TECHNOLOGICAL ADVANCES IN CRIMINAL JUSTICE: REJOICE, BUT REFLECT

Dr. Tushita Sharma, Associate Professor, VSLLS, Vivekananda Institute of Professional Studies—TC, (Accredited NAAC A++; affiliated to GGSIPU, Delhi, Recognised by Bar Council of India).[1]

ABSTRACT

Technology continues to advance at a rapid pace, and these changes show their direct impact on the areas of criminal jurisprudence and the delivery of justice. Updated technology in criminal justice has become a tool not merely in helping improve the accuracy of investigations and increasing positive outcomes for victims of crime, but also in quickening the dispensation of justice. Forensic science has seen tremendous advancements largely thanks to technology. DNA analysis has revolutionised criminal investigations, the accuracy of DNA profiling has exonerated innocent individuals and identified perpetrators in cases that were once unsolvable. Law enforcement now employs an ever-expanding range of biometric and behavioural features—including facial recognition, DNA, heartbeat detection, speech recognition, wrist-vein mapping, iris recognition, gait analysis and palmprint scanning. In the post-pandemic new normal, the advent of virtual courtrooms and online platforms has introduced significant flexibility and accessibility to legal proceedings. In India, the recently enacted Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Nyaya Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023 have accelerated this digital turn.

This paper analyses the technological changes brought about by India's new criminal law regime while sounding warning bells towards perils that demand vigilant attention: data privacy, executive overreach, evidentiary complexities and ethical concerns.

Keywords: Criminal Jurisprudence, Digital Evidence, DNA Analysis, Biometrics, Virtual Courts, BSA 2023, BNSS 2023, Data Privacy, Algorithmic Justice, Forensic Science.

[1] Dr. Tushita Sharma, Associate Professor, VSLLS, Vivekananda Institute of Professional Studies—TC, (Accredited NAAC A++; affiliated to GGSIPU, Delhi, Recognised by Bar Council of India).

I. INTRODUCTION

The interface between technology and criminal justice is neither novel nor temporary—it is axiomatic and accelerating. From the earliest deployment of fingerprint databases in the late nineteenth century to the now-pervasive use of closed-circuit television, electronic surveillance and artificial intelligence-driven predictive policing, each technological leap has reshaped both the investigative capacity of the State and the procedural rights of the accused. What distinguishes the present moment, however, is the qualitative velocity of this transformation: developments that took decades in the twentieth century now unfold within years, occasionally months. Nowhere is this more consequential than in criminal justice, where the stakes—human liberty, bodily integrity and the legitimacy of the State—are existential.[2]

India has responded to this imperative with uncommon legislative ambition. The triptych of the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has together repealed and replaced the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973, and the Indian Evidence Act, 1872 respectively—a legislative transformation of a kind unseen since the colonial codification itself. Central to this transformation is a determined embrace of technology: e-FIRs, electronic summons, digital evidence frameworks, mandatory audio-video recording of statements, and virtual trial hearings have all been incorporated with a degree of detail absent from predecessor statutes.[3]

This paper proceeds from the proposition that this technological embrace is not a uniformly celebratory event: it is an occasion for both qualified rejoicing and serious reflection. In the sections that follow, the paper examines, first, the forensic and investigative advances that technology enables; second, the procedural transformation brought about by virtual courts and digital platforms; third, the evidentiary architecture of digital and electronic evidence under the BSA; and finally, the critical perils—privacy erosion, executive overreach, algorithmic bias and ethical lacunae—that must be confronted if the promise of technological justice is to be realised rather than merely proclaimed.

---

[2] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, (hereinafter, BSA), see Chapter V; Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, (hereinafter, BNSS), see ss.171–189; Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, (hereinafter, BNS).

[3] BNSS, 2023 s. 173(1) (e-FIR) and s. 173(3) (Zero FIR); *Lalita Kumari v. Govt. of U.P.* (2014) 2 SCC 1 (mandatory registration of FIR for cognizable offences).

II. THE FORENSIC REVOLUTION: DNA, BIOMETRICS AND BEYOND

Reflecting on the DNA analysis and its exonerative capacity; the expanding biometric palette, whether facial recognition, gait, iris, voice or the heartbeat, as patterns mapped by experts; and ballistics as well as fingerprint advancement, along with the critical attention to reliability limitations and the absence of a Daubert-equivalent gatekeeping standard in India have been taken for discussion.

2.1 DNA Analysis: Exoneration and Identification

The most profound forensic revolution of the twentieth century was, without doubt, the development of DNA profiling by Sir Alec Jeffreys in 1984 and its rapid integration into criminal investigation. DNA evidence has since occupied a unique epistemic position in criminal proceedings. Its discriminating power—where fully interpreted profiles yield identification probabilities in the order of one in several billion—approaches certainty at a level unmatched by any anterior forensic technique. Critically, DNA has served not merely as a sword for prosecution but as a shield for the wrongly convicted. Studies in the United States document that of the first 375 post-conviction exonerations secured through DNA, approximately 71 per cent involved erroneous eyewitness identifications—highlighting that DNA's greatest contribution may lie not in conviction but in exoneration.[4]

In India, the legal framework governing DNA evidence has evolved fitfully. The Indian Evidence Act, 1872 offered no provision specifically addressing biological evidence; courts admitted DNA reports under the general provisions on expert opinion, later supplemented by provisions governing electronic records of such reports. The DNA Technology (Use and Application) Regulation Bill, 2019, which sought to establish a national DNA databank and regulatory structure, was introduced in Parliament but lapsed—leaving India without a dedicated DNA governance statute at the time of writing.[5]

The BSA takes a cautious step forward by explicitly listing DNA analysis among the categories of expert opinion admissible under its provisions, while the BNSS mandates forensic

[4] Brandon L. Garrett, *Convicting the Innocent: Where Criminal Prosecutions Go Wrong* (Harvard University Press, 2011, pp. 97–143.

[5] The DNA Technology (Use and Application) Regulation Bill, 2019, introduced in Lok Sabha; Standing Committee on Science and Technology, 148th Report (2019). See also Kiran T Shinde, "DNA Evidence in Indian Courts: An Appraisal," *JILI (2021) 63(2) 201.*

examination—including DNA analysis—for offences punishable with seven or more years of imprisonment where the circumstances so warrant. The certification and chain-of-custody requirements under Section 63 BSA also apply to laboratory reports generated digitally, addressing a persistent lacuna regarding the authenticity of forensic documentation. However, the absence of a statutory regulatory authority—specifying accreditation standards for DNA laboratories, permissible uses of databanks, retention limits and destruction obligations—remains a serious gap.[6]

2.2 The Expanding Universe of Biometric Identification

Beyond DNA, the biometric palette available to law enforcement has expanded dramatically. Contemporary identification technology encompasses facial recognition systems, iris scans, voice-print analysis, gait recognition, palmprint mapping, wrist-vein patterns and, most recently, cardiac rhythm detection—each offering a distinct physiological or behavioural signature that may be linked to an individual with varying degrees of reliability. The appeal of these modalities to law enforcement is self-evident: they permit identification at a distance, without consent, and often without the subject's awareness, enabling surveillance on a scale previously confined to the dystopian imagination.[7]

Facial recognition technology (FRT) merits particular scrutiny. Studies at the Massachusetts Institute of Technology demonstrated that commercially deployed FRT systems exhibited error rates of up to 34.7 per cent in classifying darker-skinned females compared with near-zero error rates for lighter-skinned males—a disparity so significant that its deployment in law enforcement contexts carries substantial risks of discriminatory misidentification. India's Automated Facial Recognition System (AFRS), developed by the National Crime Records Bureau, has been operational in a number of states; yet there is neither a statutory basis governing its deployment nor a publicly accessible audit of its accuracy rates or demographic error differentials.[8]

Gait Analysis— the identification of individuals through their distinctive pattern of

[6] *Anvar P.V. v. P.K. Basheer & Ors.,* (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* (2020) 7 SCC 1 (certification requirement under s. 65B revisited).
[7] Anil K. Jain, Arun A. Ross & Salil Prabhakar, "An Introduction to Biometric Recognition," *(2004) 14(1) IEEE Transactions on Circuits and Systems for Video Technology 4.*
[8] Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,"*(2018) 81 Proceedings of Machine Learning Research 1; National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT), NISTIR 8280 (2019).*

movement—represents an emerging biometric frontier. While it has been admitted as expert opinion in certain jurisdictions, questions of inter-examiner reliability, the effect of footwear and injury on gait patterns, and the absence of a standardised validation methodology continue to cloud its evidentiary status. Similarly, voice recognition and heartbeat detection technologies, while scientifically intriguing, lack the breadth of validation studies that would justify their uncritical admissibility in criminal proceedings.[9]

III. Ballistics and Fingerprint Analysis: Incremental Precision

Ballistics analysis— comparing the striations left on fired projectiles and cartridge cases with the barrel and firing mechanism of a weapon—has undergone significant technological enhancement through the introduction of databases such as IBIS (Integrated Ballistics Identification System) and automated microscopic comparison. These developments increase the probability of matching ammunition to weapons across multiple crime scenes, facilitating the detection of serial criminal activity. Nonetheless, a landmark report by the National Academies of Sciences, Engineering and Medicine observed that ballistics comparison, like other pattern-based forensic disciplines, lacks the controlled scientific studies necessary to precisely characterise the accuracy of examiners' conclusions—a caveat that courts must internalise when evaluating such testimony.[10]

Fingerprint analysis— long regarded as the gold standard of forensic identification, has similarly benefited from automated database matching (AFIS) and improved ridge-detail resolution. However, the same concern about examiner subjectivity and confirmation bias—documented in blind studies where fingerprint examiners reached conflicting conclusions when contextual information was varied—applies here. The BSA's provisions on expert opinion do not articulate reliability standards for pattern-based sciences, leaving Indian courts without the equivalent of the American Daubert gatekeeping doctrine to screen out scientifically unreliable expert testimony.[11]

---

[9] Mark S. Nixon & Johanna Carter, "Automatic Recognition by Gait," *2006, 94(11) Proceedings of the IEEE 2013*; *R v. Otway [2011] EWCA Crim 3* (gait analysis admitted as expert opinion in England).

[10] *National Research Council, Strengthening Forensic Science in the United States: A Path Forward* (National Academies Press, 2009, pp. 153–174; see also, President's Council of Advisors on Science and Technology (PCAST), Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods (2016).

[11] *Daubert v. Merrell Dow Pharmaceuticals, Inc.,* 509 U.S. 579 (1993); *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016) (upholding use of COMPAS recidivism algorithm at sentencing while raising transparency concerns), available at,

IV. VIRTUAL COURTS AND THE DEMOCRATISATION OF JUSTICE

Tracing the constitutional lineage of the right to speedy trial, stemming from *Hussainara Khatoon* and right to the virtual hearing provisions encapsuled in the BNSS, this section evaluates the varied gains in undertrial detention reduction.

4.1 A Case for Technology Enabled Adjudications

India's chronic case pendency crisis has long been identified as the most severe structural challenge confronting the justice delivery system. With over forty-five million cases pending across all tiers of the court hierarchy as of early 2025, and an average trial duration that extends to several years for serious criminal matters, the constitutional promise of a speedy trial under Article 21 has often remained aspirational. The Supreme Court in *Hussainara Khatoon,*[12] recognised speedy trial as an inalienable facet of the right to life and personal liberty, yet structural causes—judicial vacancies, inadequate infrastructure, and procedural abuses—continued to frustrate realisation of that right for decades.[13]

Against this backdrop, the introduction of virtual court hearings—first deployed at scale as an emergency measure during the COVID-19 pandemic from March 2020—proved transformative in ways that transcended the immediate health exigency. Supreme Court data reveals that between March 2020 and December 2022, over 1.8 million cases were heard through video conferencing, a volume that would have been impossible to process through purely physical infrastructure during the same period. High Courts across the country reported measurable reductions in short-cause and bail matters pending, attributable in significant part to the ability to conduct these hearings without requiring physical presence.[14]

The BNSS has institutionalised these gains. Section 530 of the BNSS expressly permits the conduct of trials, inquiries, proceedings and depositions through electronic mode, subject to the accused's right to be physically present when required by the court. Electronic service of summons and warrants, recognised under Section 531, addresses one of the most persistent

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf visited on 17.01.2026

[12] *Hussainara Khatoon & Ors. v. Home Secretary, State of Bihar* (1980) 1 SCC 81.

[13] *Id*, see also, *Kartar Singh v. State of Punja*b (1994) 3 SCC 569 (speedy trial linked to Article 21).

[14] *Supreme Court of India, Annual Report 2022–23* (New Delhi, 2023); National Informatics Centre, *eCourts* Mission Mode Project Phase III, Government of India (2023); see also, *Swapnil Tripathi v. Supreme Court of India,* (2018) 10 SCC 628 (live-streaming of court proceedings upheld).

sources of procedural delay: the failure of physical service. The e-FIR mechanism under Section 173(1) enables first information reports to be lodged electronically, reducing delay at the critical investigative commencement stage.[15]

V. Speedy Trial and the Reduction of Undertrial Detention

Social justice dimensions of technological court infrastructure are most acute in the context of undertrial detention. India's prison population comprises, consistently, over 75 per cent undertrials— individuals incarcerated pending trial, not as a consequence of conviction. Many undertrials spend periods in custody that substantially exceed the maximum sentence for the offence with which they are charged, a situation that represents an acute violation of the presumption of innocence and the principles of proportionality. Virtual bail hearings, by eliminating the logistical barriers that previously delayed scheduling—production of the undertrial from a distant jail, availability of physical courtroom space—offer a meaningful mechanism for reducing this injustice.[16]

The BNSS's time-bound investigation and trial completion provisions—charge-framing within 60 days, judgment within 30 to 45 days of final arguments—when combined with virtual hearing infrastructure, create a structural environment more conducive to speedy disposal than any prior legislative arrangement. The *eCourts* Mission Mode Project Phase III, with its ambition to achieve a fully digital case lifecycle, represents an administrative complement to the legislative framework that, if implemented with fidelity, could materially reduce the volume of cases classified as "older than five years" on the National Judicial Data Grid.[17]

VI. EVIDENTIARY ARCHITECTURE OF THE BSA, 2023

To study the challenges to evidence law, a fairly detailed examination of s. 63 BSA has been undertaken in reference to electronic record framework, metadata recognition and the deepfake

[15] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 530: Trials and Proceedings Through Electronic Mode; *Department of Justice, Report on Arrears and Backlog: Creating Additional Judicial (wo)manpower* (MoL&J, 2014), available at, https://lawcommissionofindia.nic.in/report_twentieth/, visited on 20 January, 2026, (chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2022/08/2022081643.pdf.

[16]National Judicial Data Grid, District and Taluka Court Pendency Dashboard, available at, https://njdg.ecourts.gov.in, visited on 26 January 2026, and Law Commission of India, Report No. 245, Arrears and Backlog: Creating Additional Judicial (wo)manpower (2014), *Id*.

[17] e-Courts Mission Mode Project, Phase III Document (Department of Justice, Ministry of Law and Justice, Government of India, 2023); High Court of Bombay, Annual Report 2022–23, noting measurable reduction in pending matters attributable partly to virtual hearings.

or AI generated evidence. This leads into evaluating the evidentiary architecture of the BSA, 2023.

6.1 Electronic Records and Framework of s. 63, BSA

The Indian Evidence Act, 1872 was designed for a world of paper and ink. Its foundational categories— oral evidence and documentary evidence— were adequate for their time but proved increasingly strained as electronic communication became the primary medium of human interaction. The amendments introduced through the Information Technology Act, 2000 (Sections 65A and 65B) were a significant intervention, but their implementation generated protracted judicial controversy that the Supreme Court sought to resolve in *Anvar P.V. v. P.K. Basheer*[18] and later *Arjun Panditrao v. Kailash Kushanrao Gorantyal,*[19] without fully settling the practical difficulties experienced by litigants and investigators.[20]

Section 63 of the BSA represents a comprehensive restatement and improvement of the electronic record admissibility framework. It requires a certificate identifying the electronic record, describing the device on which it was produced, confirming the device's proper operation during the relevant period, and certifying that the record was produced from activities regularly carried on by the organisation. Critically, the BSA clarifies that certificate requirements may be relaxed where the original device is produced for inspection, and extends the electronic records category to expressly encompass metadata, server logs, social media communications, GPS data, cloud records and AI-generated outputs—each of which presented interpretive difficulties under the predecessor regime.

The significance of metadata as evidence cannot be overstated in the digital age: a WhatsApp message not only conveys its text but generates metadata indicating time of sending, the device from which it was dispatched, read receipts, and geolocation of both parties at the moment of transmission. This secondary layer of digital information frequently proves more reliable, and less susceptible to manipulation, than the message content itself. The BSA's explicit recognition of metadata within the definition of electronic records is therefore a materially significant

[18] *Supra*, n. 5, (2014) 10 SCC 473.
[19] *Id,* (2020) 7 SCC 1.
[20] Digital Personal Data Protection Act, 2023, No. 22 of 2023; Vrinda Bhandari & Faiza Rahman, "India's New Data Protection Act: A Critical Analysis" (2024) *36 National Law School of India Review 45.*

development for investigative practice and evidentiary law alike.[21]

VII. Deepfakes, AI-Generated Evidence and Evidentiary Integrity

The very technological capacities that make digital evidence powerful also render it peculiarly vulnerable to fabrication and manipulation. Deepfake technology—the use of generative artificial intelligence to produce video, audio, or image content depicting events that did not occur—represents perhaps the most serious evidentiary integrity challenge that courts will face in the coming decade. Unlike traditional document forgery, which required specialist skill and left detectable physical traces, deepfakes can be produced by individuals with modest technical capability using freely available software, and may be indistinguishable to the human eye even upon careful examination.[22]

The BSA addresses this challenge only obliquely. Section 63, read with its Explanation, provides that artificially generated electronic records are subject to authentication requirements; the BSA permits expert opinion on the functioning of computer systems and by extension on the authenticity of digitally generated content. However, the statute does not specify standards for deepfake detection, does not mandate independent forensic examination before AI-generated content is admitted against an accused, and does not impose a disclosure obligation on the party adducing such content to notify the adverse party of its AI-generated provenance.

Courts will accordingly be required to develop admissibility jurisprudence in this domain largely through case law, in the absence of a gatekeeping standard equivalent to the Daubert doctrine. The risk of wrongful conviction based on fabricated digital evidence—a risk magnified by the authority that visual evidence commands over judicial reasoning—is not theoretical; it is an imminent practical danger that warrants urgent legislative attention.[23]

VIII. WARNING BELLS FOR A DIGITAL CRIMINAL JUSTICE SYSTEM

The Five critical risks that pose as perils or warning bells to digitalisation in the criminal justice

[21] Police and Criminal Evidence Act 1984 (UK), Code D, revised 2023; Law Commission (UK), Digital Evidence and Electronic Disclosure (Consultation Paper No. 264, 2022).

[22] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993); see also, *State v. Loomis,* 881 N.W. 2d 749 (Wis. 2026) upholding the use of COMPAS recidivism algorithm at sentencing while raising transparency concerns; see also, Engel, C., Linhardt, L. & Schubert, M. "Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism," *Artif Intell Law* 33, 383–404 (2025), https://doi.org/10.1007/s10506-024-09389-8.

[23] Bobby Chesney & Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security," *(2019) 107 California Law Review 1753;* see also, s. 63 BSA: Explanation— artificially generated electronic records subject to authentication.

system. These are analysed in greater details and have been categorised as data privacy, particularly as seen in the post-*Puttaswamy* era, executive overreach, algorithmic bias, evidentiary complexities, and the digital divide in access to justice.

8.1 Data Privacy and the Surveillance State

The greatest systemic risk posed by the technological transformation of criminal justice is not the failure of any individual technology—it is the emergence of a pervasive surveillance infrastructure whose data collection capacities far exceed the legitimate needs of criminal investigation and whose boundaries are inadequately defined by law. The nine-judge constitutional bench in *K. S. Puttaswamy v. Union of India*[24] unanimously recognised informational privacy as a fundamental right under Article 21, holding that the State's power to collect and process personal data must satisfy a four-fold test of legality, legitimate aim, proportionality and procedural guarantees.[25]

India's Digital Personal Data Protection Act, 2023 represents a significant step toward a statutory privacy framework, but it explicitly exempts state agencies acting in the interests of sovereignty, security and public order from key data protection obligations. This creates a structural lacuna: precisely the contexts in which privacy protections are most urgently required—law enforcement, intelligence gathering, criminal investigation—are those in which the statutory framework is most attenuated. The result is a legal architecture that proclaims privacy as a constitutional right in doctrine while creating substantial space for its de facto erosion in practice.[26]

CCTV surveillance networks, automated facial recognition deployments, call detail record analysis, social media monitoring, location tracking and the emerging practice of intercepting encrypted communications all generate vast repositories of personal data about individuals who may never be subjects of criminal investigation. The aggregation of such data— individually innocuous observations that in combination yield detailed behavioural profiles— has been characterised by Shoshana Zuboff as the hallmark of "surveillance capitalism." When the State becomes the primary beneficiary of such aggregation, the criminal justice system risks

[24] (2017) 10 SCC 1.
[25]Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1; see also, I*d,* on right to privacy recognised as a fundamental right.
[26]Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India); Vrinda Bhandari & Faiza Rahman, "India's New Data Protection Act: A Critical Analysis" *(2024) 36 National Law School of India Review 45.*

transformation from an instrument of individual accountability into a mechanism of social control.[27]

IX. Executive Overreach and Accountability Deficits

Technology does not merely change what the executive can do— it changes the ratio of executive action to judicial oversight. Traditional investigative techniques— physical search, witness interview, surveillance on the street— were constrained by resource limitations that functioned, incidentally, as a check on arbitrariness. Mass digital surveillance is constrained by no equivalent resource bottleneck: once infrastructure is in place, monitoring thousands of individuals costs little more than monitoring one. This asymmetry demands proportionally more robust legal safeguards, yet the BSA and BNSS do not institute corresponding improvements in judicial authorisation requirements for invasive digital investigative techniques.[28]

The handcuffing provision in Section 43 BNSS— creating a statutory basis for a practice the Supreme Court in *Prem Shankar Shukla*[29] had confined to case-specific judicial necessity— is indicative of a broader tendency in the new legislation to expand executive power without proportionate accountability. Similarly, the extension of police custody periods, the broadening of preventive detention triggers, and the absence of a mandatory, independent police oversight mechanism reflect a legislative calculus that consistently privileges executive capability over executive accountability.[30]

The absence of a statutory exclusionary rule— requiring courts to exclude evidence obtained through constitutional violations— further diminishes accountability incentives. Indian courts, following *Pooran Mal v. Director of Inspection,*[31] admit illegally obtained evidence if relevant, removing the disincentive that an exclusionary rule would otherwise create for unconstitutional investigative conduct. In a digital environment where a single unlawful search of a mobile

[27]Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs, 2019); Ranjit Singh, "Surveillance Capitalism and the Criminal Justice System in India" *(2022) 62(3) JILI 310.*

[28] Surveillance Studies Network, *A Report on the Surveillance Society (2006);* Bhairav Acharya, "Watching the Watchmen: CCTV Surveillance, Privacy and the Panopticon in India" *(2012) 54(4) JILI* 557.

[29] *Prem Shankar Shukla v. Delhi Administration* (1980) 3 SCC 526.

[30] *D. K. Basu v. State of West Bengal (1997) 1 SCC 416* laying guidelines on custodial rights; see also, UN Standard Minimum Rules for the Treatment of Prisoners (Nelson Mandela Rules), GA Res. 70/175 (2015) Rules 47-48.

[31] (1974) 1 SCC 345.

device may yield years of personal communications, the failure to create an exclusionary rule is a structural accountability deficit of considerable significance.[32]

X. Algorithmic Justice and the Risk of Automated Bias

Predictive policing algorithms, risk assessment instruments at bail and sentencing, and facial recognition systems in investigation share a common epistemological feature: they generate probabilistic outputs derived from historical data that reflects past patterns of enforcement. Where those enforcement patterns are themselves the product of discriminatory policing— where particular communities have been subjected to disproportionate surveillance, arrest and prosecution— the algorithm learns and perpetuates that discrimination, conferring upon it a false authority of mathematical objectivity. Bernard Harcourt's critique of actuarial penology— that prediction instruments shift punishment from the established fact of past conduct to the statistical probability of future behaviour— applies with particular force to communities already over-policed.[33]

The Wisconsin Supreme Court in *State v. Loomis*[34] upheld the use of the COMPAS recidivism algorithm at sentencing, even while acknowledging that the defendant could not access or challenge the proprietary algorithm's methodology. This transparency deficit is constitutionally problematic— the right to a fair trial, protected under Article 21 and elaborated through the Supreme Court's due process jurisprudence, must encompass a right to understand and contest the basis on which judicial decisions adverse to one's liberty are made. An algorithmic determination, however sophisticated, that cannot be examined, challenged or falsified does not provide the procedural foundation that constitutional fairness demands.[35]

India has not yet developed a statutory or judicial framework governing the admissibility and evidentiary weight of algorithmic outputs in criminal proceedings. NITI Aayog's Responsible AI principles and the proposed National Data Governance Framework represent policy-level

[32] *K. S. Puttaswamy (Aadhaar) v. Union of India* (2019) 1 SCC 1 SC laid the four-fold proportionality test: *legality, legitimate aim, proportionate means, and procedural guarantees* — applicable to surveillance technology in policing.
[33] Bernard Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*, University of Chicago Press, 2007; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Crown, 2016.
[34] Supra. notes. 10 and 23.
[35] Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York University Press, 2017; Rashida Richardson, Jason Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice" (2019) 94 *New York University Law Review Online 192.*

engagement, but the absence of binding legal standards for algorithmic transparency, explainability and demographic impact assessment in the criminal justice context remains a serious gap that the BNS-BNSS-BSA triptych does nothing to fill.[36]

XI. Evidentiary Complexities in the Digital Age

The promise of digital evidence, which basks in its objectivity, permanence and precision, also conceals significant evidentiary complexities that courts and practitioners must navigate with care. Electronic records may be authentic yet misleading: a message may be genuine but deliberately sent to create a false impression; metadata may be manipulated without affecting visible content; digital forensics may recover deleted communications while losing the context necessary for accurate interpretation. The law of evidence has historically been concerned not merely with relevance but with reliability; the challenge for the BSA framework is to ensure that the admission of digital evidence does not conflate technological novelty with epistemic authority.[37]

The certification requirement of Section 63 BSA, while designed to authenticate electronic records, creates practical difficulties of considerable scope. Major communication platforms, such as, WhatsApp, Google, Meta — are incorporated in foreign jurisdictions and are not subject to Indian court orders in the same manner as domestic entities. Obtaining a Section 63 certificate from a foreign platform requires either the platform's voluntary cooperation or the cumbersome process of Mutual Legal Assistance Treaty requests, neither of which is reliably swift or complete. In practice, courts have been compelled to develop flexible interpretations that risk undermining the certification requirement's integrity[38]

XII. The Digital Divide and Access to Justice

Technology's democratising potential in justice delivery is conditioned on a foundational assumption: that all participants in legal proceedings can access and use the technology in question. This assumption is empirically problematic in India's context. While internet

[36]European Commission, Proposal for a Regulation on a European Approach for Artificial Intelligence (AI Act), COM (2021) 206 final; NITI Aayog, Responsible AI for All: Applying the Principles for Responsible AI (2021); UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021

[37] See also, Innocence Project, DNA Exonerations in the United States (2024), available at https://innocenceproject.org/dna-exonerations-in-the-united-states, visited on 20 January, 2026.

[38] Deepanker Singhal & Pragya Narang, "AI-Generated Evidence in Indian Courts: Admissibility, Reliability and the Chain of Custody Challenge," *Indian Journal of Integrated Research in Law*, Vol. V Issue V, pp. 186-204.

penetration has expanded dramatically, significant rural-urban, gender and socioeconomic digital divides persist. The International Telecommunication Union's 2023 data records that despite approximately 900 million internet subscribers in India, meaningful digital access for legal purposes—requiring stable connectivity, appropriate devices, digital literacy, and private secure spaces—remains unavailable to a substantial proportion of the population.[39]

Virtual hearings that benefit educated, urban, economically stable litigants may simultaneously disadvantage rural, poor, and marginalised participants who cannot attend proceedings, access case records, challenge evidence, or communicate with counsel through digital means. The undertrial in a poorly equipped jail, the agricultural labourer witness in a village with intermittent electricity, the domestic violence survivor whose abuser controls household digital devices—for each of these individuals, a technology-first justice system creates barriers rather than access. The BNSS introduces provisions enabling electronic communication of processes and virtual production of accused persons; however, it does not expressly incorporate mandatory accessibility safeguards (such as assistive technological support, accommodations for persons with disabilities, or protections addressing the digital divide) to ensure meaningful participation in virtual proceedings.[40]

XIII. COMPARATIVE PERSPECTIVES AND THE WAY FORWARD

International comparative analysis offers both cautionary tales and constructive models. The General Data Protection Regulation provides a framework of data minimisation, purpose limitation and enforceable individual rights that constrain the collection and use of personal data,[41] including in criminal justice contexts when read alongside the Law Enforcement Directive, which specifically governs data processing by competent authorities for law

[39] International Telecommunication Union, Measuring Digital Development: Facts and Figures 2023, *ITU Publications, Geneva, 2023*; Telecom Regulatory Authority of India, *Annual Report 2022–23,* recording approximately 900 million internet subscribers, yet finding significant rural-urban and gender digital divides persist.

[40] *The Bharatiya Nagarik Suraksha Sanhita, 2023*, ss. 63, 336 (providing for electronic service of summons and use of audio-video electronic means in inquiry, trial and proceedings, without prescribing mandatory accessibility or digital accommodation safeguards). See also, *In Re: Guidelines for Court Functioning Through Video Conferencing During COVID-19 Pandemic*, (2020) 6 SCC 686, wherein, the Supreme Court of India recognised validity of virtual hearings while emphasizing fairness and access concerns; see also *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 which underscored the centrality of internet access to exercise of fundamental rights, relevant to concerns of digital exclusion.

[41] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (*General Data Protection Regulation*), 2016 O.J. (L 119) 1, arts. 5(1)(b)–(c), 6, 12–22.

enforcement purposes.[42] In the United Kingdom, the Forensic Science Regulator, placed on a statutory footing under the Forensic Science Regulator Act, 2021, imposes quality standards and codes of practice on forensic science providers.[43] Concerns regarding the scientific validity and reliability of several pattern-based forensic disciplines were prominently articulated by the National Academy of Sciences in its landmark 2009 report on forensic science.[44]

The EU's proposed Artificial Intelligence Act classifies certain AI systems used in law enforcement and criminal justice—including predictive policing tools and AI-based risk assessment systems—as "high-risk" applications subject to stringent obligations relating to risk management, transparency, accuracy, documentation, and human oversight.[45] This emerging regulatory framework provides a legislative template that comparative jurisdictions, including India, may carefully examine. The Innocence Project has documented over 375 exonerations in the United States secured through post-conviction DNA testing, many involving convictions grounded in unreliable or overstated forensic science evidence.[46] These findings echo broader scientific critiques, including those advanced by the National Academy of Sciences, underscoring the dual capacity of technological innovation to both produce and correct miscarriages of justice.[47]

For India, the path forward requires legislative and institutional action across several dimensions. A dedicated forensic science regulatory framework—providing for mandatory accreditation of laboratories and certification standards for experts—would align with existing quality-control mechanisms such as those overseen by the National Accreditation Board for Testing and Calibration Laboratories and respond to longstanding scientific critiques regarding

[42] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (*Law Enforcement Directive*), 2016 O.J. (L 119) 89, arts. 4, 8, 13–16.

[43] *Forensic Science Regulator Act 2021*, c. 14 (U.K.), ss. 1–6 which establish the Forensic Science Regulator and empower issuance of statutory codes of practice and compliance mechanisms.

[44] National Research Council of the National Academy of Sciences, *Strengthening Forensic Science in the United States: A Path Forward*, National Academies Press, 2009, pp. 7–8, pp. 87–110, highlighting systemic issues in pattern-comparison disciplines such as bite mark, hair, and toolmark analysis.

[45] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (21 April 2021), Articles 6, 8–15 & Annex III— classifying AI systems used in law enforcement and administration of justice as high-risk and prescribing requirements of transparency, accuracy, risk management, and human oversight.

[46] Supra, n. 37, documenting over 375 DNA-based exonerations and identifying contributing factors including misapplied forensic science. See also, supra n. 4.

[47] *Supra* n. 44, see, critiquing methodological weaknesses in several pattern-comparison forensic disciplines.

the reliability of forensic disciplines.[48] Comparative experience, including the statutory model adopted under the Forensic Science Regulator Act 2021 (U.K.), further illustrates the importance of an independent regulator empowered to issue binding codes of practice.[49]

The Digital Personal Data Protection Act, 2023 presently provides exemptions for processing by the State in specified circumstances, including law enforcement functions, raising concerns regarding proportionality and necessity safeguards[50] The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), which replaces the Code of Criminal Procedure, 1973, does not codify a general exclusionary rule for improperly obtained evidence, leaving admissibility primarily to judicial discretion under the Indian Evidence Act, 1872 framework.[51] Comparative constitutional jurisprudence—most prominently under the Fourth Amendment to the U.S. Constitution—has developed a structured exclusionary doctrine to deter unlawful searches and seizures.[52] Finally, emerging scholarship on algorithmic governance underscores the need for statutory regulation of automated decision-support systems in criminal justice, including requirements of explainability, auditability, demographic impact assessment, and meaningful human oversight.[53]

XIV. CONCLUSION

Technological advance in criminal justice is neither an unqualified good nor an unqualified threat—it is a set of powerful tools whose effects depend entirely on the normative framework within which they are deployed and the institutional vigilance with which their exercise is scrutinised. DNA exoneration and mass surveillance are both products of the same technological revolution; deepfake fabrication and deepfake detection are the obverse and reverse of the same algorithmic capability. The question that confronts Indian criminal

[48] *Ibid;* see also role of accreditation bodies such as the National Accreditation Board for Testing and Calibration Laboratories (NABL) operating under the Quality Council of India.

[49] *Forensic Science Regulator Act 2021* (U.K.), c. 14, ss. 1–9— placing the Forensic Science Regulator on a statutory footing and empowering issuance of binding codes of practice.

[50] *Digital Personal Data Protection Act, 2023* (Act 22 of 2023), s. 17 (providing exemptions for processing by the State and its instrumentalities in specified circumstances); see also ss. 7 & 8— general obligations of data fiduciaries.

[51] *Bharatiya Nagarik Suraksha Sanhita, 2023* (Act 46 of 2023); cf. *Indian Evidence Act, 1872*, ss. 5, 24, 27; see *Pooran Mal v. Director of Inspection (Investigation)*, (1974) 1 SCC 345, holding that evidence obtained through illegal search is not per se inadmissible under Indian law.

[52] See *Mapp v. Ohio*, 367 U.S. 643 (1961) (incorporating the exclusionary rule against the States); see also Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* (6th ed., West Academic, 2020).

[53] See Sandra Wachter, Brent Mittelstadt & Chris Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 *Harvard Journal of Law & Technology* 841; see also Andrew D. Selbst et al., "Fairness and Abstraction in Sociotechnical Systems" *(2019) 103 Conference on Fairness, Accountability, and Transparency (FAT) Proceedings* 59.

jurisprudence at this pivotal moment is not whether to embrace technology—that question has effectively been answered by the BNS, BNSS and BSA— but how to govern its embrace with constitutional fidelity.

The Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam represent an ambitious, overdue and largely commendable attempt to equip India's criminal justice apparatus for the digital age. Their recognition of electronic evidence, virtual proceedings, forensic imperatives and victim information rights marks genuine progress. Yet genuine progress is not sufficient progress. The perils catalogued in this paper— privacy erosion, executive overreach, algorithmic discrimination, evidentiary vulnerability, and the digital divide— are not hypothetical future risks; they are present realities that the new framework inadequately addresses.

The jurisprudential tradition of the Supreme Court of India— which has, from *Hussainara Khatoon* to *Puttaswamy,* consistently expanded the frontier of constitutional protection for individual liberty against state power—provides a foundation of principle adequate to meet these challenges. What is required is legislative will to translate constitutional principle into operative statutory safeguards, institutional capacity to implement those safeguards effectively, and judicial vigilance to ensure that technology serves the ends of justice rather than the ends of those who deploy it. The hour calls not for technophobia, but for technologically informed constitutionalism. Rejoice, certainly—but reflect, always.