LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

The Bharatiya Sakshya Adhiniyam, 2023 and the Evolution of Evidentiary Standards: Implications for Judicial Remedies

Author
Manish Tundelkar

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

The Bharatiya Sakshya Adhiniyam, 2023 and the Evolution of Evidentiary Standards: Implications for Judicial Remedies

Manish Tundelkar
LLM (Criminal Law)
Amity Institute of Advanced Legal Studies
Amity University, Noida, (UP)

Abstract

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 marks a significant development in India's criminal justice system, replacing the colonial-era Indian Evidence Act, 1872 with a modern framework designed to address contemporary evidentiary challenges. The new legislation seeks to align the law of evidence with technological advancements, changing modes of communication, and the growing reliance on electronic records in judicial proceedings. By recognizing digital and electronic evidence more comprehensively, the Act aims to enhance the efficiency, transparency, and reliability of the adjudicatory process.

This research paper critically examines the evolution of evidentiary standards under the Bharatiya Sakshya Adhiniyam, 2023 and analyzes its implications for judicial remedies in India. The study explores the key reforms introduced by the legislation, including the expanded recognition of electronic and digital evidence, revised provisions relating to admissibility, documentary evidence, presumptions, and witness testimony. Particular attention is paid to the manner in which these reforms influence the burden of proof, standards of reliability, and the overall administration of justice.

The paper further evaluates the impact of the new evidentiary framework on judicial decision-making and the effectiveness of remedies available to litigants in both civil and criminal proceedings. It examines whether the incorporation of technology-oriented provisions adequately addresses issues such as authenticity, integrity, and admissibility of electronic evidence while safeguarding the principles of fairness, due process, and natural justice. The study also compares selected provisions of the Bharatiya Sakshya Adhiniyam, 2023 with those of the Indian Evidence Act, 1872 to identify areas of continuity and transformation.

Adopting a doctrinal and analytical methodology, the research relies on statutory provisions, judicial precedents, legislative debates, and scholarly literature. The study concludes that while the Bharatiya Sakshya Adhiniyam, 2023 represents a progressive step toward modernizing India's evidentiary regime, challenges relating to implementation, digital literacy, forensic infrastructure, and judicial interpretation remain significant. The paper suggests measures to strengthen evidentiary standards and ensure that judicial remedies remain effective, accessible, and responsive to the demands of a rapidly evolving digital society.

Keywords: *Bharatiya Sakshya Adhiniyam, 2023, Evidence Law, Digital Evidence, Criminal Justice System, Judicial Decision-Making.*

Introduction

The implementation of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) is the most significant structural realignment of the Indian evidentiary field since the late nineteenth century. The Indian Evidence Act, 1872 (IEA) was the inflexible, but still becoming obsolete, paradigm of judicial truth-seeking and had been fashioned in a period when the concept of evidence was virtually synonymous with physical documents and oral witness testimony. Although the IEA was a masterpiece of Victorian draftsmanship, it was based on a paper-based bureaucracy and a linear time and space concept. The BSA, however, turns out to be a paradigm shift, the realization of the fact that in the modern era, the overwhelming majority of the legally relevant facts are created, relayed, and stored in digital forms or are embodied in the biological indicators of individuals. This is not just an update of modernisation; it is a radical rethinking of the notion of Sakshya the act of witnessing in order to adjust to a world in which semiconductor memory, communication equipment and algorithmic markers have replaced the quill and the ledger.

In the past, the IEA had difficulties in supporting the specifics of digital information. In an effort to provide a stop-gap, the Information Technology Act, 2000 tried to add Sections 65A and 65B to the IEA that created an incomprehensible and widely mistaken regime over admissibility of electronic records. These were often a source of incompatible judicial interpretations, which swung between the liberal standards of admission apparent in such cases as State (NCT of Delhi) v. Navjot Sandhu[1] and the rigid certification requirements of Anvar P.V. v. P.K. Basheer[2]. The BSA is meant to put to an end these years of legal gray areas by developing a more comprehensive and technology-focused set of evidentiary code to put electronic and digital records on an equal legal plane with the rest of traditional documentary evidence. The BSA is aimed at streamlining the process of trial and increasing the persuasiveness of digital evidence by reclassifying digital records in particular circumstances and broadening definitions of document and oral evidence.

The change in philosophical approach with the BSA is in the de-colonization of Indian jurisprudence of the name of the Bar, such as of Barrister and Vakil, with Advocate, and the name of the Crown with the name of a modern and sovereign nation. Nevertheless, the essence of this change is Section 2 that has seen the definitions of document and evidence broadened to include the digital realities of

[1] State (NCT of Delhi) v. Navjot Sandhu, 2005 11 SCC 600
[2] P.V. v. P.K. Basheer, Air 2015 Sc 180

the twenty first century. An electronic record on emails, server logs, smartphones, websites and locational evidence now constitutes a document, whereas an oral evidence comprises of statements made electronically with witnesses and victims being able to give evidence electronically. This inclusivity is not just a convenience factor, but a realization that the digital trail of an individual left by his location data, voice messages, and logs left on his servers is often a more factual and resistant-to-tampering depiction of events than is possible by relying on human memory alone[3].

Biometric evidence takes a niche position in this new regime and is a highly sensitive and specialized one. With technologies such as facial recognition, iris scans, and DNA profiling becoming ubiquitous in policing and business, the law will have to contend with the dual realities of their being both an extremely accurate form of identification and potentially invasive surveillance technology. Biometric data cannot be changed; an individual can change their password, but he or she cannot change his or her fingerprints or retinal pattern. This irreversibility requires a high standard of evidentiary that accrues safety and technical integrity of the sensors and algorithms involved in the capture of such data. The BSA handles this by a refreshed certification process in Section 63 to have the statement of an operator and also the authentication of an expert so that the digital templates have not been tampered or corrupted.

Judicial review under the BSA has also changed to that of a mere fact-finder to that of a close examiner of a technologically challenging evidence. The judges now have a responsibility to evaluate the probative value of forensic evidence and this includes taking an inquiry into the chain-of-custody procedures, hash analysis, and the qualifications of electronic examiners. It has been a difficult process, with numerous judicial officers and legal practitioners not having been trained in the specifics of digital forensics or how algorithms can be biased. Moreover, bits and bytes are fragile and digital evidence can be easily hacked, manipulated and give rise to so-called deepfakes, which demands that the court should take care of so-called travesties of justice caused by untested electronic evidence.

Parallel to these developments in evidence, the law on judicial remedies has been broadened by the Bharatiya Nyaya Sanhita (BNS), and the Digital Personal Data Protection Act, 2023 (DPDPA). The victims of biometric data theft or any other form of unauthorized disclosure are currently in a position of accessing a liability matrix that incorporates a substantial civil compensation, administrative fines, and criminal incarceration on data theft, currently a property crime. The

[3] Stevens, Rock, and Jeffrey Biller. "Offensive Digital Countermeasures: Exploring the Implications for Governments." The Cyber Defense Review, vol. 3, no. 3, 2018, pp. 93–114. JSTOR, https://www-jstor-org.rgnul.remotexs.in/stable/26555000. Accessed 26 Mar. 2026.

establishment of the Data Protection Board of India (DPBI) has given a fresh opportunity of seeking damages through a regulatory board, whereas the old courts still act as the custodians of the constitutional rights. The historic Puttaswamy case that established privacy as a basic right through Article 21 is the constitutional North Star of this whole regime and privacy invasion by any state should be legal, necessary and proportionate.

This chapter examines the complex aspects of this new evidentiary regime which considers the admissibility standards of electronic records, the technical integrity of biometric data and how the judiciary is changing its role in balancing the imperatives of investigation with the constitutional right of a fair trial and due process. It evaluates whether the BSA, in a bid to make things simple, and make them digital, has given rise to new procedural paradoxes, and analyzes the sufficiency of the provided remedies to guard people against the dangers of digital society. However, the success of the BSA will be determined by the capability of judges of the legal ecosystem, lawyers, and forensic experts to convert these legislative prescriptions into a practice that does not only bring justice but is perceived to bring justice in the digital age[4].

5.1 Admissibility, Authenticity, and the Enigma of Section 63

The part of the Bharatiya Sakshya Adhiniyam, 2023, that will be the subject of the treatment of electronic and electronic records is found in Section 61, 62, and 63, which use the place of the highly litigious Section 65A and 65B of the Indian Evidence Act. These provisions have a general goal of ensuring that digital evidence is not locked out simply due to its electronic nature and at the same time sets strict criteria that can be used to ascertain its authenticity. Section 61 gives the principles: nothing in the Adhiniyam shall be applied to deprive the admissibility of an electronic or digital record as evidence on the ground that the record is an electronic or digital record. This non-discrimination clause gives digital information the same legal standing as paperwork eliminating the historical bias that electronic records were inferior to paper records.

The rule of admissibility, however, is still subjected to the difference between primary and secondary evidence. Section 57 of the BSA in a radical step reclassifies the digital records as primary evidence. In the same way, the Explanation 4 to Section 57 says that in cases where the production of a digital record is through proper custody, the same constitutes primary evidence unless it is refuted. This acknowledges that in most contemporary settings, including logs of servers or blockchain-like interactions, the original is a distributed or system generated document that is functionally equivalent to any output obtained out of

[4] Marks, Mailise R., et al. "RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY." *Tort Trial & Insurance Practice Law Journal*, vol. 56, no. 2, 2021, pp. 303–20. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/27306022. Accessed 26 Mar. 2026.

it. Also, the BSA explains that in the case where an electronic record has been stored in more than one file in sequence, each file is considered primary evidence. This change intending to make it a status of a Primary Evidence is meant to simplify the trial process but it poses a legal contradiction to the current demand of certification.

Section 63 of the BSA defines the admissibility of electronic records in the so-called self-contained code, which generally preserves the words of the former Section 65B and substantially improves the procedure. It provides that any information stored in an electronic record and printed on paper or stored on optic or magnetic media will be considered a document provided that it satisfies four conditions. First, the device of computer or communication must have been frequently utilized to create or store information towards any activity that was commonly being executed in that time by an individual who lawfully had possession of the device. Secondly, the information contained in the record should have been fed into the machine during that period, in the normal discharge of such activities. Third, the device is to have been in proper operation or in a case where it was not, the malfunction should not have had any influence on the precision of the record. The last thing is that the information in the output must be reproduced or derived of the information that is inputted in the device[5].

The most severe barrier to the admissibility of digital evidence is the requirement of certification as in Section 63(4). This certificate has now to be of a more stringent two-tiered structure under the BSA. It has to establish the electronic record, and explain how it was made but should be signed by two persons, the one who was in control of the computer or the communication equipment and an expert. This is a significant departure of IEA where a certificate by the individual in charge was usually deemed acceptable. It is evident that the goal of the legislation is to provide a technical confirmation to the evidence as digital data is very prone to tampering and hacking. Yet, the credentials and qualification requirements of these experts are not set out in the BSA, which raises the issue of procedural disparities and the possibility of a battle of experts in court.

The legal meaning of these certification requirements has long been difficult. The Supreme Court in Anvar P.V. v. P.K. Basheer (2014)[6] has ruled that the certificate is a preconditioned condition to admissibility of electronic records, which was repeated and explained in the Arjun Panditrao Khotkar v. Gorantyal, Kailash Kushanrao (2020).[7] Arjun Panditrao determined that the certificate should be produced only in the situation when the individual who creates the evidence will

---

[5] Goodman, Eduard F. "Your Duty If You Discover a Data Breach." *GPSolo*, vol. 25, no. 8, 2008, pp. 16–19. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/23630012. Accessed 26 Mar. 2026.
[6] Air 2015 Sc 180
[7] AIRONLINE 2020 SC 641

not have the original device. This judicial trend seems to be followed in the BSA in categorizing the digital records as primary evidence where the records are formed by the rightful custody, though the non-obstante clause of 63(1) Notwithstanding anything contained in this Adhiniyam) arguably results in the certificate being obligatory on all the electronic records whether they are primary evidence or secondary evidence. This certification enigma can provoke a possible bottleneck in the judicial system, because parties can have difficulties receiving certificates issued by experts or third-party service providers such as social media giants, or telecom operators.

The changing role of the courts to this effect is to play a gatekeeper of the digital truth. Judiciary cannot just examine the presence of the certificate but should also evaluate the chain of custody, the process of tracing evidence since its origin at the place of collection through its presentation in the court. Any interruption to this chain of evidence like inappropriate handling, storage, and unauthorized access may hamper credibility of the evidence and rejection may occur. The BSA along with the Bharatiya Nagarik Suraksha Sanhita (BNSS) requires investigative agencies to observe a set of unambiguous procedural requirements when it comes to the seizure and preservation of digital evidence, the application of so-called Faraday bags to prevent remote wiping, and the availability of the presence of qualified forensic experts during search and seizure activities.

Critical questions are also raised by the old law towards the new law in terms of pending trials. Section 170 of the BSA proposes the possibility of transitional rules on electronic evidence provided under the old regime, but the courts will have to determine whether a deficient or absent certificate under Section 65 B of the IEA can be corrected or substituted under the new Section 63. This necessitates a subtle judicial practice that is not hyper-technical but at the same time, has a strict criterion of overall reliability. Finally, the BSA is intended to bring a balance between the expectations of a digital society and the conventional legal safeguards of authenticity and integrity. This balance is mainly achieved by the Section 63, whether it is successful or not will be determined by the establishment of a sound digital forensic infrastructure and the ongoing technical education of the judiciary.

5.2 Biometric Evidence: Technical Integrity and Forensic Reliability

Biometric evidence, which includes facial recognition, fingerprint analysis, iris scan, and DNA profiling is the edge of the technological integration in the Indian criminal justice system. With the Bharatiya Sakshya Adhiniyam, the examination of this evidence has ceased to fall into the category of expert opinion and has risen to a better-central pillar of evidence. Section 39 of the BSA maintains the model of expert reports, which asserts that the judgment of a person who is particularly proficient in science or art is a material fact, but it extends it to cover

the judgment of an Examiner of Electronic Evidence as interpreted under the IT Act. This modernization acknowledges that biometric identification is not merely that of the physical pattern anymore; it is that of the algorithmic processing of the digital templates that are held in semiconductor memory[8]. The hardware employed in the capture and the software employed in the analysis of biometric evidence is a factor in the technical integrity of the evidence. Presentation attacks are susceptible to biometric systems, and fraudulent efforts are applied to a sensor with the use of synthetic media, masks, or high-resolution photographs. In order to make sure it is reliable, the judiciary has to refer to international standards like the ISO/IEC 30107 that gives a guideline of how such attacks can be detected and prevented. The accuracy of a biometric system is determined by the error rates, that is, the False Match Rate (FMR) and the False Non-Match Rate (FNMR). These technical measures in the courtroom establish the probative weight of the identification but they are not well comprehended by lawyers. Section 63(4) of the BSA requires the two-tiered certification of the BSA to ensure that this technical scrutiny is incorporated into the books of the law and that an expert is required to testify to the integrity of the biometric system[9].

The gathering and utilization of biometric information in India is majorly controlled by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which defines biometrics as a Sensitive Personal Data. These regulations stipulate that the collection of biometric data must be done with express and prior permission to fulfill a legitimate purpose and that the data collection and subject must be notified of what data is being collected and its purpose. Although the Digital Personal Data Protection Act, 2023, replaces the rules of 2011, it still focuses on the consent but does not differentiate between the sensitive category and the rest of personal data. This move has been condemned as potentially watering down the increased safeguards initially granted to biometric identifiers that are in essence entirely distinct to any other form of data since they are permanent and cannot be replaced[10].

The Criminal Procedure (Identification) Act, 2022, only complicates the biometric environment by increasing the authority of law enforcement to gather biological samples and behavioral characteristics of individuals, including preventive detainees. This Act permits the storage of biometric information up to 75 years with no clear indications of consent or judicial review, which can be

---

[8] Black, Kyle D., et al. "RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY." Tort Trial & Insurance Practice Law Journal, vol. 54, no. 2, 2019, pp. 403–34. JSTOR, https://www-jstor-org.rgnul.remotexs.in/stable/27010241. Accessed 26 Mar. 2026.

[9] BROOKES, JENNIFER, et al. *America's 5G Era: Balancing Big Data and Privacy*. RAND Corporation, 2022. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/resrep42025. Accessed 26 Mar. 2026.

[10] Jia, Mark. "Authoritarian Privacy." *The University of Chicago Law Review*, vol. 91, no. 3, 2024, pp. 733–810. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/27348370. Accessed 26 Mar. 2026.

considered a serious constitutional issue. The courts under the BSA are faced with the challenge of imposing the conditions of technical reliability and constitutional acceptability on the biometric evidence that has been obtained under these broad authority powers. The use of DNA profiling e.g. is classified as an opinion evidence under the BSA in Section 39(1) i.e. it is advisory and as a rule needs corroboration to have a conviction. The quality of DNA evidence relies really hard on the capability of the professional collecting the samples and the strictness with which the chain of custody will be upheld to avoid contamination.

Biometric algorithms also pose the threat of algorithmic bias in the evaluation. Since AI-based applications are utilized to analyze forensic images and predictive policing, transparency related to black box algorithms can become a source of systematic errors and miscarriage of justice. The Indian judicial system has acknowledged that although AI can be used to bolster judicial efficiency, it is not capable of providing the discretionary and interpretative legal tasks with the subtlety and human touch that involves judgment. Moreover, in Selvi v. the Supreme Court. State of Karnataka interpreted compulsory narco-analysis and brain-Mapping to be contrary to mental and bodily privacy, which is an inseparable part of the right against self-incrimination under Article 20(3). With the development of the biometric technologies to even gauge the behavioral characteristics and gait pattern, the courts will need to establish where the boundary between acceptable identification and unconstitutional coercion can be drawn[11].

The hash verification is intrinsically linked with the integrity of biometric records in court. Each biometric template a computerized image of a fingerprint or iris is provided with a hash value, which functions as a digital signature. When there is a modification in the template, the hash value will not be equal and it will give an immediate notification of the tampering. Section 63 of the BSA has a certificate which must be certified by an expert in that these hash values are really a copy of the data taken at the origin. But the reality that is harder to overcome is that the laboratories of the forensic system in India are overloaded and that there is no standardization of the private experts who can be summoned to provide such certificates[12].

The Aadhaar decision was aware of not using biometric identifiers after their use, and the court made it clear that any penetration of a state would be reasonable and targeted to achieve a certain legitimate purpose. Having implemented

[11] SEKHON, NIREJ. "PURPOSE, POLICING, AND THE FOURTH AMENDMENT." The Journal of Criminal Law and Criminology (1973-), vol. 107, no. 1, 2017, pp. 65–130. JSTOR, https://www-jstor-org.rgnul.remotexs.in/stable/48572209. Accessed 26 Mar. 2026.

[12] Sandvik, Kristin Bergtora. "Digital Refugee Lawyering: Risk, Legal Knowledge, and Accountability." *Refugee Survey Quarterly*, vol. 40, no. 4, 2021, pp. 414–32. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/48812880. Accessed 26 Mar. 2026.

biometric systems to make commercial payments and to log into the system, the digital economy in which voluntariness may be an illusion is created. Judiciary is expected to make sure that the convenience of biometric authentication does not lead to systemic exclusion and a surveillance regime is not established. With biometric evidence getting into the very core of judicial process through the BSA, the courts could not maintain the standard of convenience inaccessible to, and undeserving of, constitutionality. Finally, biometric evidence reliability is determined by a strong system of technical verification, forensic standard, and constitutional control. The BSA offers the legal foundation of this framework but its success will lie in the ability of the judicial system to adjust to the technological reality of biometrics. This does not only entail providing more explicit procedural guidelines to certify digital records but also a better perception of the ethical and technical risks pertaining to biometric surveillance. The application of biometric evidence should be a two-sided sword in a democracy under the rule of law, which maximizes accuracy in the evidences and also tightly controls the autonomy and dignity of the individual[13].

5.3 Judicial Remedies: Liability, Compensation, and Data Theft

The Bharatiya Sakshya Adhiniyam, the Bharatiya Nyaya Sanhita, and the Digital Personal Data Protection Act have been fundamentally changing notions of legal regime towards judicial remedies in the context of biometric and electronic data. There were numerous fragmented remedies on issues on data breaches before these enactments due to the narrowness of the IT Act, 2000. The new law system creates an extensive system of liability that considers both the civil and criminal aspects of data misuse, offering victims more potential remedies and restitution systems.

According to the Digital Personal Data Protection Act, 2023, the category of people known as "Data Principals" is entitled to receive compensation related to a very broad range of damages caused by a data breach. Such harms are financial loss and identity theft, fraudulent transactions, reputation damage, and mental and emotional distress. The Act provides an institution of Data Protection Board of India (DPBI) as the main enforcement body that can investigate breaches, issue audit and directly compensate victims. Board is able to give big fines to non-compliant Data Fiduciaries, up to 250 crores in case they do not adopt reasonable security measures. The DPDPA however replaces Section 43A of the IT Act, which gave a better right to compensation on negligence, giving rise to the fear that the new Board-centric model may not set out a clear system of direct

[13] Nair, Prianka. "SURVEILLING DISABILITY, HARMING INTEGRATION." Columbia Law Review, vol. 124, no. 1, 2024, pp. 197–271. JSTOR, https://www-jstor-org.rgnul.remotexs.in/stable/27286856. Accessed 26 Mar. 2026.

individual recovery without a separate civil suit[14]. Section 2(22) of the Bharatiya Nyaya Sanhita, 2023, presents criminal liabilities which consider data as "moveable property" in the form of data. Such categorization makes it possible to prosecute the theft of data in accordance with the general property crime provisions, including Section 303 (Theft), which provides up to three years of incarceration. Another common vehicle of data breach is theft by an employee that is addressed under Section 306 that gives a maximum imprisonment of seven years. Moreover, in cases of subjection to criminal breach of trust, it is provided in Section 316, and in case of habitual dealing with stolen data, heavy punishment is provided in Section 317 that may involve life imprisonment. Such provisions give a strong indication of a change in the policy of the judicial system, which still considers the misuse of the data as a simple breach of the law and views it as a substantial offence punishable by imprisonment.

The Information Technology Act continues to play a significant role in the liability table especially via Section 72A that penalizes the willful dissemination of personal information against the consent of specific persons with up to three years of imprisonment. This is because section 43A of the IT Act continues to address negligent acts of companies in processing sensitive personal data, thus compensation as a result of unsafe downloading or extraction of materials. The principles of equity and law of breach of confidence have also been developed in the courts to act as an indirect safeguard to informational privacy to support the point that informational privacy is an aspect of the right to life in Article 21. The courts have been reported to impose costs of compensation ranging between 50,000 and more than 5 crores; in situations involving simple misuse or financial fraud and sensitive data.

Another important judicial remedy is the so-called evidentiary exclusion of evidence gained by illegal means. Although traditional Indian courts used to grant relevance evidence, regardless of whether it was obtained by unlawful methods, the Puttaswamy case has brought about a stricter interpretation of the constitutional rights. In a recent case of Himachal Pradesh High Court, the court held that telephonic conversations referred to as recorded without consent were against the fundamental right to privacy and thus could not be used as evidence. This confirms that the Article 21 constitutional protections override the procedural flexibility of the statutes such as the Family Court Act. With increased surveillance readily available through technology, the role played by the courts is to strengthen the fact that ease of technology does not lead to a loss of

[14] Kim, Pauline T., and Matthew T. Bodie. "Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy." ABA Journal of Labor & Employment Law, vol. 35, no. 2, 2021, pp. 289–316. JSTOR, https://www-jstor-org.rgnul.remotexs.in/stable/27186005. Accessed 26 Mar. 2026.

constitutional rights[15]. The award of damages as provided by the Data Protection Board will depend on the sensitivity of the data, the level of exposure, the nature of the damage and negligence of the company. In biometric data, where once stolen the information cannot be revised, the damage is permanently fixed, and therefore a greater level of care and possibly bigger awards of compensation are required. DPDPA also gives the rights to the erasure of data and also to correction where an individual requests that his or her data be erased after the reason why it was collected is fulfilled. Such companies that do not inform individuals about a breach or conceal it are now liable to punishable violations under DPDPA.

Moreover, the protocols of the chain of custody and hash verification provided in the BSA and BNSS can be seen as a proactive solution since it guarantees that only valid information is employed in trials. In case the integrity of a digital record is affected because of its unproper handling, it may be omitted in the evidence, which can virtually deprive it of its influence on the judicial decision. This procedural solution is crucial in ensuring justice in the digital age of trial manipulation. The changing role of the courts is to monitor this liability matrix, where the Data Protection Board should take the strongest measures against defaulters and personalities should be compensated properly, both in terms of financial and emotional damages.

During the initial 24 hours of data leak, one is encouraged to save evidence and report the case to the DPB and cybercrime agencies. The judicial system has come to realize that data is not merely an artifact of privacy that it owns. With the BSA, BNS, and DPDPA combined, there is an effective combination of a structure where data theft, data misuse, or even negligent leaks can result in regulatory fines as well as imprisonment. The inclusion of all these remedies in one is the expression of the power of judicial intent of protecting individual dignity and personal freedom of choice in a world where information is becoming the new oil, but also the new target of criminal activity[16].

5.3.1 Evolving Judicial Role and Constitutional Safeguards

Bharatiya Sakshya Adhiniyam, 2023, will be applied as a constitutional framework that has been transformed radically, as a result of the understanding of the right to privacy as a fundamental right. The case that changed everything the landmark case of K.S. Puttaswamy v. Union of India (2017) decided that informational privacy the right to manage own information is an inherent right of the right to life and personal liberty in Article 21. This has huge repercussions on

---

[15] Marcus, Daniel J. "THE DATA BREACH DILEMMA: PROACTIVE SOLUTIONS FOR PROTECTING CONSUMERS' PERSONAL INFORMATION." *Duke Law Journal*, vol. 68, no. 3, 2018, pp. 555–93. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/48563659. Accessed 26 Mar. 2026.

[16] Thomas, Linden, et al. "Regulatory Framework." *The Clinical Legal Education Handbook*, edited by Linden Thomas and Nick Johnson, University of London Press, 2020, pp. 57–239. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/j.ctvk8w167.7. Accessed 26 Mar. 2026.

the evidentiary regime since any government incursion on digital or biometric information should now be explained through the three-prong test of legality, necessity, and proportionality. The judiciary has also changed to be a critical evaluator of the facts but turned out to be an active protector of these constitutional and civil rights. The proportionality test entails the fact that an invasion of privacy cannot be performed without a valid state object and that the actions that are carried out must be the least restrictive ways to attain such a purpose.

Constituting the BSA, that is to say the tool of the search and seizure of electronic gadgets or the compulsory gathering of biometric information should be questioned as to whether they were needed in a democratic society. Researchers have identified that the existing provisions of search in most cases lack sufficient procedure protection, which can be easily challenged constitutionally in the post-Puttaswamy era. To take the example, the compilation of nation-wide biometric records to welfare delivery should be severely restricted to that end to avoid "function creep" to mass surveillance. The courts should make sure that the technological convenience does not surpass the constitutional vigilance because the infrastructures that are meant to serve the common good can be easily transformed into the surveillance infrastructure.

The judicial role in digital age is also dominated by the right to the fair trial as guarantied by the Article 21. Right to a fair trial requires that the evidence used against a person should be credible and an accused as well be provided a chance to develop an effective defense. Supreme Court in P. Gopalkrishnan Vs. State of Kerala[17] believed that in case prosecution is based on electronic record, the accused should be provided with a cloned copy so that they can contest on its integrity. The reliance of the BSA on expert certification and the possibility of its certificates being admitted without facing adversarial challenges under Section 330 of the BNSS is a threat to these rights, however, especially to low-income litigants who are not able to afford their own forensic experts.

The courts should not be left behind in ensuring that there is a balance between the digital facts and the legal provisions, whereby the court does not convict an innocent person because forensic examination was not carried out in relation to the digital evidence[18]. Self-incriminating evidence created by biometrics and AI is also a new challenge to the protection of this right under Article 20(3). Selvi

[17] AIRONLINE 2019 SC 1599

[18] Anderson, Janna, and Lee Rainie. The Future of Digital Spaces and Their Role in Democracy: Many Experts Say Public Online Spaces Will Significantly Improve by 2035 If Reformers, Big Technology Firms, Governments and Activists Tackle the Problems Created by Misinformation, Disiriformation and Toxic Discourse. Others Expect Continuing Troubles as Digital Tools Andforums Are Used to Exploit People's Frailties, Stoke Their Rage and Drive Them Apart. Pew Research Center, 2021. JSTOR, https://www-jstor-org.rgnul.remotexs.in/stable/resrep57316. Accessed 26 Mar. 2026.

judgment developed that mental privacy is secured, yet the legislation has not been clear on the behavioral characteristics gathered under the Criminal Procedure (Identification) Act, 2022. Since AI is implemented to assess the trends in behavior or gait, the courts will have to decide whether this qualifies as pushing a person to become a witness against himself. The changing jurisprudence implies that privacy should be complemented by a wider concept of bodily autonomy and individual dignity that makes sure that the state cannot use biometric data to circumvent constitutional rights. Moreover, the exclusionary rule is also spreading in India as the solution to the breach of the constitution. On the contrary to the old method of admitting any evidence, the courts are now refusing to admit evidences that have been obtained by the help of a severe breach of privacy.

In His decision on the case of recorded telephonic conversations, the Himachal Pradesh High Court pointed out that the constitutional rights must not be violated even in cases of matrimony disputes. This premeditated exclusionary model fortifies constitutional rule and the protection of human rights without completely undermining the running of criminal justice. The judiciary has now to make use of its discretion to suppress evidence that is unacceptable under the constitution and prevent illegal conduct of the state and enforce the rule of law[19].

The conflicting nature of the Digital Personal Data Protection Act and the rights to information (RTI) Act also need to be solved in the court. The changes made to the RTI act in Section 8(1)(j) will establish a blanket ban on the disclosure of personal information, which may mean that the various functionaries elected by the people can avoid being held to account. This was criticized by petitioners as an infringement of the right to know as stipulated in Article 19 (1) (a) and the right to information as stated in Article 21. This case has been passed on to a bigger bench by the Supreme Court, which reflects the imperative of the court in ensuring that the right to privacy is weighed against the transparency in a democratic society.

The courts also play a crucial role in checking the Data Protection Board and making sure that the powers of this body are exercised in an ethical and non-opaque manner. The DPDPA carries the option of appealing to the Appellate Tribunal (TDSAT) and then the High Courts and the Supreme Court, which guarantees a level of judicial control. In the transition to an AI-powered judicial system in India, the courts should continue being human-centric, meaning that they need their algorithms to be used to complement but not to replace human judgment. The success of the BSA, as well as the digital legal regime in general, will be ultimately based on judicial interpretation, technological infrastructure

[19] MacCarthy, Mark. "Privacy Rules for Digital Industries." *Regulating Digital Industries: How Public Oversight Can Encourage Competition, Protect Privacy, and Ensure Free Speech*, Brookings Institution Press, 2023, pp. 171–230. *JSTOR*, https://www-jstor-org.rgnul.remotexs.in/stable/10.7864/jj.10354693.7. Accessed 26 Mar. 2026.

and continuous legal training. The judiciary needs to confront such complications in order to see the "Sakshaya Adhiniyam" as a solid frame of justice in the digital age, which will hold the state to account and align the legal principles with the technological developments[20].

Conclusion

The Bharatiya Sakshya Adhiniyam, 2023, is a landmark development in the history of Indian jurisprudence, marking a final departure of the paper-based reasoning of the nineteenth century, and the adoption of the digitalities of the twenty-first century. The BSA by redefining the status of electronic and digital records as primary evidence applies the idea of locational data, server logs and electronic statements as primary medium of social and legal interaction to the status of document and oral evidence. Nevertheless, this change is not simply an administrative re-adjustment; it necessitates a fundamental reorientation of the evidentiary norms, judge review, and constitutional protection. Section 63 certification requirement stands out as the most important figure of admission to digital and biometric evidence admissibility. Although this is set to guarantee authenticity and integrity in the face of tampering and manipulation, its two levels of expert authentication is highly challenging to implement in practice, both in terms of practical delays in the process, and in terms of dismissing valid evidence because forensic infrastructure has failed. The role of the judiciary is currently changing to serve as an apolitical and constitutional adjudicator, by making sure that the probative value of the biometric templates and algorithmic outputs is proved beyond reasonable doubt, without interference with the fair trial rights of the accused.

The liability scheme that the BNS and the DPDPA have put in place offer an elaborate, albeit intricate, approach to remedies against biometric data theft. The law acknowledges the exclusivity and irreversible nature of biometric markers by considering the data a property and permitting individuals to recover significant amounts of money as a result of emotional and reputational injuries. However, the effectiveness of these solutions lies in the openness of the Data Protection Board and the desire of the courts to use a balanced exclusionary rule when using evidence acquired as a result of breaching privacy.

The Bharatyaya Sakshya Adhiniyam is however a good place to build a future-ready judicial system, however, it will only work in the long term when the legal ecosystem is invested in technology and trained. Puttaswamy judgment is the constitutional anchor to this regime and the search toward the truth in the digital age can never disrespect the basic rights to privacy, dignity, and due process. With

[20] DENARDIS, LAURA. "Cyber-Physical Security." *The Internet in Everything: Freedom and Security in a World with No Off Switch*, Yale University Press, 2020, pp. 93–131. *JSTOR*, https://doi-org.rgnul.remotexs.in/10.2307/j.ctvt1sgc0.7. Accessed 26 Mar. 2026.

biometrics and AI on the verge of revolutionizing the world, the Indian judiciary must be on the lookout to ensure that the convenience provided by technology does not erode the constitutional rights and justice is audible, just, and available to every citizen.

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618