law demands only that hardware functioned; it doesn't demand intelligence is trustworthy.

Additionally, no standard exists for reliability or accuracy. In America, Daubert v. Merrell Dow Pharmaceuticals standard requires scientific evidence be testable, peer-reviewed, and generally accepted by scientific community. India's AI tools have no such legal requirement. AI product

ISSN: 2582-6433

rejected globally might be accepted in Indian court if it has Section 63 certificate.

Deepfake problem is especially grave. BSA doesn't define "synthetic media" and sets no high standard for AI-created content. It doesn't clarify whose burden it is proving whether video is real or AI-created. Given technology's current state—where AI detectors are often less accurate than AI generators—this ambiguity is catastrophic.

"Algorithmic tampering" concept is absent. Traditional tampering means file alteration. But AI evidence can be "tampered with" during training phase—fed biased or selective data—without final output file being touched. Certificate checking "integrity" might pass while evidence is fundamentally poisoned. BSA's "chain of custody" doesn't extend this far back.

Finally, law is silent on AI-generated text and automated forensic reports. Many labs use software auto- generating analysis reports. If software's database is flawed, report is flawed. BSA gives such reports same deference as expert opinion, without requiring statistical validation. This is accepting "expert system output" as expert testimony without asking whether system is actually expert.

5.7 *Comparison with Indian Evidence Act 1872*

Comparing BSA with 1872 Act illuminates progress and remaining gaps. The 1872 Act was entirely paper-based. BSA treats digital records as normal. This is massive shift in legislative thinking.

However, changes are mostly formal. Evidence law's foundational concepts—relevance, admissibility, weight—remain identical. BSA asks same questions as 1872, merely in digital form. It doesn't introduce fundamentally necessary new epistemological categories like "algorithmic creation" or "synthetic evidence."

1872 Act had advantage that forgery was physically visible. AI's world, deepfakes appear entirely genuine. Law must be more intervening, more demanding of evidence, more skeptical of technology. BSA is *less* skeptical than 1872, having relaxed admissibility processes. In AI context, this simplification is dangerous.

Ultimately, this comparison reveals missed legislative opportunity. BSA makers could have

ISSN: 2582-6433

introduced provisions mandating "algorithmic impact assessments" before any AI tool's use in evidence gathering. They could have created dedicated chapter on "synthetic and AI-generated evidence" with higher standards. They didn't. BSA shows best of what we knew in 2021, not best of what we need in 2023.

CHAPTER 6: HUMAN RIGHTS IMPLICATIONS OF AI IN JUDICIAL PROCEEDINGS

6.1 *Right to Privacy and AI Data Collection*

In K.S. Puttaswamy v. Union of India, a nine-judge bench declared privacy a fundamental right under Article 21. This decision set historic three-part test for any state interference with privacy: there must be law authorizing interference (legality); it must have legitimate purpose (necessity); and interference's extent must be proportionate to objective (proportionality). This framework directly applies to state- operated AI surveillance.

In justice systems, AI requires enormous data. To train facial recognition model for Indian context requires millions of face images. To build crime-risk tool requires decades of conviction data. This collection rarely occurs with consent. It happens through government databases, surveillance cameras, and social media. Collection's legality is often unclear, based on vague CrPC or IT Act provisions rather than specific laws.

Proportionality standard is especially important. Is scanning every railway station traveler's face to catch one suspect proportionate? AI systems answer this question; that's policy question law should address. Current framework doesn't require proportionality analysis before AI deployment. Thus, AI justice transforms into "total surveillance state" that Constitution specifically meant to prevent.

AI surveillance's "chilling effect" cannot be ignored. When citizens know they're constantly monitored and analyzed, they change behavior. They avoid protests, religious meetings, or anything an algorithm might misread. This self-censorship indirectly violates Articles 19(1)(a) and 19(1)(b)—speech and assembly freedoms. Thus, AI harm extends beyond individual privacy to democratic freedoms' collective exercise.

"Purpose limitation principle"—data collected for one purpose cannot be used for another—is

ISSN: 2582-6433

violated in AI policing. Aadhar data collected for welfare might train facial recognition models. Traffic camera data might monitor protests. Strict data governance is absent; AI justice creates absolute surveillance state.

6.2 *Algorithmic Discrimination and Equality Before Law*

Article 14 guarantees equality before law and equal protection of laws. It is state arbitrariness's constitutional enemy. If AI systems aren't carefully designed, they become inequality machines. They often perform poorly on minority populations. Facial recognition systems show higher error rates for women and dark-skinned people. Using such tools in court denies those groups equal protection, putting them at higher wrongful conviction risk merely due to identity. This plainly violates Article 14.

"Disparate impact" concept is crucial. Any law or tool appearing neutral might still discriminate if a protected group faces disproportionate adverse impact. While Indian constitutional law hasn't fully embraced "disparate impact" arguments (preferring direct discrimination claims), algorithmic bias's systematic and pervasive nature might force Supreme Court to reconsider. If safeguard tools themselves become discrimination instruments, "equal protection right" loses meaning.

6.3 *Transparency and Right to Know*

Democratic society operates on transparency principle—government work must be visible, rational, and subject to scrutiny. AI's "black box" fundamentally contradicts this. When court uses algorithmic score as part of decision, affected party has right understanding how that score arose. However, if algorithm is proprietary and its logic is unexplainable, affected party faces complete darkness.

EU's GDPR, Article 22, gives individuals right to not be subject to purely automated decisions affecting them significantly, and right to explanation. India's Digital Personal Data Protection Act lacks equivalent provision. This represents major governance gap exactly where AI's most aggressive application occurs.

Consider practical scenario: judge denies bail because risk tool scores "8/10 High Risk." Accused asks: why high risk? Police say: algorithm says so. Company says: trade secret. Judge says: I cannot explain, algorithm told me so. Accused remains information-blind. Cannot

ISSN: 2582-6433

challenge unexplained reasoning; cannot defend themselves. Judicial transparency principle—decisions must appear just—is abandoned.

System's credibility requires transparency. If public cannot understand how decisions are made, courts' moral authority weakens.

6.4 *AI Surveillance Evidence and Self-Incrimination*

Article 20(3) provides no accused can be forced to give evidence against themselves. This is right against self-incrimination. In physical world, meaning is clear: cannot beat confession out of someone. But AI's digital world blurs lines. Advanced AI analyzing micro-expressions, voice tremors, or gait can estimate 'guilt suspicion.' These tools effectively extract testimony from accused's body without consent.

Selvi established that 'mental privacy' is part of Article 20(3). AI tools attempting to "look into" mind— estimating intent or deception—violate this 'mental sanctuary.' If state uses AI analyzing my social media to "estimate" my criminal mindset, it extracts testimony from my data in ways I never imagined. BSA, coming after Selvi, doesn't codify this constitutional standard into law. It doesn't require informed consent before AI profiling. This legislative gap leaves citizens unprotected from state's most intrusive intervention—algorithmic examination of inner world.

6.5 *Presumption of Innocence Under Algorithmic Profiling*

Criminal jurisprudence's golden principle—established in Woolmington v. DPP and firmly in Indian law—is every accused is innocent until proven guilty. This is not mere procedural formality; it expresses supreme value we place on individual freedom. State must prove guilt; citizen need not prove innocence. Algorithmic profiling attacks this principle's root.

Predictive AI classifies individuals not based on what they did but on statistical likelihood of what they *might* do. "High" risk score doesn't mean person committed crime; it means person shares traits with past criminals. Yet, this score influences real decisions—bail, custody, sentencing. Once labeled "high risk," innocence presumption quietly weakens. Judge reading this score unconsciously becomes prejudiced. Person's legal identity shifts from innocent to suspicious. This is "pre-crime" logic—punishing for unconvicted possibility rather than actual evidence.

ISSN: 2582-6433

Philosophically, "pre-crime" violates fundamental retribution principle—punishment must match actual wrong, not hypothetical risk. When sentencing uses recidivism scores, person gets longer sentence not because of crime committed but because algorithm predicts future crimes. This fundamentally violates presumption principle.

6.6 *Absence of Oversight Mechanisms*

Perhaps most concerning deficiency is complete lack of institutional oversight for AI in Indian justice. No independent regulatory body tests, certifies, or monitors AI tools used by police or courts. There is no Indian equivalent of UK's Forensic Science Regulator or EU's upcoming AI supervisory authority. Absent oversight, AI tools are essentially self-regulated by police departments purchasing and using them.

Accountability gap is stark. If AI tool misidentifies someone, resulting in wrongful arrest and detention, who is responsible? Police officer "just following algorithm"? Company selling tool? Government buying it? Currently, no clear liability framework exists. Wrongfully imprisoned person has no specific legal remedy for algorithmic error. This represents unacceptable human rights gap.

India needs dedicated "National Judicial AI Regulatory Council" with technical experts, legal scholars, civil rights activists, and judges. This body should certify AI tools before use; investigate existing tools for bias; handle complaints; and recommend corrective measures. Without systematic oversight, AI justice operates in rights-free zone.

CHAPTER 7: CHALLENGES IN ENSURING

FAIRNESS IN AI-ASSISTED DECISION-MAKING PROCESSES

7.1 *The Problem of "Black Box"*

The "black box" is modern AI's most powerful and simultaneously most troubling characteristic. Deep learning models—which underlie facial recognition and natural language processing—operate through hundreds of artificial 'neuron' layers. Each neuron performs mathematical transformation on data. By the time input passes through all layers to produce output, the connection between input and output becomes so complex that humans can barely understand or trace it. The U.S. Defense Advanced Research Projects Agency (DARPA) invested heavily in "Explainable AI" (XAI) research precisely because even the military cannot

ISSN: 2582-6433

fully trust a system it cannot understand.

For judiciary, the "black box" directly contradicts core duty of giving reasoned decisions. Any judge relying on AI output without understanding it is not exercising "judicial reasoning"; they are delegating this power to someone else. The duty to state reasons behind decisions is not mere administrative formality; it is shield against arbitrariness and foundation for appellate review. If decision's basis lies hidden in neural network's depths, appellate courts have nothing to examine.

COMPAS litigation history clearly shows black box's impasse. In State v. Loomis, defendant challenged COMPAS use because Northpointe (developer) invoked "trade secret" protection refusing source code disclosure. Court acknowledged concern but ruled since judge didn't base decision solely on score, "due process" wasn't violated. This dangerous precedent allows opaque AI into judicial reasoning if other reasons also exist. It doesn't require transparency; it merely requires additional supporting reason.

In India, Supreme Court's emphasis on "reasoned orders" (especially recent "electoral bonds" cases) provides strong constitutional foundation challenging AI-based evidence. Any judicial order citing AI score without explaining its basis or methodology could violate reasoned decision-making duty, subject to appellate challenge.

7.2 *Risk of Algorithmic Discrimination*

Fairness is justice's highest measure. We create elaborate procedures—blindfolded justice statue, anonymous juries—to achieve it. AI was thought perfect: no prejudice, no bad days, no hidden bias. This assumption is dangerously false. AI is mirror. It reflects data patterns it is trained on, and if that data contains social bias, AI reproduces it faithfully at scale with "scientific truth" authority.

Bias manifests in multiple ways. **Historical bias** occurs when training data embeds past discrimination (e.g., higher conviction rates for certain castes). **Measurement bias** occurs when proxy for concept itself is biased (e.g., using "previous arrests" as "criminality" proxy—when arrest rates themselves are racially biased). **Aggregation bias** occurs when model trained on one population is applied to different population.

ISSN: 2582-6433

India's social fabric is complex: 3,000 castes, dozens religions, hundreds languages, severe economic inequality. Risk assessment tool trained on Delhi urban crime data applied to Bihar rural crimes becomes biased. Law enforcement's caste and religious discrimination means any Indian AI will learn these biases. Using this with judicial evidence authority constitutionally violates Article 15, which prohibits caste, religion, sex, or birthplace discrimination.

U.S. NIST's facial recognition assessment found some systems' false-positive rates for African or Asian faces 100 times higher than Caucasian faces. Given Indians' darker skin and facial diversity across 28 states and 8 union territories, commercial FRT's accuracy for Indian use cases is highly uncertain.

"AI hallucination" problem adds another layer. Generative AI confidently produces factually false outputs. AI summarizing case file might state fact never existing in original document. If judge relies on AI- generated summary without reading original, case misjudgment becomes nearly certain.

7.3 *AI Tools' Reliability and Accuracy*

Justice requires certainty: guilt must be proven "beyond reasonable doubt." AI gives probability, not certainty. This is epistemological mismatch. Facial recognition tool claiming 93% certainty also admits 7% chance of error. In billion-person India, daily thousands of identifications with 7% error rate means thousands monthly false identifications. In criminal cases, even 1% error rate is unacceptable.

NIST's facial recognition evaluation revealed shocking disparities: some systems' error rates for African or Asian faces 100 times higher than Caucasian faces. India's demographics—darker skin, greater facial diversity—means commercial FRT's reliability for Indian use remains highly uncertain.

"AI hallucination" issue adds further uncertainty. Generative models confidently state false information. An AI summarizing case might confidently state facts never existing in original documents. If judges rely on AI summaries without checking originals, justice goes awry. We have seen U.S. cases where AI- prepared legal briefs cited non-existent case law.

Criminal law demands "beyond reasonable doubt" standard. AI's probabilistic outputs—with

ISSN: 2582-6433

unknown error rates in Indian contexts—cannot satisfy this standard. Courts must rigorously examine whether AI's certainty score genuinely meets this threshold or merely creates illusion of certainty.

7.4 *Judicial AI Literacy Deficiency*

Even best-designed safeguards fail when implementers lack capacity to use them. Survey data from judicial training institutions reveals most current judges received minimal or zero technology training during legal studies. Machine learning, neural networks, statistical probability—remain largely foreign to them. This creates "automation bias"—unconscious reliance on automated system without scrutiny. Psychology research shows people accept computer information more readily than human information without questioning. Judges unfamiliar with facial recognition's limitations will treat "match" as absolute fact. Algorithm becomes unquestionable arbiter.

National Judicial Academy (NJA) and State Judicial Academies must immediately incorporate AI literacy into curricula. Purpose is not making judges computer engineers but enabling them to ask right questions: What is error rate? Was tool tested on our demographics? Can defense effectively challenge this? Can this be explained in open court?

UK's Judicial College created AI-assisted decision-making modules for judges covering how machine learning works, what bias means, and how to evaluate expert testimony on AI tools. India should adopt similar framework, potentially through IIT collaboration and National Law Schools.

7.5 *Defense Counsel's Access to AI Evidence*

Criminal justice's adversarial system depends on opposing parties presenting arguments before neutral arbiter. Justice emerges from rigorous collision of contrary positions. If one side has powerful AI tools and other doesn't, this collision becomes one-sided slaughter. State, with vast resources, can acquire expensive forensic AI. Average accused—often poor and represented by overworked legal aid lawyers— lacks capacity to challenge such tools.

Algorithm's commercial secret protection—as in Loomis case—becomes systemic barrier to fair defense. Current legal framework doesn't obligate source code disclosure to accused. "Forensic AI discovery" has no statutory right. BNSS's Section 207 (evidence disclosure) may

ISSN: 2582-6433

not extend to proprietary AI tools.

Defense's right challenging evidence is constitutional right. If evidence is algorithmic, effective challenge requires technical expert access. For poor defendants—India's criminal accuseds' vast majority—hiring data forensics expert is economically impossible. State's free legal aid must extend to covering technical expert costs in AI-involved cases. This is not luxury; it is constitutional necessity.

7.6 *Maintaining Human Discretion in Decision-Making*

Decision-making's core is distinctly human act: discretion. Discretion involves weighing incommensurable values—freedom versus security, individual rights versus social welfare—in specific factual contexts with empathy and moral reasoning. No algorithm can do this. AI can tell you statistical recidivism likelihood; it cannot feel emotional burden of imprisoning young first-offender.

"Automation creep" danger is real. It starts with AI as tool—one data point among many. Gradually becomes habit—judges routinely relying on AI. Eventually becomes dependency—judges feeling uncomfortable deciding without AI score. At this point, real decision-making has been handed to machine, and AI becomes actual judge.

"Human-in-the-loop" emphasis in EU AI Act addresses this by requiring human able to intervene in, modify, and take final responsibility for AI decisions. In judicial context, this means final decision always rests with human judge—based on their own reasoning—with AI merely informing.

Supreme Court should set example. If using AI for case management (appropriate), operate with full transparency. If AI affects decision-making in any way, issue comprehensive guidelines. Judiciary's credibility rests ultimately on public belief that human judge—bound by oath, accountable to law— decides their fate.

CHAPTER 8: COMPARATIVE PERSPECTIVE ON AI AND FAIR HEARING

8.1 *United States: COMPAS and the Loomis Decision*

The United States serves as global laboratory for AI in criminal justice, offering India both cautionary tales and partial models. COMPAS (Correctional Offender Management Profiling

ISSN: 2582-6433

for Alternative Sanctions), developed by Northpointe Inc. (later Equivant), gives defendants 1-10 risk scores based on over 100 questions covering criminal history, social circumstances, and attitudes. Courts use this score for bail, sentencing, and parole decisions.

State v. Loomis became watershed legal battle. Eric Loomis was convicted of shooting-related car driving. At sentencing, judge incorporated his COMPAS score—7 out of 10 (quite high)—among factors for six- year imprisonment. Loomis challenged it, arguing the algorithm was gender-biased (using gender as risk factor) and denying due process (unable to challenge secret algorithm). Wisconsin Supreme Court rejected his challenge, ruling since the score wasn't sole basis and judges were warned of limitations, due process was met.

However, this decision draws academic and legal criticism. ProPublica's investigation into COMPAS (published after Loomis) revealed stark racial bias: Black defendants were flagged "high risk" at double the rate of White defendants with identical criminal histories. If similar tools deployed in India, our own historical caste and religious data biases would produce identical distortions. AI would effectively encode centuries of structural discrimination in mathematical "objectivity."

The "trade secret" problem persists unresolved. Defendants cannot examine the algorithm underpinning their fate. This contradicts confrontation right—facing evidence against you.

America's experience teaches institutional failure. Technology advanced far faster than law. Courts applied old "due process" frameworks to new algorithmic realities without adaptation. When COMPAS bias became apparent, thousands of sentences already incorporated flawed algorithm. India has "hindsight" advantage; we should use it.

8.2 *European Union: AI Act and Judicial Standards*

The EU AI Act (2024) is world's most comprehensive AI regulatory framework, setting standards for rights-based AI governance. Its significance for India's judicial AI is enormous. This Act adopts risk- based approach, categorizing AI into four: unacceptable risk (prohibited), high risk (strictly regulated), limited risk (transparency obligations), minimal risk (largely unregulated).

Crucially, AI used in justice administration and democratic processes falls within "high risk"

ISSN: 2582-6433

category. This means any AI tool used for evidence evaluation, risk assessment, or case management must meet strict conditions: maintain detailed technical documentation; ensure data governance and training data quality; achieve high accuracy, robustness, and cybersecurity; and implement human oversight allowing authorized personnel to "monitor, understand, and, where necessary, intervene in or override" the system.

The Act also explicitly prohibits certain AI practices violating fundamental rights: AI using subliminal or manipulative techniques influencing behavior; biometric classification systems inferring protected characteristics (race, religion) from appearance; and real-time remote biometric identification in public spaces by law enforcement (with limited exceptions).

For India, EU's Act provides legislative blueprint balancing rights with innovation. Judicial AI's "high- risk" classification with explainability, monitoring, and human override requirements directly addresses Indian concerns. India could adopt similar framework, adapted to constitutional context.

EU's experience shows strict regulation and technical progress aren't contradictory. EU remains innovation leader while protecting rights. India's AI ambitions can proceed alongside robust judicial safeguards.

8.3 *United Kingdom: Criminal Justice AI Guidelines*

UK adopted sector-specific, slower approach. No single AI law yet, but rich ecosystem of guidelines, best practices, and sector regulations creates meaningful framework for criminal justice AI.

The **Forensic Science Regulator**, established under 2021 Act, oversees forensic science standards in criminal cases, now extending to digital forensics including AI tools. This regulator issues codes of practice and conduct requirements for forensic service providers, including standards for testing, quality assurance, and reporting error and bias rates.

UK experience also illustrates automation's dangers, as illustrated by Post Office Horizon scandal—one of UK legal history's greatest justice failures. Faulty accounting software (Horizon) created false transaction records used to prosecute 700+ Post Office sub-postmasters for theft and fraud. Courts accepted computer data without questioning reliability. Hundreds

ISSN: 2582-6433

were wrongly convicted. Decades passed before this systemic injustice was remedied. This real-world example powerfully demonstrates why courts cannot simply trust AI evidence.

The Law Society of England and Wales issued detailed guidelines on AI use in legal practice, emphasizing lawyers must understand AI tools they rely on and inform clients of limitations. The Judicial College trains judges on algorithm-based decision-making. "Explainability requirement" as ethical and legal standard shows one practical model India could adopt.

The Human Rights Act 1998, incorporating European Convention on Human Rights (Article 6—right to fair hearing), gives UK courts powerful tool challenging improper AI use in justice.

8.4 *Lessons and Best Practices for India*

Combining U.S., EU, and UK experiences yields crucial lessons. First, America's experience teaches consequences of inaction: without regulatory safeguards before AI's judicial introduction, bias becomes entrenched and remedying it becomes nearly impossible. Timing of regulation is crucial—before, not after, deployment.

Second, EU's model demonstrates rights-based regulation and technical progress aren't opposed. Classifying judicial AI as "high-risk" with transparency, human monitoring, and accuracy requirements provides effective framework. India could amend BSA adding dedicated chapter regulating "AI-generated and AI-processed evidence" modeled on EU's high-risk framework.

Third, UK's sector-specific approach—particularly Forensic Science Regulator model—shows specialized oversight bodies work. India needs "National Forensic AI Standards Board" certifying and auditing AI tools in criminal investigation before court use. Registry of approved and rejected tools; periodic bias audits; annual reports on AI's judicial impact; and complaint handling for AI-caused harm. Such body provides accountability currently absent.

Fourth, all three jurisdictions emphasize "human-in-the-loop"—AI outputs are advisory not final in criminal cases. India should legislatively ensure AI evidence remains advisory, with final decision resting with human judge exercising independent reasoning.

Finally, India must adapt these frameworks to distinctive context. Caste, linguistic diversity,

ISSN: 2582-6433

and digital divide present challenges American or European frameworks address differently. India's "Made in India" AI governance should require "caste-impact assessments" before deploying any criminal justice AI tool.

CHAPTER 9: EVALUATION OF INDIAN EVIDENCE ACT, 2023 FROM ARTICLE 21 PERSPECTIVE

9.1 *Preamble*

Having mapped AI's fair hearing impact and examined other jurisdictions' responses, this chapter brings analysis home: does Indian Evidence Act, 2023, meet Article 21's constitutional standard? That standard, set by Menaka Gandhi, requires that procedures be "fair, just, and reasonable"—not arbitrary, fanciful, or oppressive.

Evaluation framework asks: Does BSA's digital evidence framework, when applied to AI, permit uses that are arbitrary (due to black-box opacity), oppressive (due to biased algorithms), or incompatible (due to excessive data collection) with Article 21? Analysis shows mixed conclusions. BSA is not bad law; it is incomplete law. Intent is right but specific mechanisms addressing AI's unique challenges are absent. It answers 2015 questions in 2023, while actual questions are 2025 and beyond.

This chapter identifies six specific areas where BSA, as currently written, falls short of Article 21's standards when applied to AI. It concludes with overall constitutional suitability assessment.

9.2 *Inadequacy of AI-Specific Safeguards in BSA*

BSA's fundamental deficiency is treating all electronic records monolithically. WhatsApp message and deepfake video are both "electronic records" under Act, both admissible under Section 63, subject to identical procedure. This equality is constitutionally problematic because these evidence types present fundamentally different reliability challenges.

WhatsApp message, though alterable or screenshotable, records human communication. Its authenticity can be challenged through traditional forensics—hash verification, metadata analysis, sender cross- examination. Deepfake is entirely fabricated, mimicking reality so perfectly courts cannot distinguish it through ordinary examination. BSA doesn't require courts

ISSN: 2582-6433

scrutinize deepfakes more rigorously than authentic messages. This procedural equivalence is unreasonable.

Menaka Gandhi's standard demands procedure be "rational." Rational procedure for AI evidence would include: distinct AI-generated content category; heightened evidence standards for such content; mandatory AI tool accuracy, error rate, and validation history disclosure; and defense right to challenge not just AI outputs but AI methodology itself. BSA contains none of these.

Without these safeguards, BSA permits evidence acceptance that is arbitrary (due to black-box opacity), potentially discriminatory (due to biased algorithms), or excessive in data collection (due to privacy violations). This procedure is not "fair, just, and reasonable" under Menaka Gandhi.

9.3 *Discretion Without Accountability*

BSA grants judges considerable discretion in weighing electronic evidence. While judicial discretion generally aids contextual justice, without clear legal guidance it becomes arbitrary. When judges lack frameworks evaluating AI evidence, they decide inconsistently and potentially unpredictably.

This arbitrariness directly violates Article 14, barring state arbitrariness. Different judges, with different technical literacy, treat identical AI evidence entirely differently. One judge, knowledgeable about technology, scrutinizes risk score rigorously. Another, unknowledgeable, accepts it without question. Same accused faces vastly different outcomes depending on judge assignment—not on law but on chance.

This inconsistency demands more uniformity. Either Supreme Court must issue comprehensive guidelines or Parliament must amend BSA providing clear standards. Absent this, AI evidence's admissibility and weight become arbitrary.

9.4 *Consent, Coercion, and Digital Evidence*

AI profiling demands biometric data—face photos, voice samples, gait recordings—collected for profiling. BSA regulates such data's court admissibility but doesn't mandate it's collected with informed consent regarding AI profiling purposes. This creates serious Article 20(3)

ISSN: 2582-6433

issues regarding self- incrimination.

Selvi established "voluntary participation" standard for scientific evidence affecting mind. But BSA doesn't mandate consent before AI profiling use. Nor does it legally operationalize Selvi's constitutional standard into statutory mandate.

"Forced digital surrender" also problematic. When police seize phone and demand biometric unlock, is this evidence or compulsion? BSA doesn't answer. Some U.S. courts distinguish biometric unlock (not evidence, thus non-compellable) from passcode (evidence, thus compellable). India needs clear legal answer, particularly since unlocked data feeds AI analysis.

9.5 *AI Surveillance and Privacy Rights*

Evidence law historically followed inclusive rule: relevant evidence generally admissible regardless of collection method. America's "exclusionary rule" (excluding illegally obtained evidence) was exception. India preferred admitting relevant evidence and separately addressing constitutional violations if necessary.

But this approach becomes dangerous with AI enabling pervasive government surveillance. Puttaswamy's proportionality test—surveillance must be proportionate to need—offers potential bridge. AI evidence illegally obtained through disproportionate surveillance might be excluded under Puttaswamy principles even if admissible under general evidence rules.

Yet BSA, enacted after Puttaswamy, doesn't operationalize this constitutional principle into statutory rule. It doesn't require courts exclude AI evidence obtained through disproportionate surveillance. This legislative gap leaves citizens unprotected from state's most invasive surveillance via AI.

Digital Personal Data Protection Act, while progress, carves out vast exemptions for state security and law enforcement—precisely where AI surveillance is most aggressively used.

9.6 *Judicial Oversight and Its Limits*

Current system relies on judges as AI oversight's centerpiece. Judges evaluate AI evidence, assess reliability, and determine weight. This theoretically aligns with independent judiciary

ISSN: 2582-6433

checking executive overreach. Practically, it fails. AI's complexity exceeds most judges' expertise. Judges lack capacity to scrutinize what they don't understand.

BSA doesn't grant judges power to appoint independent technical experts suo motu (on their own motion) to examine complex AI evidence. Courts have inherent powers to appoint experts, but no specific provision addresses AI evidence's technical complexity.

As AI deployment increases, judiciary needs structural support: court-appointed independent AI auditors panel for complex cases; training programs; and technical advisory services. Without infrastructure, relying solely on judges for AI scrutiny is institutionally insufficient.

9.7 *Summary Assessment*

Overall, BSA's evaluation against Article 21 yields this conclusion: BSA is essential and praiseworthy modernization advancing Indian evidence law from colonial past into digital age. Its merit lies in clearly recognizing electronic records, streamlining acceptance procedures, and conceptually embracing digital world.

From Article 21 perspective, deficiencies are: (1) AI-specific standards absent; (2) explainability requirement lacking; (3) no evidence exclusion for disproportionate surveillance; (4) inadequate consent and self-incrimination protections in digital context; (5) excessive reliance on judicial discretion without guidance; and (6) no mandatory independent oversight.

Each deficiency is potential constitutional challenge basis. As AI evidence proliferates, courts will face challenges. Ultimately, Supreme Court must decide whether BSA, when applied to AI evidence, meets Article 21's "fair, just, and reasonable" standard. This analysis suggests it presently does not.

However, this isn't despair message. BSA is law subject to amendment. Judiciary can fill gaps through interpretation. Questions are whether sufficient political will and judicial foresight exist to make necessary reforms before algorithmic injustice becomes irreversible. India has "hindsight advantage"; question is whether we'll use it.

ISSN: 2582-6433

CHAPTER 10: RECOMMENDATIONS FOR RIGHTS-BASED AI INTEGRATION IN THE JUDICIARY

10.1 Enact Dedicated Rules for AI Evidence

The most immediate legislative requirement is enacting specific rules under BSA governing "AI-generated and AI-processed evidence." These rules should define "algorithmic evidence" as distinct category from standard electronic records. They should establish heightened admissibility standard requiring the party presenting AI evidence to establish: identification and version of AI tool used; documented error rates and validation history; demographics of training data; and results of any independent bias audit. This approach aligns with EU AI Act's documentation requirements for high-risk AI systems and addresses regulatory vacuum. Canada's "Automated Decision-Making Directive" provides practical precedent India can follow.

10.2 Establish "Explainability Standards" for AI Tools

No AI output should be accepted as evidence unless its reasoning can be explained in manner comprehensible to ordinary judge. Parliament should amend BSA adding requirement that any party presenting AI evidence, alongside Section 63 certificate, also submit "explainability statement" describing AI tool's logic, inputs, and limitations in simple language. If AI system cannot provide such explanation— if it is genuinely a "black box"—its output should not be accepted as substantial evidence. This directly addresses opacity problem and ensures satisfaction of constitutional duty to give reasoned decisions. UK's AI ethics guidelines' "explainability requirement" provides practical model.

10.3 Establish Independent AI Oversight Bodies

An independent "National Judicial AI Council" should be statutorily established, comprising retired Supreme Court judges, IIT senior faculty, ethics experts, civil society representatives, and legal aid advocates. Its mandate should include: pre-deployment certification of AI tools proposed for criminal justice use; maintenance of public registry of approved and rejected tools; periodic bias audits of deployed tools; publication of annual reports on AI's judicial impact; and complaint handling for those harmed by defective AI evidence. UK's Forensic Science Regulator and EU's forthcoming AI supervisory authority provide models. Such body provides institutional accountability currently absent.

ISSN: 2582-6433

10.4 Mandatory Judicial AI Training

National Judicial Academy must implement mandatory AI literacy course for all newly appointed judges and integrate it into continuing legal education for current judges. Curriculum should include: machine learning basics; meaning of bias and its manifestations; evaluating expert testimony on AI tools; writing reasoned orders critically examining AI evidence; and case studies from India and abroad showing judicial AI failures. Training should come through collaboration with IIT and National Law Schools to ensure technical depth and legal relevance. Without judicial AI literacy, no legislative reform achieves practical efficacy.

10.5 Strengthen Defense Counsel's Rights Challenging AI Evidence

Accused's effective defense right must be adapted to AI context. NALSA's (National Legal Services Authority) framework should expand to provide state-funded forensic data experts in cases where prosecution presents AI evidence against poor accused. Additionally, BSA should be amended clarifying that in AI-involved cases, defense has right to examine algorithm's "source code" and "training data" before neutral expert appointed by court when defense challenges tool's reliability. This balances vendors' legitimate trade secret interests with constitutional confrontation rights. Without this, "equality of arms" becomes legal fiction.

10.6 Codify Consent and Privacy Safeguards

BSA amendments or judicial guidelines should explicitly incorporate Selvi standard into digital context. Biometric or behavioral data obtained without informed consent for AI profiling should be prima facie inadmissible, though subject to rigorous judicial examination against Puttaswamy proportionality framework. Additionally, Digital Personal Data Protection Act should be amended removing blanket exemptions for law enforcement, replacing them with specific, time-limited, and judicially-supervised exceptions. Consent and privacy aren't obstacles to justice; they are essential conditions.

10.7 Mandate Algorithmic Impact Assessments

Before any government department or police force deploys AI tool in criminal justice—whether for surveillance, investigation, or risk assessment—mandatory "Algorithmic Impact Assessment" (AIA) must be conducted by independent body, not deploying agency itself. AIA should test tool for bias across demographic groups (caste, religion, gender, region), assess accuracy and error rates, identify intended and unintended uses, and evaluate privacy harm relative to proportionality. AIA report should be publicly available. Canada's "Automated

ISSN: 2582-6433

Decision-Making Directive" and EU's fundamental rights impact assessment requirements provide templates. This pre-deployment scrutiny is minimum necessary protection.

10.8 Judicial Guidelines on AI Evidence Admissibility

Pending legislative action, Supreme Court should issue comprehensive guidelines under Article 142 authority on AI evidence admissibility and evaluation in criminal proceedings. Guidelines should adopt modified version of U.S. Daubert standard: AI tool must be testable and peer-reviewed; have known and acceptable error rate; be governed by standards controlling its operation; and be generally accepted by relevant scientific community. Guidelines should establish that Section 63 certificate is necessary but insufficient condition; courts must separately assess tool's reliability. Guidelines should clarify that AI- generated material carries heightened burden showing authenticity.

10.9 Adopt EU-Style Restrictions on Prohibited AI Practices

India should legislatively prohibit certain AI practices incompatible with fundamental rights in criminal justice: AI-based lie detection and deception analysis used as substantial evidence; predictive policing based purely on profiling without specific, articulate, evidence-based suspicion; mass real-time biometric surveillance in public spaces for identification and profiling purposes; and AI systems inferring religion, caste, political belief, or sexual orientation from physical appearance or behavioral data. These restrictions are not radical; they are minimum necessary to ensure AI doesn't become weapon of state oppression.

10.10 Develop National AI Ethics Framework for Justice System

Pending comprehensive legislation, Law Ministry working with Electronics and IT Ministry, Supreme Court, Bar Council, and civil society should develop "National AI Ethics Framework for Justice System." This framework should embed core values governing judicial AI: dignity (AI must respect each person's humanity before courts); fairness (AI must not discriminate); accountability (human always responsible for AI-assisted decisions); transparency (AI's reasoning must be explainable); and reversibility (AI errors must be legally correctable). Such framework guides development and regulation pending legislation.

10.11 Strengthen Chain of Custody for AI Evidence

Chain of custody for digital evidence should be extended backward to include AI tool itself. New protocols must mandate detailed logs whenever AI is used collecting, analyzing, or processing

ISSN: 2582-6433

evidence. Logs should record: AI tool's specific version; date and time of use; operator; any alerts or warnings generated; and raw output before human interpretation. Distributed ledger technology (blockchain) could create tamper-proof, unalterable records of AI custody chain. Without extended chain, guaranteeing AI- processed evidence's reliability under Section 63 becomes impossible.

10.12 Periodic Legislative Review

Given AI development's unprecedented pace, BSA and related rules should undergo mandatory statutory review every three years (not five years, given change velocity). Review body should include lawyers alongside technical experts, specifically assessing whether "electronic record" definition remains fit for purpose; whether new AI capabilities (generative video, emotion recognition) need special regulation; and whether current oversight mechanisms effectively prevent justice system's AI-related failures. This built- in adaptability is only way law avoids falling dangerously behind technology.

CHAPTER 11: CONCLUSION

This research has covered vast and intricate terrain: from abstract fair hearing philosophy to Indian Evidence Act's specific sections; from COMPAS algorithm's racial bias in Wisconsin to Supreme Court's privacy jurisprudence; from neural networks' opacity to constitutional mandate for reasoned decisions.

Throughout every chapter, central argument emerged: Artificial Intelligence, as currently deployed and regulated, poses genuine and serious threat to constitutional guarantee of fair hearing, and Indian Evidence Act, 2023, in its present form, provides insufficient answer to this threat.

However, concluding with complete pessimism would be intellectually dishonest. AI is not inherently opposed to justice. Used properly—for translation, legal research, case management—it can make justice system more accessible and efficient. Problem is not technology; it is governance. We have tendency rapidly embracing new technologies but considering their regulation later. India's digital evidence history—from Section 65B's chaos to Anwar P.V.'s clarifications—demonstrates we react to problems rather than anticipate them. With AI, problems will be larger and consequences more severe. We must break this cycle.

ISSN: 2582-6433

Concept of "Algorithmic Due Process" proposed in this paper is not novel or revolutionary invention. It is natural evolution of constitutional principle continuously expanding since 1950. As Court extended Article 21 to include speedy trial, legal aid, and privacy rights, so too should it now extend it to include right to understand and challenge algorithms determining one's fate. "Procedure established by law" in 21st century must include procedure by which machines generate evidence and law is applied. Any technology affecting liberty deserves same constitutional scrutiny as any state action.

Appeal to legislators is direct and simple: Twelve recommendations in Chapter 10 are not wishes; they are constitutional requirements. BSA must be amended to include AI-generated evidence standards, explainability requirements, and consent safeguards. Law must establish National Judicial AI Council. NALSA framework must expand to include technical legal aid for AI cases. Amended DPDPA must eliminate blanket law enforcement exemptions. These are not expensive measures; they are digital-age constitutional democracy's basic infrastructure.

Appeal to judiciary is equally direct: Don't await legislative action. Court's rich tradition of filling rights- protective gaps in legislation extends here. Supreme Court should issue comprehensive guidelines on AI evidence under Article 142. High Courts should actively remove AI evidence lacking minimum reliability standards. Every judge must resist automation bias and maintain independent reasoning. Judiciary's credibility ultimately rests on public belief that human judge—sworn to law, accountable for decisions— determines their fate.

Appeal to legal profession is equally vital: Lawyers and advocates must educate themselves on technology. Failure to challenge defective AI evidence—whether from ignorance or pressure—constitutes professional breach. Bar Council should include AI and digital law in All India Bar Exam. Advocates must master challenging problematic AI evidence.

Justice's scale has always been delicate, requiring constant human oversight. In AI age, this work becomes harder and more critical. Dangers are now less visible, biases subtler, power imbalance deeper. But values we protect—dignity, equality, fairness, truth—are values that inspired Constitution drafters writing Article 21 in colonial oppression's shadow. They understood, and we must understand today, that freedom doesn't maintain itself. It requires active defense against every form of tyranny—including now algorithmic tyranny. Technology must remain

ISSN: 2582-6433

justice's instrument, never its alternative.

Ultimately, just society's mark is not technological modernity but procedural fairness. India can become global AI leader and global constitutional justice exemplar. But only if, with clarity and conviction, we insist that no machine—however powerful, however efficient—will come between citizen and right to fair hearing. In end, no algorithm can replace what justice truly requires: human dignity, human judgment, human accountability.

The stakes could not be higher. The moment to act is now. The responsibility rests with all of us— legislators, judges, lawyers, and citizens. We have the knowledge, the constitutional framework, and the examples from other nations. What remains is political will and judicial vision to ensure that in India's journey into AI age, we neither abandon our constitutional soul nor compromise the fundamental rights that define us as democracy

Footnotes

1. National Judicial Data Grid (NJDG), Supreme Court of India, Pendency Statistics (2023), available at njdg.ecourts.gov.in.
2. Joanna Jolly, "Delhi Used Facial Recognition to ID Rioters. Then the Problems Started," *Time Magazine*, March 2020; Internet Freedom Foundation, "Facial Recognition Technology in India" (2020).
3. *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27.
4. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
5. *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
6. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
7. *Hussainara Khatoon v. Home Secretary, State of Bihar*, (1979) 3 SCC 1.
8. *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416.
9. *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
10. *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
11. *Anwar P.V. v. P.K. Bashir*, (2014) 10 SCC 473
12. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
13. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
14. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
15. *Zahira Habibullah Sheikh v. State of Gujarat*, (2004) 4 SCC 158.

 ISSN: 2582-6433

Bibliography

A. Primary Sources — Statutes

- The Constitution of India, 1950 (Articles 14, 19, 20(3), 21, 22).
- The Bharatiya Sakshya Adhiniyam, 2023 (Sections 2(1)(d), 57, 61, 63, 81).
- The Indian Evidence Act, 1872 (Repealed) (Sections 45, 65A, 65B).
- The Information Technology Act, 2000.
- The Digital Personal Data Protection Act, 2023.
- The Bharatiya Nagarik Suraksha Sanhita, 2023.
- The EU Artificial Intelligence Act, 2024 (Regulation (EU) 2024/1689).
- The UK Forensic Science Regulator Act, 2021.
- General Data Protection Regulation (EU) 2016/679 (GDPR).

B. Case Laws

- *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
- *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27.
- *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (Privacy Judgment).
- *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
- *Anwar P.V. v. P.K. Bashir*, (2014) 10 SCC 473.
- *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
- *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
- *Zahira Habibullah Sheikh v. State of Gujarat*, (2004) 4 SCC 158.
- *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
- *Hussainara Khatoon v. Home Secretary, State of Bihar*, (1979) 3 SCC 1.
- *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416.
- *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
- *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
- *Woolmington v. Director of Public Prosecutions*, [1935] AC 462 (HL).
- *People v. Collins*, 438 P.2d 33 (Cal. 1968).

C. Books

- Richard Susskind, *Online Courts and the Future of Justice* (Oxford University Press, 2019).
- Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press, 2018).

ISSN: 2582-6433

- Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Books, 2016).
- Abhinav Chandrachud, *Due Process of Law* (Eastern Book Company, 2011).
- M.P. Jain, *Indian Constitutional Law* (8th ed., LexisNexis, 2018).
- Sujit Choudhry et al., *The Oxford Handbook of the Indian Constitution* (Oxford University Press, 2016).
- Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).
- Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (MIT Media Lab, 2018).

D. Journal Articles and Reports

- Završnik, A., "Criminal Justice, Artificial Intelligence Systems, and Human Rights," *ERA Forum*, Vol. 20 (2020), pp. 567–583.
- Surden, H., "Machine Learning and Law," *Washington Law Review*, Vol. 89 (2014), pp. 87–115.
- Desai, D.R. & Kroll, J.A., "Trust but Verify: A Guide to Algorithms and the Law," *Harvard Journal of Law & Technology*, Vol. 31(1) (2017), pp. 1–64.
- Angwin, J. et al., "Machine Bias," *ProPublica*, May 23, 2016 (Investigation into COMPAS algorithm).
- Niti Aayog, "National Strategy for Artificial Intelligence: #AIForAll," Government of India (2018).
- Law Commission of India, 185th Report, "Review of the Indian Evidence Act, 1872" (2003).
- Law Commission of India, 269th Report, "Human DNA Profiling" (2017).
- Kleinberg, J. et al., "Human Decisions and Machine Predictions," *Quarterly Journal of Economics*, Vol. 133(1) (2018), pp. 237–293.
- Kroll, J.A. et al., "Accountable Algorithms," *University of Pennsylvania Law Review*, Vol. 165 (2017), pp. 633–705.
- Internet Freedom Foundation, "Facial Recognition Technology in India: A Compendium" (2021).
- National Institute of Standards and Technology (NIST), "Face Recognition Vendor Testing (FRVT) Part 3: Demographic Effects" (2019).