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

Criminal Liability for Biometric Data Theft Under the Bharatiya Nyaya Sanhita, 2023

Author
Manish Tundelkar
Dr Vaishnavi Yashasvi

Criminal Liability for Biometric Data Theft Under the Bharatiya Nyaya Sanhita, 2023

Manish Tundelkar
LLM (Criminal Law)
Amity University

Dr Vaishnavi Yashasvi
Assistant Professor
Amity University

Introduction

The implementation of the Bharatiya Nyaya Sanhita (BNS), 2023, is a paradigm shift in the criminal justice system of India with the conclusion of the Indian Penal Code (IPC) of 1860 and the beginning of a legal system allegedly tailored to the requirements of a sovereign, digital-first republic. The key aspect of this shift is the appearance of the biometric data as one of the most important boundaries of personal freedom, privacy, and property. The biometric data, which is a collection of unique biological identifiers in the form of fingerprints, iris patterns, facial geometries, and voiceprints, is fundamentally distinct to the traditional data due to their immutable and non-replenish character. Biometric data cannot be modified, unlike passwords or cryptographic tokens, which can be reset in case of compromise, a theft of biological data poses a security threat to the victim forever, since the biological trait cannot be changed. Bharatiya Nyaya Sanhita which will come into force on July 1, 2024, tries to justify legal procedures and to update the definition of crime to better respond to these 21st-century threats. Yet, the BNS does not provide a clear, separate statutory offense directly defined as biometric data theft, which means that the legal system has no alternative but to apply a complex array of the existing laws in the prosecution of theft, cheating, identity fraud, and criminal breach of trust.[1]

The Indian Penal Code used to be criticized as offender-oriented and too colonialist-minded, including the oppression of opposition by sedition and the safeguarding of state interests against the rights of a person. The BNS aims at inverting this emphasis by making victims and citizens center of the

[1] Dr. Rahul Kailas Bharati, "Identity Theft and Impersonation in Cyberspace (Sections 66C and 66D of the IT Act, 2000)" (2025).

legislative regime. This re-imagination is especially pertinent to the securing of the biometric information that occupies the border of the body and the property. The historic ruling of the Supreme Court of India in Justice K.S. Puttaswamy v. The right to privacy was entrenched by Union of India (2017)[2] as a fundamental right in Article 21 and that any interference of sensitive data by a state or a private individual or organization must be just, fair, and reasonable. This constitutional prism is then to be applied to the BNS whereby the criminal law must offer a deterrent that is formidable enough to safeguard the informational autonomy of the individual. This will demand a critical evaluation of the extent to which the traditional penal principles which were initially formulated in a physical, corporeal world are being stretched to accommodate the intangible and yet most powerful theft of digital biometric templates.

The legislative framework of the BNS 2023 indicates an updated concept of property and documents. The extension of the definition of document to cover electronic and digital records and by making it clear that data can be legally defined as movable property, the BNS offers a point for prosecution of crimes committed through cyber-enabling documents. Section 2(8) of the BNS recognizes a document as anything written or stated on any material by use of letters, figures or marks specifically including electronic and digital records. The Bharatiya Sakshya Adhiniyam (BSA), 2023, which supersedes the Indian Evidence Act, makes electronic records primary evidence to facilitate easier access to the evidentiary hurdle that was once inherent to digital forensics. By retrieving a mathematical hash of an iris scan or a voiceprint off a secure server, the criminal can no longer be said to be fiddling with bits; the criminal is now violating the property and the trust involved in the digital fiduciary relationship.[3]

Though such legislative steps have been made, lack of a specific provision on biometric theft is still under a heated scholarly and judicial investigation. The existing framework is based on some legal duality where the general law of the BNS is present and the special law of the Information Technology (IT) Act, 2000. Such duality is frequently the cause of the so-called prosecutorial forum shopping where the prosecution forces can opt between the softer provisions of the IT Act that can be bailed out (e.g., Section 66C of dealing with stolen property) and the stricter provisions of the BNS (e.g.,

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

[3] Priya Bairagi & Asha Rawat, "Between Innovation and Illegality: A Critical Study of Artificial Intelligence Crimes and the Limits of India's Existing Penal and Regulatory Regime" *Ianna Journal of Interdisciplinary Studies*, Vol. 7, No. 2 (2025), pp. 339–350.

Section 317 of dealing with stolen property). Another idea of the BNS is the notion of an Organized Crime that is covered under Section 111 of the act which particularly involves cybercrime perpetrated at the request of a criminal syndicate, and may result in a sentence up to life imprisonment or death under extreme circumstances. This is an indicator that a legislative effort has been made to address mass biometric data breaches, which are in most cases organized by highly organized syndicates, with maximum amounts of seriousness.[4] However, the technological environment is changing at a greater rate than the statute. The emergence of generative artificial intelligence and deepfake technology has opened new opportunities of biometric misuse, which no longer follows traditional definitions of fraud by humans in nature. Biometric "spoofing" and "synthetic media" enable the criminal to mimic the person with a disturbing degree of success, and this hampers the traditionality of mens rea (guilty intent) and attribution. Assuming that an AI system autonomously collects biometric data or creates a fake identity without any direct human involvement in each stage, the historical criminal law provision of a guilty mind is challenging to meet. This generates a border zone of liability that the BNS in its anthropocentric concerns has not completely closed. Moreover, the role of such intermediaries as the platforms and data processors that host such information is another convoluted topic because they have to balance the safe harbor protections of the IT Act and the growing due diligence obligations of the BNS as well as the Digital Personal Data Protection Act (DPDPA), 2023.[5]

The report focuses on the substantive criminal law provisions that address the issue of biometric data theft pursuant to the Bharatiya Nyaya Sanhita, 2023. It examines the property-data nexus, the mechanics of identity fraud and forgery, the doctrinal challenges of mens rea in the era of automation and changes in corporate and mediator responsibility standards. Combining the stipulations of the BNS and applicable case law along with technology trends, the analysis exposes the ambiguity and gaps in the doctrines that need to be resolved to achieve a safe biometric economy in India. With the adoption of biometric authentication as the new form of engagement in the digital life (banking, welfare delivery, etc.), the application of criminal law

[4] Arshita Sharma, “Deepfakes, Digital Manipulation and the Future of Evidentiary Integrity” in *From Mens Rea to Machine Rea: Reimagining Criminal Culpability in the Digital Age* (2026), p. 214.

[5] M. N. Jyothi, *An Evaluation of the Legal Framework of Electronic Banking with Special Reference to Data Protection and Cyber Security in India* (Ph.D. Diss., Alliance University, India, 2025).

is not only a question of penitentiary policy but also a vital condition of individual dignity and the security of the state.[6]

The Property-Data Nexus and Substantive Offences Under BNS

The building block to the problem of prosecuting biometric data theft is the conceptualization of the data as property. Previously, the Indian Penal Code limited the meaning of theft to movable property that would be taken to mean tangible, corporeal things. A broader digital-native interpretation is adopted in the Bharatiya Nyaya Sanhita, 2023. Section 2(21) of the BNS provides the definition of movable property by making it to cover all property of all description, except land and property attached to the earth. More importantly, the implementation of this definition to the digital space is based on the fact that in Section 2(22) it is stated that the data falls under Section 2(22) that defines data as a movable property. This rehousing is a turning point in Indian criminal law because it gives the opportunity to apply directly the property offenses of the past to the theft of abstract biometric templates.[7]

In accordance with Section 303 of the BNS, which substitutes the old-fashioned definition of theft, an unauthorized removal of the data is the punishment of up to three years in prison. Within the framework of biometrics, it implies that when a person has illegally copied, downloaded, or extracted biometric files out of a computer system or a cloud server, they may be convicted of stealing them. The intention of the legislation to act as a greater deterrent can be seen in the Section 303(2) which gives the ability to increase the sentence of repeat offenders to five years. This is a big change as compared to the Section 43 and 66 of the IT Act, the top penalty of unauthorized data extraction is usually three years and in most cases is bailable. The state by categorizing biometric theft as a BNS gives law enforcement greater means of detention and prosecution as the repercussions of breaching the immutable identity of an individual are dire. An extra protection is offered by the section 316 of the BNS in the form of the Criminal Breach of Trust that concentrates on the contravention of the fiduciary deal among the subject of data and the data processor. This crime involves entitlement to property, and thereafter, a misappropriation or conversion of the property through dishonesty. The biometric ecosystem is often associated with the case where individuals give their extremely

---

[6] Legha Mamta Ranjitsingh, *The Evolution of Cyber Law: A Critical Analysis of Jurisprudence, Regulation, and Digital Rights* (Crown Publishing, 2025).

[7] Marlin Lowell Fransman, *Property Rights in Personal Information: A South African Perspective* (Diss., University of the Western Cape, 2024).

sensitive fingerprints or eye scans to so-called Data Fiduciaries, including a bank or the government, to verify them. By using this access improperly to sell biometric templates in the darknet, an employee of such an organization has breached the trust of the criminal. The BNS draws a line between general breach of trust, which attracts up to five years, and breach of trust by a clerk or servant (Section 316(4)) which attracts a sentence that is seven years in duration. This is an important distinction since internal attacks and vendor carelessness are some of the most prevalent agents of biometric information attacks.[8]

Moreover, the BNS Section 317 concerns the issue of the receiving of stolen property, and in this case, the biometric information obtained as a result of theft or a violation of trust. Section 317(2) punishes the receipt or retention of such data dishonestly and Section 317(5) is directed toward the persons who aided in the concealment or disposal of such data. The most powerful section in this category is the 317(4) that focuses on habitual dealing of stolen property. This is especially true in cybercrime market where the biometric databases are not only traded or sold but also bought and re-bought several times. Repeat offending may result in a ten-year sentence or even life imprisonment, which puts the BNS at the center of an arsenal against the business side of cybercrime syndicates. This part will enable the state to pursue the so-called middlemen and the so-called data brokers who help monetize stolen identities, although they were not directly engaged in the process of extraction.[9]

Yet, the property law concerns biometrics are statistically intricate. Data, unlike a physical object, is not a rivalrous commodity, that is, the victim still has their biometrics (carried around) when the offender has copied it. The BNS gets this resolved by concentrating on the "unauthorized extraction" and the malafide intent to suffer an unjustified gain or loss. The law considers the digital biometric template as the property itself and, therefore, it regulates the security and economic damages related to the copying and possible abuse of a unique biological signature of a person. This change is necessary in a legal system that cannot ensure the citizens their protection not only in the physical deprivation but also in the digital deprivation of their very identity, called dispossession.

---

[8] Mohamed Chawki & Mohamed S. Abdel Wahab, “Identity Theft in Cyberspace: Issues and Solutions” *Lex Electronica*, Vol. 11 (2006), p. 1.

[9] WenJie Wang, Yufei Yuan & Norman P. Archer, “A Theoretical Framework for Combating Identity Theft” (2004).

The BSA, 2023, has been integrated with the BNS, which further explains the property-data nexus since it modernizes the rules of evidence. In Section 63 of the BSA, any electronic records can be used as evidence without additional evidence provided that they meet some criteria, including the requirement that they be created through the use of a computer in ordinary operation. This limits the roadblocks that existed in the process of prosecuting data-related crimes in the past. The BSA also gives the opportunity of submitting certificates to verify electronic records such as hash values and source verification that are very significant in establishing the integrity of stolen biometric data in a court of law. [10]

Besides theft and breach of trust, the BNS creates Organized Crime under Section 111 that gives a broad definition of crimes done by a syndicate through violence, coercion, or any other unlawful methods to gain financial gain. The section 111 particularly incorporates the term "cyber-crime" as a key component of organized crime. It is a provision that carries high stakes, as in case of any theft of biometric data that leads to the death of any individual (as in the case of the breach of essential medical records or security systems), the perpetrator may be sentenced to death or a life imprisonment. Although no death is committed, simply trying or engaging in organized cybercrime has a minimum sentence of five years, which could be life.

Switching to the BNS also implies a significant re-calibration of the punishments related to such offenses as mischief or trespass when they take place in the cyberspace. The most biometric thefts are preceded by digital trespassing or unauthorized access to a computer system. Although the BNS still preserves the provisions regarding physical trespass, it also covers the damage to the digital asset under the following Sections 324 and 325 which revise the penalties of mischief and damage of property. The BNS has augmented the amount of incarceration on 45 crimes, such as criminal violation of trust and cheating, and matches the penalties with the seriousness of financial and cyber scams today.[11]

---

[10] Krisztina Huszti-Orbán & Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* (Human Rights Center, University of Minnesota, Minneapolis, 2020).

[11] Mokopane Charles Marakalala & Mpho Mark Matlala, "Border Management Identification: The Biometric Technology to Detect Criminals and Terrorists Often Travel Using Falsified Identity Documents" *OIDA International Journal of Sustainable Development*, Vol. 17, No. 12 (2024), pp. 57–70.

Deception, Identity Fraud, and the Forgery of Biometric Records

Although property crimes are prosecuted on the acquisition of biometric data, the misuse of such data; once acquired, to trick systems or people is covered by the sophisticated crimes of Cheating and Forgery under the Bharatiya Nyaya Sanhita, 2023. Most biometric identity fraud consists of "spoofing" or "personation" in which an offender steals or falsely creates biometric characteristics to overcome security systems, get unauthorized access to financial accounts, or receive government benefits. The BNS modernizes these crimes and offers a more specific model to the digital era than the archaic Indian Penal Code.[12]

According to Section 318 of the BNS, Cheating is understood as the unscrupulous or unscrupulous inducement of a person to convey property or to perform an act that he/she would not have had otherwise performed. In the biometric case, this can happen when a criminal employs a deepfake or a copied biometric sample to deceive some system -or the human operator of such system- to grant authorization to a transaction. According to the BNS, there are levels of severity of cheating. Section 318(4), a replacement of the previous Section 420 IPC directly deals with cheating that is used to give the property or change a valuable security, and is punishable by a maximum of seven years of incarceration. It is among the most frequently applied charges on the financial and white-collar crimes, and its use of biometric fraud is a logical application of its legislative purpose.

A more specific and more applicable clause is the Section 319, "Cheating by Personation. It is a crime that is committed by an individual who lies or impersonates another individual to defraud the other individual or individual who conceals the identity of another individual to impersonate another individual. The final personation tool is biometric data. When an offender tricks a biometric scanner at a bank or a high-security facility with an impression of the victim by his or her distinctive biological attributes, made with a high-resolution 3D-printed fingerprint or a highly advanced facial reconstruction technique, then he or she is impersonating the victim. This is a non-bailable cognizable offense subject to a three-year sentence as provided in section 319(2). The legislation in this case is the violation of the informational autonomy of the victim and the security of the system of

[12] Simon Baechler, "Document Fraud: Will Your Identity Be Secure in the Twenty-First Century?" *European Journal on Criminal Policy and Research*, Vol. 26, No. 3 (2020), pp. 379–398.

authentications in general.[13] The BNS also brings a significant revision to the law on the area of Forgery to include the false electronic records. The provisions of section 335 through section 340 offer the structure of prosecution of forging and using forged biometric records. Section 336 establishes the existence of forgery as creating a counterfeit document or electronic record with a view to inflict damage or injury, or aid any claim or title. This directly applies to biometric theft since the manipulation of a biometric database or the formation of a so-called ghost identity, when a synthetic biometric is associated with a fake name, is the formation of a false electronic record. Section 338 is specifically important because it specifically refers to the forgery of identity documents which are government issued such as Aadhaar Cards. Since Aadhaar is the backbone of the Indian digital public infrastructure, the fraud of its digital records or the fake manipulation of its biometric authentication APIs are regarded with the increased severity.[14]

The combination of deepfakes and identity theft poses a particular dilemma to the BNS. Deepfakes are built on the idea of artificial intelligence by creating credible audio-visual effects, or essentially cloning the voice or facial geometries of a person, all of which are biometric identifiers. Although the BNS does not call this a deepfake, one can apply the criminal law of prosecuting the authors of the synthetic media in case of the intent to cheat out the victim under the provisions of Sections 319 (personation) and 336 (forgery). Nonetheless, this case is complicated in the legal environment due to the decision taken by the Supreme Court in Sharat Babu Digumarti v. Government of NCT of Delhi[15] which believed that when the offense is of electronic media, the special law (lex specialis) of IT Act shall prevail over the general law (lex generalis) of IPC/BNS. It implies that although a deepfake could be defined as any instance of forgery that falls under Section 336 of the BNS, the courts may nonetheless have to prosecute a person under Section 66D or 67 of the IT Act, assuming that the main means of transmission was digital.[16]

---

[13] Kavita Kanwar & Nikhil Kumar Goyal, "Biometric Intelligence in the War Against Cybercrime and Identity Fraud" in *Exploring the Intersection of Forensics and Biometrics* (IGI Global Scientific Publishing, 2026), pp. 1–30.

[14] Justin Picard, Claus Vielhauer & Niels Thorwirth, "Towards Fraud-Proof ID Documents Using Multiple Data Hiding Technologies and Biometrics" in *Security, Steganography, and Watermarking of Multimedia Contents VI*, Vol. 5306 (SPIE, 2004).

[15] Sharat Babu Digumarti v. Government of NCT of Delhi, (2017) 8 SCC 761.

[16] Russell G. Smith, "Identity Theft and Fraud" in *Handbook of Internet Crime* (Willan, 2013), pp. 273–301.

It is possible that this legal duality may cause a large disparity in sentences and bail. It is an example as most of the crimes that can be committed in the IT Act are bailable and can have a maximum penalty of three years, which is significantly less than the penalty that could be imposed by the BNS on fraud or organized crime. The prosecutors usually use the BNS due to the deterrent effect, and this has resulted to a risk of the occurrence of the so-called Double Jeopardy where a particular act is tried in a particular statute as well as under the other statute. The BNS tries to answer this by providing "electronic means" as part of the definition of organized crime (Section 111) and as a traitorous activity (Section 152), which may have the effect of creating a harmonious construction to enable the BNS to override the IT Act where there is an involved high-stakes national security or high-level fraud.

The use of Cheating and Forgery is also applied in the misuse of biometrics at the workplace and in a business deal. Section 306 and Section 318(3) discuss cheating in which the offender is under a legal obligation or law to guard the interest of the cheated person in a legal contract. This especially applies to data processors and third-party vendors that process biometric databases with a contract. In case a vendor sells or has an unauthorized commercial use of a client biometric information, they may be charged under these sections which are subject to a higher punishment. This guarantees that the criminal penalties of the DPDPA are supported with criminal penalties to the breach of the so-called f fiduciary duty of data protection.[17]

The BNS also provides enhanced punishment to repeat offenders and against offenses committed against women and children, which is victim-oriented. In case biometric identity theft causes a crime committed against a woman, including stalking or voyeurism (now legal in Sections 77 and 78 of the BNS), a court may impose more severe punishments. Likewise, the employment of deepfakes to formulate non-consenting intimate pictures is a severe breach of dignity that intersects the augmented obscenity and sexual offence clauses of the BNS. Taking the biometric fraud as a part of the greater web of the penal code, the BNS guarantees that the biological identity of the citizen will be secured no less vigorously than the physical one.

---

[17] Anil Kumar Pakina *et al.*, "AI-Generated Synthetic Identities in Fin Tech: Detecting Deep Fakes KYC Fraud Using Behavioral Biometrics" *IOSR Journal of Computer Engineering*, Vol. 25, No. 3 (2023), pp. 26–37.

Doctrinal Ambiguities: Mens Rea and Attribution in Automated Crimes

The greatest doctrinal difficulty in the practical application of the Bharatiya Nyaya Sanhita, 2023, to the biometric data theft is the necessity of mens rea -the guilty mind. The anthropocentric concept of traditional criminal law and, through it, the BNS is founded on the fact that all crimes are perpetrated by a human mind, one that is able to create the intention, knowledge, or recklessness. Nonetheless, automated systems, self-learning algorithms, and autonomous AI agents, which exist not within human consciousness or moral agency, are becoming the dominant biometric threat actors of the modern era. This poses a liability gap in the cases where an autonomous system causes a harm or makes a theft that a human agent could not have foreseen or intended in particular.[18]

Section 2 of the BNS spells out act, omission, and person in human related terms. Although corporations are considered a person (as we will discuss in the following section), autonomous software systems are not referred to as a person. This results in the Attribution Problem that in case a biometric harvesting bot algorithmically chooses to scrape information on a third-party server in a manner that its author did not anticipate, whose psychological state should apply to the conviction of stealing under Section 303?. Conventional legal frameworks find it difficult to pin mens rea in such cases since the AI does not have the ability to make a moral decision but its actions can result in severe damages to the identity and dignity of a person in the real-world.[19]

This attribution is further complicated by the so-called Black Box problem. Complex AI decision-making can be non-transparent and thus courts struggle to provide a clear chain of causation between a human decision and an automated criminal action. The evidentiary value of an automated system in a criminal prosecution is diminished when the result of the automated system cannot be explained or traced. This is a breach of accountability where the developer can argue that the abuse was an unanticipated occurrence of the algorithm and the user can argue that he or she was not in charge of the autonomous activities of the system. Although it has updated

---

[18] Akanksha Priya, "Criminal Accountability for AI: Mens Rea, Actus Reus, and the Challenges of Autonomous Systems" *LawFoyer International Journal of Doctrinal Legal Research*, Vol. 3 (2025), p. 273.

[19] Muhammad Ahsan Iqbal Hashmi *et al.*, "Criminal Liability in the Age of Autonomous Systems: Rethinking Mens Rea and Actus Reus" *The Critical Review of Social Sciences Studies*, Vol. 3, No. 3 (2025), pp. 290–303.

most of the definitions, the BNS nevertheless continues to be based on the actus non facit reum nisi mens sit rea maxim, which might not be adequate to deal with the so-called systemic or automated criminal conduct.[20]

Some models that have been discussed by legal scholars to fill this gap are the "Tool Model," in which the AI is a complex tool of its human operator, and the "Agent Model" in which the AI is regarded as an agent of its creator. The BNS is now inclined to the Tool Model with human supervision and liability of designers. According to this paradigm, the courts will be more inclined to blame human actors, developers, deployers, or users, and their negligence or recklessness in not taking the necessary precaution. To take the example of the BNS, Section 106 of the section dealing with death by negligence can be modified in terms of jurisprudence to impose liability on a corporation due to AI design negligence resulting in a fatal security breach. But the standard of negligence might be inappropriately low in such a high-stakes area of biometric security as Strict Liability could be more suitable.

The other point of concern is that of "Anonymous Digital Offenders" which is ambiguous too. Biometric theft has a way of going across international borders, and in such cases, it is the servers in one jurisdiction but victims in another jurisdiction. Actors, who conceal their actions behind decentralized protocols, may launch automated AI frauds and it is almost impossible to trace a particular person that can be prosecuted on the grounds of the BNS.[21] Although Section 1(5) of the BNS gives extraterritorial jurisdiction against any person who targets a computer resource located in India, its practical effect can only be facilitated through the use of the slow and inefficient Mutual Legal Assistance Treaties (MLATs). Such anonymity of jurisdiction combined with the swiftness of automated fraud provides a safe haven to cybercriminals that the traditional procedural framework of the BNS (even with the electronic upgrades of the BNSS) can hardly tap into.

Moreover, the BNS has to struggle with the Body vs. Property question of legal philosophy. In the case with human body being used as a biometric identifier, the distinction between body and data is destroyed. When BNS

---

[20] Mahmood Ahmed Shaikh *et al.*, "Fixing Criminal Liability as per Elements of a Crime: A Review in Modern Era of AI and Robotics" *Russian Law Journal*, Vol. 11, No. 4 (2023), pp. 1183–1207.

[21] Marta Bo, "Autonomous Weapons and the Responsibility Gap in Light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute" *Journal of International Criminal Justice*, Vol. 19, No. 2 (2021), pp. 275–299.

views biometrics as property, it runs the risk of commodifying the human person, but when it views biometrics as body, it might fail to have the instruments with which to manage the digital replica and sale of that information. According to recent scholarship, biometric identifiers must be considered as hybrid entities (measures of privacy, dignity, and property) and that more dynamic explanation of data protection is needed than the one currently being presented within the frames of the BNS or the DPDPA. This involves the need to consider biometric theft as a form of dignity harm and not an economic loss.[22]

In order to eliminate these ambiguities, an increasing movement towards AI-specific legislation or the establishment of Accountability by Design emerges. This involves the introduction of the liability protections into the AI lifecycle, including explainability requirements, algorithmic audits, bias detection, etc., at the heart of it. The human-centric design and accountability mechanisms highlighted in international best practices, like the OECD AI Principles, make a human always in the loop. Throughout the BNS, this might be made operational as the definition of what mischief or cheating is to be extended to explicitly include actions done by autonomous systems at the general supervision of a human being. In the absence of this kind of reform, the black box of AI can be transformed into a black hole of criminal responsibility.[23]

Lastly, although the application of digital records under the Bharatiya Sakshya Adhiniyam (BSA), 2023, makes its application more adaptable, the evidentiary criteria do not currently offer special provisions in relation to the so-called AI-generated evidence or deepfake verification. When defense make the issue of the biometric evidence being a deepfake itself in a criminal trial, then the court would have a hard time proving whether that digital material is real or fake. A lack of a more obvious forensic certification procedure with synthetic media is also a major omission of the Indian law. The more the criminals learn to leverage AI to create a biometric fake truth, the more the law will have to mirror this to avoid wrongly convicting the innocent, and acquitting the guilty.

---

[22] Ahmed Ragab Ali Abdelghany, "The Accountability Gap: Navigating Machine Crime and Legal Liability in the Age of Autonomous AI."

[23] Shefali Mahendru & Mandeep Kaur Mann, "Autonomous Systems and Criminal Accountability: Beyond Human Actor" in *From Mens Rea to Machine Rea: Reimagining Criminal Culpability in the Digital Age* (2026), p. 176.

Systemic Accountability: Corporate and Intermediary Liability

The last aspect of the criminal framework that the biometric data theft within the BNS is the responsibility of the corporations and intermediaries. When it comes to the contemporary digital economy, where people are not the ones in charge of their biometric information, it is amassed, stored, and processed by the big players: Data Fiduciaries, which can be financial institutions and telecommunication giants, but also government platforms. Section 2(26) of the Bharatiya Nyaya Sanhita, 2023, deals with this by defining a person to be any company, association or body of persons, incorporated or not. It is this definition that grounds the very notion of Corporate Criminal Liability permitting corporations to be responsible to the actions of their employees or agents in the occurrence they are committed in the scope of their employment and to the advantage of the corporation.[24]

According to the Indian laws of jurisprudence, the so-called Doctrine of Identification states that the mental personality of the driving mind and will of a firm, its directors and senior management is ascribed to the firm. In case a corporation has not taken the necessary measure of "Reasonable Security Safeguards" (as stipulated in the DPDP Rules 2025, Rule 6) and the breach leads to mass biometric data breach, the corporation may face the criminal liability of violation of the Section 316 of the BNS, which is the liability of Criminal Breach of Trust. This is a much more severe implication of the DPDPA than the civil fines, which may culminate in criminal fines, seizure of assets, and disqualification of directors. The BNS also admits that there is also a concept of Collective Blindness in which a corporation is liable, despite the fact that no individual had the necessary information or intent to commit the crime, yet the corporation was negligently organized as a whole.[25]

Nonetheless, the liability of the so-called Intermediaries who are platforms and service providers through which they are intermediaries to the data is subject to the issue of a complex interaction between the BNS and Section 79 of the Information Technology Act, 2000. Section 79 grants a "Safe

---

[24] Debashish Goswami & MD Nazrul Islam Khan, “Cybercrime and Contractual Liability: A Systematic Review of Legal Precedents and Risk Mitigation Frameworks” *Journal of Sustainable Development and Policy*, Vol. 1, No. 1 (2025), pp. 10–63125.

[25] Md Nazrul Islam Khan & Md Soyeb Rabbi, “Cybercrime, Legal Accountability, and Contractual Risk: A Systematic Review of Jurisprudence and Protective Frameworks” *American Journal of Advanced Technology and Engineering Solutions*, Vol. 4, No. 1 (2024), pp. 71–100.

Harbour" where the intermediaries are exempted of liability of third-party contents provided they exercise due diligence and have no actual knowledge of the illegal activity. The BNS makes this immunity more difficult because it adds a new practice known as Organized Crime (Section 111), which consists of cybercrime carried out on behalf of a syndicate. Assuming that some sort of intermediary has facilitated, aided, or encouraged a criminal activity, such as by simply allowing a darknet marketplace of stolen biometric data to reside on its computers, might be found to have lost safe harbor privileges under Section 79(3)(a) and may itself be prosecuted as an Abettor or even a member of the criminal enterprise.

The Information Technology (Intermediary Guidelines) Rules, 2021, and BNS introduce the strict requirements on the Notice and Takedown. The intermediaries will be obligated to respond in an expeditious manner to remove the illegitimate material (e.g. leaked biometric databases or deepfake identity materials) in 36 hours of being served with a court order or a message via the government. The lack of compliance does not only result in the loss of safe harbor but it may also cause the so-called consequence action or prosecution by the BNS. It implies that in case of failure to eliminate hazardous synthetic media that poses a danger to the safety of a person or a community, an intermediary may be accused of such offenses as Criminal Intimidation (Section 351) or Statements Conducing to Public Mischief (Section 353).[26]

Moreover, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, that replaces the Code of Criminal Procedure, enlarges the authorities of the state to gather biometric evidence in the course of investigation. In the BNSS section 349, magistrates will have the authority to request any person, including the accused, to submit fingerprints, palm prints, or any other form of biometric samples to assist in a criminal investigation.[27] This has been a great weapon of the law enforcers; however, it also creates self-incrimination issues of Article 20(3) of the Constitution. Although it has always been the case with the courts that giving out biological samples to be identified is not a testimonial compulsion (Selvi v. The increased range of biometrics provided by the BNSS and the Criminal Procedure

[26] Daniel J. Solove, "Identity Theft, Privacy, and the Architecture of Vulnerability" *Hastings Law Journal*, Vol. 54 (2002), p. 1227.

[27] Giancarlo Frosio, "Regulatory Shift in State Intervention: From Intermediary Liability to Responsibility" in *Constitutionalising Social Media* (Hart Publishing, forthcoming, 2021).

(Identification) Act, 2022, in the State of Karnataka), has to be adjusted against the Just, Fair, and Reasonable standards desired by Article 21.
The other punishment that the BNS presents is the Community Service, which is punishment, in cases of minor crimes like minor theft or defamation. Although this does not apply to serious biometric theft, this is one move to restorative justice which may be applied to corporate groups in case of minor regulatory non-compliance. Nevertheless, the major discouragement towards corporations is the excessive monetary fines and exposure of directors to personal liability. Fines according to the BNS have been adjusted on the present economic situation and increased on more than 80 crimes including the maximum 10 lakh penalty on death due to the organized crime. This guarantees that in the case of a corporation, the cost of crime is punitive enough to make it invest in effective and efficient cybersecurity and biometric protection systems.[28]

To sum up, the publication of the Bharatiya Nyaya Sanhita, 2023, can be viewed as one of the steps towards the modernization of the criminal law of biometric data theft in India. The BNS offers the state a full arsenal of digital age by defining identity fraud and forgery, enhancing the definition with the strong legislation of organized cybercrime. Nonetheless, the effectiveness of this framework will be determined by eliminating the ambiguities in doctrinal terms of mens rea in automated crime as well as a harmonious interpretation between the BNS and the IT Act. With biometrics as the new default mode of authentication within the Indian economy, the law needs to develop to be proactive, accountability-by-design, and less human-centric, that is, to safeguard the biological identity of the citizen as a central principle of sovereignty and dignity. The effectiveness of the BNS will be ultimately evaluated based not on the volume of sections of the system, but on whether it provides the so-called speedy, transparent, and victim-centric justice in an even more complicated digital environment.[29]

[28] Elfriede Sixt, "Restoring Trust in European Payment Rails: A Framework for a Shared Liability Reform" (Available at SSRN 5456554, 2025).
[29] Patricia Haley, "The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent" *Sensors*, Vol. 25, No. 10 (2025), p. 3160.

EDITORIAL TEAM

INTERNATIONAL EDITORIAL TEAM

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