Central University of Kashmir Law Review
Online First
eISSN: 2583-6935
pp. xxx-xxx

Privacy and Data Confidentiality Concerns in Neuro-Data Management: An Analysis

Kush Kalra*
Janhavi Kanodiaǂ

Abstract

Exponential data growth demands efficient management, especially near-data processing, which enhances performance but raises privacy and confidentiality concerns at the intersection of law and constitutional rights. This paper examines these issues through India's Criminal Procedure (Identification) Act, 2022, analyzing its impact on privacy and civil liberties. Data confidentiality—protecting sensitive information from unauthorized access—is crucial for trust in digital systems. Robust encryption, access controls, and governance policies can mitigate risks, but evolving laws like the 2022 Act, permitting large-scale biometric data collection, spark fears of abuse and privacy erosion under Article 21 of the Indian Constitution. The paper explores the legal framework, implications of the Act, and potential privacy violations. It highlights ethical data management, urging proactive organizational measures, stakeholder dialogue, and stringent safeguards. Balancing near-data processing benefits with privacy protection requires ongoing research and collaboration to address challenges at the crossroads of data management and legal frameworks.

Keywords: *Data, Privacy, Criminal Identification Act, Neurotechnology, Neurodata Management*

1. Introduction

Data production is unprecedentedly increasing in the digital world due to the use of connected devices, social media, and IoT.[1] Neuro-data refers to data derived from the human brain and nervous system, collected through technologies such as electroencephalography (EEG), functional magnetic resonance imaging (FMRI), brain-

* Assistant Professor, NMIMS University, Maharashtra, India
ǂ Student, NMIMS University, Maharashtra, India. email: drkushkalra023@gmail.com

[1]Langley, D., et al. (2020) *The internet of everything: Smart things and their impact on business models*, *Journal of Business Research*. Available at *https://doi.org/10.1016/j.jbusres.2019.12.035*

computer interfaces (BCIs), and other neuroimaging techniques. This category of data captures neural activity, cognitive patterns, and even emotional responses, making it uniquely sensitive due to its direct link to an individual's mental and physiological states. Unlike conventional data, neuro-data can reveal deeply personal information, including thoughts, preferences, and potential medical conditions, raising significant ethical, legal, and privacy concerns. The increasing use of neurotechnology in healthcare, marketing, and AI-driven applications has amplified the need for clear regulatory frameworks to protect individuals from misuse. Given its intimate nature, neuro-data demands stricter safeguards than ordinary personal data, particularly concerning consent, storage, and access. The paper explicitly defines and explores this concept, as its implications for privacy and confidentiality differ substantially from other forms of data. Integrating this explanation into the introduction will provide necessary context for analyzing how Near-Data Processing (hereinafter referred to as NDP) impacts neuro-data management, especially under laws like India's Criminal Procedure (Identification) Act, 2022, which may not adequately address its distinct challenges. In fact, NDP has now become a necessary strategy to deal with these issues by allowing data processing closer to the source for better efficiency and lower latency. Correspondingly, with organizations still implementing NDP, they will also be obligated to face the issues of privacy and confidentiality in a rather complex manner due to handling sensitive information in this manner.

Data growth is not a trend; rather, it's a sea change for organizational operations and decision-making. According to a report, the global datasphere will grow from 33 zettabytes in 2018 to up to 175 zettabytes in 2025.[2] Multiple causes can be attributed to this rapid growth of creation: an increase in connected devices, increasing usage on social media, and business processes moving almost completely to digital means. Data management entails different practices targeted at collecting, storing, organizing, and securing data to make the data available for analysis and subsequent decision-

[2] Hojlo, J. (2024) *Future of industry ecosystems: Shared data and Insights*, *IDC Blog*. *available at:* https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/ (Accessed: 10 September 2024).

making. This is one of the crucial processes of today's data-driven economy, where organizations take data as one of the most critical assets for their competitive advantage. In this respect, NDP plays an important role by allowing processing to be done in real time at the point of, or close to the source of, the data. This will reduce not only the time and bandwidth required for the transfer of data, but faster insight and quicker decision-making will also be assured.

One of the main challenges of privacy in NDP concerns data leakage. Local processing of data can expose them to potential attackers or insiders who would aim at accessing or even stealing the data.[3] This can get particularly risky when data is processed on untrusted or shared infrastructure, like public cloud platforms or edge devices. Other challenges include that, in NDP environments, enforcing policies and regulations for data protection would be extremely difficult. Access controls or encryption would be either ineffective to apply, or just impractical, in a situation involving distributed and dynamic processing of data.[4] Consequently, ensuring this processing complies with applicable laws and regulations, such as GDPR (General Data Protection Regulation) or Health Insurance Portability and Accountability Act (hereinafter referred to as HIPAA), is more difficult. Additionally, the use of NDP does tend to make it more difficult to monitor and audit data processing activities. In cases where data is processed closer to its source, tracking and logging of every activity is sometimes deemed more difficult. Finally, the usage of NDP may finally create new vectors and vulnerabilities not well-understood or fixed with security measures already deployed. For instance, the usage of edge devices or Internet of things (hereinafter referred to as IoT) sensors within NDP environments may bring new attack surfaces that are unwell-protected or unmonitored.

---

[3] Grammatikis, Panagiotis (2018) *Securing the internet of things: Challenges, threats and solutions*, *Research Gate. available at:* https://www.researchgate.net/publication/329183740_Securing_the_Internet_of_Things_Challenges_Threats_and_Solutions (Accessed 10 September 2024).

[4] Burman , A. (2023) *Considering India's encryption policy dilemma* , *Carnegie . available at:* https://carnegieindia.org/research/2023/11/considering-indias-encryption-policy-dilemma?lang=en (Accessed 10 September 2024).

2. Balancing Innovation and Privacy: Navigating Near Data Processing in the Digital Age

While all other approaches involve the transfer of data to a central processing unit for computation, NDP does computations near where data reside. The main idea behind the approach of NDP is to achieve data processing and improvement in performance with reduced transference data and latency periods. This typically includes transferring data from storage over a traditional computing architecture to the separate processing unit, which can introduce significant latency and energy consumption due to the movement of that data.[5] NDP addresses this by placing the processing capability closer to where the data is stored, either in-memory computing or near the memory chips themselves. The core idea of NDP is to perform the computation and analytics, etc., closer to where the data is originating from or is seated. That would mean using all sorts of advanced hardware and software technologies to enable such processing close to the data source on an edge device, a local server, or even integrated into the storage system in a special-purpose processing unit.[6] Traditional models for data processing involve transferring voluminous amounts of data to a central processing unit, which presents several limitations, including high latency and increasing bandwidth consumption with potential bottlenecks. With NDP doing the processing of data closer to its origin, it minimizes the need for extensive transfers of data, hence reducing latency and improving performance. Valuable in more applications where real-

[5] Jamale, R. (2016) *A study on near Data Processing , Research gate . available at:* https://www.researchgate.net/publication/308916429_A_Study_On_Near_Data_Processing (Accessed 10 September 2024).

[6] (2021) *Consultation paper on Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India*, *Telecom regulatory authority of India*. *available at:* https://www.trai.gov.in/sites/default/files/CP_16122021_0.pdf (Accessed 10 September 2024).

time or near-real-time responses are necessary, such as autonomous vehicles, industrial automation, and IoT systems.[7]

2.1 Unlocking Efficiency: The Multifaceted Benefits of Near Data Processing (NDP)

(a) Reduced Latency: It involves the reduction of time consumed by data to move from its source to the processing unit and *vice-versa*. This feature becomes critical when immediate responses are critical. In this context, the NDP accelerates performance by conducting computations closer to where data is generated, hence reducing delays in data transmission over the network.

Instances:

- Autonomous Vehicles: Real-time sensor data processing within an autonomous driving system-especially from LIDAR and cameras-is highly needed in making immediate decisions for safe navigation. In other words, Tesla's "autopilot" system performs a local processing on the onboard computer in the car, interpreting sensor data in real time to enable quick reactions to the surroundings and possible dangers.[8]
- Financial Trading: For financial trading, too, the NDP plays an important role in high-frequency trading platforms that need to process financial data with the least latency. Algorithmic trading firms establish local processing near or within data centers located close to the stock exchanges to shave precious milliseconds over their competitors and execute trades faster.

(b) Bandwidth Efficiency: It saves on the amount of information to be transferred over the network. By processing data locally, NDP reduces the volume of data sent to central servers, hence easing network congestion and reducing operational costs.

Instances:

- Video Analytics at the Edge: Large-scale video surveillance installations, as done by city authorities for public safety, can enable video analytics at the very source of the feed through NDP.

---

[7] Hassanpour, M.; Riera, M.; González, A. A Survey of Near-Data Processing Architectures for Neural Networks. *Mach. Learn. Knowl. Extr.* 2022, *4*, 66-102 *available at:* https://doi.org/10.3390/make4010004

[8] Gupta, A. et al. (2021) *Deep learning for object detection and scene perception in self-driving cars: Survey, Challenges, and open issues*, Available at https://doi.org/10.1016/j.array.2021.100057

Cameras, for instance, can be enabled to analyze video feeds at the edge for unusual activities, recognize faces, or whatever, and send only relevant data-alerts-to the central servers. This reduces the amount of video data being transmitted across, hence reducing the network load.[9]

- IoT Sensor Networks: Many Industrial IoT applications make use of more than one sensor, each generating quite a large volume of data. For example, smart factories are using edge computing to analyze data locally from machinery for anomalies and to project where maintenance is needed without sending the data to the central server continuously. This minimizes network overheads and allows for far more efficient handling of the data.[10]

(c) Higher Scalability: The facility of extending a system and handling it in a better way by distributing the processing work. NDP basically enables scalability by permitting local processing across more devices or nodes, hence spreading the computational load and reducing stress on the central systems.

Instances:

- Smart Grids: In the modern smart grid, through solar panels and wind turbines, distributed energy resources become managed at the local edge device level. Processing on-site data, such devices manage the distribution and consumption of energy optimally, thereby reducing the burden of central grid management systems to scale the grid efficiently with increased new energy sources.[11]
- Content Delivery Networks (CDNs): These are systems of CDN that utilize edge servers for caching and delivery of web content closer to the end users. For example, Netflix is a video streaming firm that depends on a network of edge servers that process the content for delivery at the location of each user.

(d) Better Data Privacy: The idea here is to reduce the 'exposure' risk of sensitive data by keeping its processing closer to the source. A

---

[9] Myagmar-Ochir, Y.; Kim, W. A Survey of Video Surveillance Systems in Smart City. *Electronics 2023*, *12*, 3567. *available at:* https://doi.org/10.3390/electronics12173567

[10] Dave , D. (2024) *Edge computing: Use Cases in Manufacturing and IoT*, *Available at https://doi.org/10.21428/e90189c8.91411aea*

[11] Meliani , M. (2021) *Energy management in the smart grid: State-of-the-art and future trends*, *Sage Journals*. *available at:* https://doi.org/10.1177/184797902110329

design would minimize the need to transport data, which can be intercepted or suffer a breach.

Instances:

- Health information can be processed within the edge, meaning it is within the medical device or even within the hospital system. It remains better protected because less data is sent out of the device, and only what's considered necessary information is accessed.[12]
- Smart Home Devices: The typical example of devices that use more of local processing includes smart home systems, voice assistants, and smart thermostats that handle user commands and user preferences. This helps protect user privacy because the amount of data being sent over the internet is reduced.[13]

3. Balancing Innovation and Privacy: Navigating the Risks of near Data Processing

While Near Data Processing offers a number of benefits, it is also lumbered with a whole load of privacy and security risks that have to be ironed out. This results from its processing done locally and proximity-based nature of NDP.

3.1 Vulnerabilities and Exposure to Sensitive Data

(a) Security of Local Device: The edge devices and local servers used in NDP may not provide the same level of protection as does the centralized data center for the security-sensitive information. Because they are often at the edge of the network or in remote locations, they may be more vulnerable owing to limited resources and lack of dedicated security personnel, even physical tampering.[14] Without proper safeguards, they might become potential entry points into the network by malicious actors who want to steal sensitive data or disrupt critical operations.

Examples:

---

[12] Li , C. (2024) *A review of IoT applications in healthcare*, *Neurocomputing,* Elsevier*, available at:* https://doi.org/10.1016/j.neucom.2023.127017

[13] *Ibid*.

[14] Ganesh, D. (2022) *Improving security in edge computing by using cognitive trust management model*, *Proceedings of the International Conference on Edge Computing and Applications, Available at:* https://doi.org/10.1109/ICECAA55415.2022.9936568

- IoT Device Vulnerabilities: The Mirai botnet attack in 2016 satisfactorily showed the security risks of IoT devices. The attackers used the vulnerabilities in unsecured IoT devices and then launched a large-scale Distributed Denial of Service (DDOS) attack.[15]
- Medical Devices: Connected medical devices, such as insulin pumps, were reported to have security defects in 2020. Such defects could enable unauthorized access to sensitive patient information and the operations of the device.[16]

(b) Data Breaches: The concept of local storage and processing increases the risks of data breaches naturally by increasing the number of vulnerable points which could be targeted within a network. Unlike centralized data centers that have stronger and more focused security measures, every edge device and each local server in the configuration of an NDP represents a single line of vulnerability to be protected. Such edge devices range from IoT sensors to industrial controllers, often deployed across varied and sometimes less-than-secure environments. As a result, they will miss out on some of the advanced security features inherent in the architectures of centralized systems, such as advanced firewalls, intrusion detection systems, and occasional software updates.

Examples:

- Ransomware attacks: The 2021 ransomware attack against Colonial Pipeline led to fuel supply-chain hiccups in the U.S. The attackers took advantage of the weakest links within the local IT infrastructure in order to encrypt data and demand a ransom. This has been indicative that local processing systems may be focused targets for breaches and ransomware attacks.[17]

---

[15] Wazzan, M.; Algazzawi, D.; Bamasaq, O.; Albeshri, A.; Cheng, L. Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research. *Appl. Sci.* 2021, *11*, 5713. *available at:* https://doi.org/10.3390/app11125713

[16] Sadek, I. (2022) *Security and privacy in the internet of things healthcare system: towards a robust solution in real life deployment, Computer methods and programs in biomedicine update,* Elsevier*, available at:* https://doi.org/10.1016/j.cmpbup.2022.100071

[17] Mackenzie , A. (2022) *Cyber risks, potential liabilities and insurance responses in the marine sector, Swansea University's research repository, available at:*

- Attacks on Edge Devices: Researchers in 2022 identified specific vulnerabilities on different smart home devices. Those are able to get unauthorized access and further cause data breaches.[18]

(c) Physical Access Risks: It is very crucial to provide physical security to the devices that are related to Near Data Processing, as this unauthorized access can bring high risk. As such, edge devices and local servers often need to be deployed in diverse, and sometimes insecure, physical environments, such as public spaces, remote locations, or workplaces with limited physical security measures. Consequently, this might lead to serious consequences if unauthorized access is gained to these devices for the purpose of extracting or tampering with data.[19] But this exposure not only puts the confidentiality and integrity of data at risk but also may lead to larger security breaches, with the compromised devices probably turning into points of entry.

Examples:

- Data Center Breaches: Physical security breaches in data centers, where unauthorized access was given to sensitive data, came into light many times in 2021.
- Smart City Infrastructure: Most of the critical infrastructures in smart cities rely on local processing, including traffic management systems. Physical attacks on such systems could compromise sensitive data and city operations.

3.2 Proximity-Based Processing and Unauthorized Access

(a) Increased Attack Surface: Offloading processing to a large number of edge devices and local nodes significantly increases the attack surface, meaning there would be a larger number of entry points that an attacker can penetrate. Unlike the traditional centralized systems with a couple of highly secured data centers, the NDP environment contains an innumerable amount of edge devices, starting with IoT sensors and industrial controllers to smart appliances and even local servers, which are deployed across diverse

---

https://cronfa.swan.ac.uk/Record/cronfa62362/Download/62362__26326__fd31d95fab164cdea1bd085141e62012.pdf (lasted visited September 10, 2024).

[18] *ibid*.

[19] Schiller, E. (2022) *Landscape of IOT Security, Computer Science review,* Elsevier, *available at:* https://doi.org/10.1016/j.cosrev.2022.100467

and often less secure locations.[20] Each of these devices presents another one-dimensional vulnerability opening yet another door for bad actors if not properly protected. However, this challenge is exacerbated by the heterogeneity of these devices, which come with different levels of security measures, firmware, and configurations that make enforcing uniform protection hard. Also, most of these devices are deployed in an environment where physical security is lax, thus making them highly susceptible to tampering and unauthorized access.

Examples:

- 5G Networks: The rollout of 5G brings in many edge devices to handle the additional data traffic. That is to say, as the 5G networks expand, so does the attack surface.[21]
- Smart Farming: Precision agriculture deploys devices along the edge that monitor or set different farming operations. Each of these devices represents another point of vulnerability that has to be secured from unauthorized access and breaches.
- Data Interception: Even though the volume of data transmitted over networks is low, hence the local processing in NDP systems makes sure that massive data transfers are minimal in need, data transmission does not totally disappear.

(b) Data interception: There are multiple scenarios where data needs to be synchronized with the central servers for aggregation, analysis, and even sharing between devices; this clearly introduces the risk of data interception during transmission. This is because while local processing handles the data on-premise, the transportation of information between local devices and central systems may expose sensitive information to interception, should it not be encrypted to an adequate standard.[22]

Examples:

---

[20] *Ibid*.

[21] Dangi, R.; Lalwani, P.; Choudhary, G.; You, I.; Pau, G. *Study and Investigation on 5G Technology: A Systematic Review*. *Sensors* 2022, *22*, 26. *available at:* https://doi.org/10.3390/s22010026

[22] Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. *A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review*. *Sensors* 2023, *23*, 4117. *available at:* https://doi.org/10.3390/s23084117

- Video Surveillance: Unencrypted data streams were intercepted in video surveillance systems, reported in 2023. The situation clearly indicates the requirement for data encryption during transmission between local processing units to the central servers.
- Smart Grid Communications: In smart grids, data transmitted between local energy meters and central systems can be sniffed if not encrypted. Therefore, this provides a high risk that warrants a secure protocol for protecting data in flight.
- Data Integrity: Assurance of integrity of the data being locally processed is of paramount importance in trusting data-driven systems. As they are processed on the edge or on local servers, these data become exposed to many risks that may affect their accuracy and veracity. If proper validation and verification do not take place, data can be manipulated or altered well before the time of analysis or transition of data to central repositories.

(c) Data integrity: This risk is very high in an environment when multiple devices or systems handle the data, each having its own set of vulnerabilities. Therefore, technologies like blockchain can make an immutable record of data transactions that enhance data integrity by detecting and verifying unauthorized changes.[23]

Examples:

- Data Integrity Blockchain: IBM, in 2022, did introduce blockchain-based solutions that ensure data integrity in supply chain management. Blockchain's tamper-evident features indeed help to maintain data accuracy and prevent unauthorized modifications, thus showing good attitude towards protection against data integrity in local processing environments.[24]
- Federated Learning: The use of federated learning-harnessing companies like Google and Apple-allows training a model without necessarily centralizing raw data on local devices. This approach

[23] Sashidhar, D. (2023) *Impact of controls on data integrity and information systems, Science and technology review,* Science and Technology, 2023; 13(2): 29-35, *available at:* https://doi.org/10.5923/j.scit.20231302.04

[24] Xu P, Lee J, Barth JR, Richey RG (2021), "Blockchain as supply chain technology: considering transparency and security". International Journal of Physical Distribution & Logistics Management, Vol. 51 No. 3 pp. 305–324, Available at https://doi.org/10.1108/IJPDLM-08-2019-0234

contributes to data integrity by keeping it local, hence reducing its vulnerability to tampering during transmission.

3.3 Latest advancements in NDP and Privacy Management

a) Edge AI and Federated Learning: Edge AI allows them to process more data with advanced analytics on the device itself, while in the case of federated learning, training of models across a host of devices is possible without the need for data centralization. Federated Learning by Google: Google has already applied it in their Gboard keyboard. Predictive text models get trained on the user's device and do not send raw data to the cloud.[25]
b) Improved Encryption Protocols: So far, the development in encryption technologies like homomorphic encryption and secure multi-party computation has allowed processing data without decryption. In 2023, a team of researchers at MIT demonstrated that performing secure data analysis using homomorphic encryption is practical. This technology allows for keeping data encrypted even while it is in process, hence allowing minimal unauthorized access to the data.[26]
c) Security Solutions Integrated: Secure boot, hardware-based encryption, and intrusion detection systems are among many security features integrated into modern devices on the edge or local servers. Intel Hardware Security: Advanced security capabilities, such as hardware-based encryption and secure boot mechanisms, are integrated into Intel's processors starting with products introduced in 2024 to protect locally processed data.
d) Blockchain Technology: Blockchain, due to its decentralized nature, enhances security and integrity in the data maintained at the local level and provides a tamper-evident record of transactions. Supply Chain Solutions: This year, 2023, companies

[25] Singh, R. (2023) *Edge AI: A survey, Internet of things and cyber physical systems*, Elsevier, *available at:* https://doi.org/10.1016/j.iotcps.2023.02.004

[26] Lezzi, M. (2020) *Practical privacy-preserving data science with homomorphic encryption: An overview*, *Research gate. available at:* https://doi.org/10.1109/BigData50022.2020.9377989

such as IBM and Walmart were able to apply the technology in blockchain to track and verify supply chain data.[27]

4. Guardians of Data: Navigating Confidentiality and Safeguards in the Digital Age

Data confidentiality refers to the protection of information against unauthorized access and exposure. In modern digital systems, this would mean the basis for individual privacy and trust in technological infrastructures.[28] As data becomes more pervasive and computing capabilities advance, sensitive information-anything from personal identification details to financial records-is ever more exposed to the risks of unauthorized access and exploitation. Data confidentiality ensures that data is made available only to those who are explicitly authorized; hence, it protects the right to privacy and prevents possible misuse.

As data is generated and shared at a very fast rate in this digitized world, protection of data confidentiality cannot be viewed as purely a technical issue but a fundamental right to the person. Legal regulatory frameworks such as the General Data Protection Regulation in Europe and the California Consumer Privacy Act of the United States, among others, make safeguarding personal information a paramount concern and one of the most essential elements of privacy protection.[29]

4.1 Fortifying the Frontier: Strategies for Securing Data in Near Data Processing Environments

The principle of NDP is to bring processing closer to the source of data. Better performance and efficiency can be seen through reduced latency and bandwidth usage.[30] This proximity to data increases some

---

[27] Sharma, M. and Kumar, P. (2021a) *Adoption of Blockchain Technology: A case study of walmart*, *Research gate*. *available at:* https://www.researchgate.net/publication/352698139_Adoption_of_Blockchain_Technology_A_Case_Study_of_Walmart (Accessed: 12 September 2024).

[28] *Ibid*.

[29] General Data Protection Regulation (EU).

[30] Santos, C. and Carro, P. (2021) *Survey on Near-Data Processing: Applications and Architectures,* Journal of Integrated Circuits and Systems. *available at:* https://doi.org/10.29292/jics.v16i2.502

interesting challenges regarding the confidentiality of data. Several strategies can be adopted to mitigate these risks:

a) Encryption: One of the best ways to ensure data confidentiality is through the method of encryption. In encryption, information is converted into a form that cannot be read except through the use of the proper decryption key. In NDP environments, encryption may be applied to both data at rest-that is, stored data-and data in transit-that is, data in transfer. Advanced encryption standards provide one widely used technique for securing sensitive information.
b) Access Controls: Strong access controls ensure that sensitive data is accessible to only authorized users and systems. This is implemented through mechanisms of permission and authentication to verify the identity of users and their associated rights of access. Mechanisms such as multi-factor authentication make this even more secure by requiring more forms of verification. Both Role-Based Access Control and Attribute-Based Access Control work to control access based on the user roles and attributes, respectively. In either case, access is allowed only to users with permissions that provide access to view the data.
c) Data Governance: Effective data governance entails a set of policies and procedures that concern the availability, use, and integrity of data. It has well-defined regulations concerning the processing of data, like data classification, retention policies, and incident response schemes. The implementation of data governance tools will monitor and prevent data from being accidentally or mischievously leaked, such as the use of DLP solutions.
d) Data Masking and Anonymization: Different techniques can be employed: these are namely data masking and anonymization. Masking is the process whereby sensitive data is replaced by fictional data, yet as realistic as possible. In anonymization, the removal of personally identifiable information should be done in such a way that traceability is not possible.

4.2 Guarding the Gates: Overcoming Challenges in Achieving Robust Data Security

Despite the implementation of advanced security measures, several challenges persist in maintaining data confidentiality, especially in NDP environments:

a) Complexity of Security Integration: It follows, therefore, that complex processing of data may not be conducive to pervasive security. Normally, NDP environments consist of many layers of processing and storage; each layer may also have its own requirements from the viewpoint of security. When each and every component is to be secured, then ensuring that clouds are properly protected can be a challenging affair—it may prove to be very costly.[31]

b) Emerging Threats: The threat landscape keeps on changing; every day, some new vectors of attack or advanced technique keep on surfacing. Cybercriminals and hackers come up with novel ways to exploit emerging vulnerabilities daily.[32] Therefore, the ways in which security controls are applied should be renewed and altered at regular intervals also.

c) Human Error: Most breaches and security incidents in general happen because of human mistakes. Misconfigurations, poor access controls, and even incorrect publication of sensitive data are very common to accidentally break data confidentiality.[33] Training and awareness programs do much to alleviate these risks, but the human element seems to be a persistent problem in the pursuit of good security.

---

[31] Rafael Yuste (2023) *Advocating for neurodata privacy and neurotechnology regulation,* Nature protocols, *available at:* https://doi.org/10.1038/s41596-023-00873-0

[32] Jared Genser et al., (2024) *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies,* Neurorights foundation, *available at:* https://perseus-strategies.com/wp-content/uploads/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf (Accessed: 12 December 2025).

[33] Daniel Susser & Laura Y. Cabrera (2023): *Brain Data in Context: Are New Rights the Way to Mental and Brain Privacy?*, AJOB Neuroscience, *available at:* https://philpapers.org/archive/SUSBDI-2.pdf (Accessed: 12 December 2025).

d) Performance v. Security Trade-offs: In general, some kind of tradeoff needs to be done in NDP environments: a tradeoff between performance and security. While encryption and access controls enhance data confidentiality, they add latency and computational overhead, potentially degrading performance.
e) Legal and Regulatory Compliance: If one adds adherence to legal and regulatory requirements, it gets even more complicated. Various jurisdictions have different regulations with respect to data protection, and sometimes such adherence turns out to be quite problematic for those organizations which operate across several regions.[34]

5. Navigating Privacy in Law Enforcement: A Critical Examination of the Criminal Procedure (Identification) Act, 2022

The Criminal Procedure Identification Act 2022 marks a paradigm shift in the Indian legal regime with respect to dealing with the collection and management of biometric data.[35] The Act was enacted in August 2022 and enabled the police to collect far-reaching biometric data of persons convicted or suspected of certain serious offenses.

5.1 Legal Implications of the Act on Data Privacy

The Criminal Procedure (Identification) Act, 2022, raises significant concerns regarding data privacy and constitutional rights, particularly the right to privacy under the Indian Constitution.

5.1.1 Article 21 and the Right to Privacy[36]

(i) The Criminal Procedure (Identification) Act, 2022: An Overview

The Act significantly expands the scope of biometric data collection by law enforcement agencies. It allows the collection of the following data:

- Fingerprints, palm prints, and footprints
- Iris scans, retina scans, and facial recognition data
- Physical and biological samples, including DNA
- Behavioral data such as handwriting and voice samples

---

[34] D. Hallinan et al., 2014, Privacy issues in neurodata management, Surveillance and Society, *available at:* https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata. (Accessed: 12 December 2025).

[35] The Criminal Procedure Identification Act 2022.

[36] Art.21, The Constitution of India.

The Act allows the police to collect such information from not just convicted persons but even from persons arrested on charges punishable with imprisonment for more than a year. It replaces the more limited Identification of Prisoners Act, 1920, which allowed basic identifiers (such as fingerprints) to be collected only from convicted individuals or those on trial.[37]

(ii) Right to Privacy and the Puttaswamy Judgment

The right to privacy was established as a fundamental right emanating from Article 21 of the Constitution.[38] The Supreme Court held that the right to privacy is an inalienable ingredient of the right to life and personal liberty and should be guarded against any action of the state which is unwarranted. In so doing, it evolved a three-pronged test to establish whether a law circumscribing privacy may be valid:

- Legitimate Aim: The restriction is to serve a legitimate state interest.
- Proportionality: The means adopted to achieve that aim must be proportionate.
- Necessity: The measure must be the least restrictive alternative available to achieve the legitimate aim.[39]

(a) Violation of the Proportionality Principle

The sweep itself makes the Criminal Procedure Identification Act fail the proportionality test. Invasive biometric data collection can be allowed on one hand for individuals who have been arrested for an offense punishable with imprisonment for a term of one year or more, without any regard to the seriousness of the crime.

Issues:

- Broad scope of data collection: Collecting DNA and other biological samples from individuals who may not even be convicted or formally charged is a disproportionate threat compared with the personal liberty of the individual. DNA has the ability to disclose extremely private information about a person, such as genetic predispositions, far beyond identification purposes.

---

[37] The Identification of Prisoners Act, 1920.

[38] Art.21, The Constitution of India.

[39] Justice K.S.Puttaswamy vs Union of India, AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018) 12 SCALE 1, (2018) 4 CURCC 1, (2018) 255 DLT 1, 2018 (4) KCCR SN 331 (SC), AIRONLINE 2018 SC 237.

- Lack of differentiation: There is no clear distinction between different classes of crimes committed concerning the requirement of collecting data. The Act operates indiscriminately both for serious and minor offenses, totally disregarding the principle of necessity and disproportionate invasion of privacy.

(b) Absence of Adequate Safeguards

Another major problem with the Act is that there are no safeguards with respect to data retention, use, and destruction.

Issues:

- Lack of clear limits on data retention: Further, the Act fails to give any length of time for which this data is retained or when deleted, particularly when charges against the person are acquitted or dropped. This raises valid concerns of perpetual surveillance.
- Ambiguity in data sharing: There is no transparency regarding who has access to this data, how it will be shared with other government or non-government entities, and for what purposes.[40].

5.1.2 Violation of Article 20(3): Protection Against Self-Incrimination

Article 20(3) of the Constitution has thus provided that "no person accused of any offense shall be compelled to be a witness against himself."[41] The Supreme Court has explained this provision to imply that an accused cannot be compelled to give testimonial evidence of communicative nature, disclosing personal knowledge or information.

While physical identifiers like fingerprints and facial recognition data clearly fall within the non-testimonial evidence category, DNA and other biological samples that would be collected under the Act could well cross that line. Whereas DNA provides not only identification information but also incriminating evidence-for example, whether one was at a crime scene, personal information about one's medical history, and genetic disorders-all very different from being a neutral identifier.

Issues:

---

[40] Siddharth Shekhar (2023) *An Analysis of The Criminal Procedure (Identification) Act, 2022,* Indian journal of integrated research in law, *available at:* https://doi-ds.org/doilink/06.2023-22636387/A29

[41] Art.20, The Constitution of India.

- Use of DNA as evidence: DNA evidence discloses intimate facts about a person, which might incriminate him before the court of law; it is inherently speech-like in content. Forcing an individual to submit such evidence may amount to violating Article 20(3) in those cases where the person is not convicted.
- Potential for misuse: The DNA extracted could be used by the police in some other case to implicate a person or force confessions out of him-an act that may be termed self-incrimination of a sort.[42]

5.1.3 Article 14: Equality Before Law and Arbitrary State Action

Article 14 provides for the right to equality before the law and protection from arbitrary exercise of state power. A law is vulnerable to being struck down as unconstitutional if it enables arbitrary or disproportionate action.[43]

Issues:

- Arbitrary application: The Act provides untrammeled powers to the police without laying down guidelines on how these powers would be exercised; given this fact, there is a strong possibility of selective targeting and disproportionate utilization of the methods of data collection, more so against communities that are already marginalized.
- Discriminatory impact: This failure to distinguish clearly among offenders according to the seriousness of their alleged offense or their potential for recidivism opens the door to arbitrary exercise of authority. Such selective application of the law can result in the harassment of weak segments of society, such as minorities and economically underprivileged classes of citizens, which in effect denies equality before the law.[44]

---

[42] Dhaval Kakkad (2023) *The Criminal Procedure (Identification) Act, 2022 And Its Relation With The Identification Of Prisoners Act, 1920,* Indian Journal of Law and Legal Research, *available at:* https://d1wqtxts1xzle7.cloudfront.net/112107645/ (Accessed: 12 December 2025).

[43] Art.14, The Constitution of India.

[44] Angad Chaudhary (2022), *The New Criminal law Identification Act 2022,* Indian journal of law and legal research, *available at*: https://ijirl.com/wp-content/uploads/2022/09/new-criminal-law-identification-amendment-act-2022-.pdf (Accessed: 12 December 2025).

5.1.4 Concerns about Mass Surveillance and State Overreach

This offers a gateway to mass surveillance by collecting biometric data from the citizens on such a large scale. The centralization of this biometric database also opens up a potential for using this information for uses other than criminal investigations, such as for the purpose of surveillance, profiling, or even tracking an individual. Such possible misuse directly threatens civil liberties, especially when looked at through the lens of state overreach.

Issues:

- Mass data collection and surveillance: It creates a system of mass surveillance, in which large-scale collection of biometric data among scores of people, many of them perhaps innocent and some accused of minor offenses, is being carried out. The potential for misuse by law enforcement or other state agencies is high, in the absence of strong legal safeguards.
- Precedent for future expansions: Once there is a centralized biometric database, it sets a dangerous precedent toward expansion in other areas of civil life. The risk now becomes greater or diminishing civic freedoms as the state will have acquired the potential to track movements and transactions undertaken by the citizens[45].

5.2 Civil Liberties at Risk

The introduction of extensive biometric data collection under the Criminal Procedure (Identification) Act, 2022, has raised concerns about the potential for misuse and the erosion of civil liberties.

(a) Potential for Misuse of Biometric Data:

- Data Security Risks: This single point of failure creates a central repository of this information. A breach in the stored data or unauthorized access to the database may result in sensitive personal information being exposed and is usable for identity theft or other such pernicious activities.
- Surveillance and Tracking: This will create a broad database on biometric information that might lead to mass surveillance. It

[45] Vaibhav Yadav (2022), *Analysis of India's Criminal Procedure (Identification) Act, 2022: Determining Potential Misuse and Possible Violations of Fundamental Rights,* Cambridge University Press, *available at:* https://doi.org/10.1017/cri.2022.17

adds to the concerns of law enforcement agencies misusing the information provided to them for purposes other than its usage and to monitor people without adequate checks and controls.[46]

(b) Concerns Around Abuse and Mass Surveillance:

- Overreach by Law Enforcement Agencies: General provisions of the Act are too wide and could be lead to overreach by law enforcement agencies. It may also be used discriminatorily against marginalised communities.
- Lack of Oversight and Accountability: The Act is silent on the procedural aspects of oversight and accountability in dealing with biometric data. Without appropriate mechanisms of transparency and accountability, abuse is more likely to occur, which may affect the trust that the general public would show toward the use of their biometric data in the realm of criminal justice.

5.3 Judicial response

(a) Selvi vs. State of Karnataka (2010)[47]

The Supreme Court was called upon to decide upon the involuntary extraction of scientific evidence and its clash with Article 20(3), which guarantees protection against self-incrimination. The matter involved the admissibility of scientific techniques such as narco-analysis, polygraph tests, and brain-mapping. The Court held that the involuntary administration of such techniques was in violation of Article 20(3), for the reason that the use of compulsion upon the individual to implicate himself violated his right to privacy and personal liberty under Article 21, too. It was held by the Court that none of these techniques can be employed without obtaining the consent of the individual. This judgment is very relevant in the context of examination of the Criminal Procedure (Identification) Act, 2022, more particularly concerning mandatory collections of biometric data inclusive of DNA samples. DNA collection can be argued to fall under

---

[46] GS Bajpai et al., (2022) *Questioning the Feasibility of the Criminal Procedure (Identification) Act, 2022,* Practical lawyer, *available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4795941 (Accessed: 12 December 2025).

[47] *Selvi & Ors v. State of Karnataka*, AIR 2010 SUPREME COURT 1974 2010 (7) SCC 263, 2010 AIR SCW 3011.

the purview of self-incriminating evidence, especially when it is collected from individuals who are mere suspects or those not convicted of any crime.

(b) State of Bombay v. Kathi Kalu Oghad[48] (1961)

The Supreme Court interpreted Article 20(3), which dealt exclusively with the issue of self-incrimination. The Court held that fingerprints, handwriting samples, and other physical identifiers do not come under the purview of self-incriminating evidence since they do not involve imparting personal knowledge. These physical characteristics, the Court held, are used only for identification purposes. While Kathi Kalu Oghad supports the collection of physical identifiers like fingerprints, the Criminal Procedure Identification Act, 2022 goes beyond that in allowing the collection of more invasive data like DNA and biological samples, which may not be merely for identification purposes but could reveal intimate personal details likely to violate privacy and the right against self-incrimination.

(c) Report of the Justice B.N. Srikrishna Committee (2018) on Data Protection[49]

The Srikrishna Committee, headed by the Chair Justice B.N. Srikrishna, had been formed to draft a data protection framework for India. Its report reflected that there was a dire requirement for a comprehensive data protection law, especially due to the development of new technologies and the collection of massive amounts of data by public and private entities. Based on that report, the Data Protection Bill drafted a number of safeguards.

- Limitation of purpose: The collection should be for a defined and legitimate purpose.
- Data Minimization: It emphasizes that collection of data should be restricted to what is absolutely necessary for a certain purpose.
- Storage limitation: Personal data should not be stored longer than necessary.

---

[48] State of Bombay vs. Kathi Kalu Oghad 1961 AIR 1808, 1962 SCR (3) 10, AIR 1961 SUPREME COURT 1808

[49] A free and fair digital economy, *available at*: https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (Accessed: 12 December 2025).

Most of the safeguards listed herein are missing in the Criminal Procedure Identification Act, 2022, hence raising reasons of apprehension as regards data retention and purpose limitation and data minimization. It is, in fact, at this juncture that the Srikrishna Committee report mentions that any collection of sensitive personal data such as biometric data has to be facilitated by a proper data protection framework, which is lacking in India at present.

5.4 International and Human Rights Perspectives

(a) European Union's General Data Protection Regulation (GDPR) and International Data Protection Standards

While not a judicial precedent, the GDPR provides an important reference point for understanding international best practices in data protection and the rights of individuals concerning their personal data. The GDPR establishes:

- The right to be forgotten
- The right to data portability
- Consent-based data collection

Although India's legal framework differs from the EU's, these standards offer insight into the shortcomings of the Criminal Procedure (Identification) Act, 2022, which lacks clear provisions for data protection, consent, and the right to erasure.

(b) Reports and Observations by Human Rights Organizations

Several human rights organizations and civil society groups have raised concerns about the Criminal Procedure (Identification) Act, 2022 and its impact on privacy and civil liberties.

- Amnesty International has pointed out that biometric data collection could lead to disproportionate state surveillance.[50]
- The Internet Freedom Foundation (IFF) in India has raised concerns about the Act's potential for misuse, particularly the risk of profiling and targeting marginalized communities.

These organizations emphasize the need for:

- Judicial oversight over data collection processes;
- Strict data protection measures;

---

[50] *Amnesty International and more than 170 organisations call for a ban on biometric surveillance,* Amnesty International, *available at:* https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/ (Accessed: 12 December 2025).

- Transparency and accountability mechanisms in the use of biometric data.

6. Striking the Right Balance: Aligning Data Management Efficiency with Privacy Protections

Presently, efficient data management really needs to be weighed against robust privacy protection, an issue which is rapidly reaching an extremely urgent state. This is because, with the rapid rise in technologies for collecting, processing, and storing huge volumes of personal data, especially biometric data, there are new challenges for both individuals and their regulatory bodies. While the Criminal Procedure (Identification) Act, 2022 seeks to enhance the police in gathering much information, especially on biometric data, the consequences have extremely cogent ethical questions on privacy and civil liberties, which, consequently, could lead to misuse.

6.1 Ethical Concerns in Data Management

The data of biometrics include DNA samples, iris scans, and fingerprinting-essentially very sensitive information and quite unique to individuals. Misuse or unauthorized access to this data may lead to situations that are serious, from violation of privacy to wrongful identification and discrimination.

(a) The Ethical Dilemmas of Biometric Data Use

Unlike other data, biometric data can never be replaced since it is permanent and remains identical throughout a person's life. Thus, there is an ethical dilemma on how such data will be collected, stored, and used by the state. Because it is permanent data, breaches have serious long-term impacts which may affect individuals for all their lives. The application of biometric data in criminal justice bears the potential of increasing inequality conditions than trying to solve them. Such collected data may be further used for profiling against marginalized groups, such as minorities or economically deprived groups of society, with the potential to further lead to discriminatory practices. Secondly, the lack of consent/choice in providing such data may be further questioned from the perspective of personal autonomy and ethical principles of informed consent.[51]

---

[51] Jeevan Shekar, *The Cultures, Colonialities and Criminal Identifications,* SSRN, *available at:*

(b) Privacy as a Fundamental Ethical Concern

The noxious ethical debate in the issue of data management arises on the point of privacy. Privacy, as a fundamental right, has been identified to be intrinsic to personal liberty by the judgment of *Puttaswamy*. A situation when an individual is compelled to submit his biometric data to the state, that is an invitation for the state towards surveying and controlling. There is, therefore, a tendency that, if not put under stringent checks and balances, the collection may exceed the intention and will breach the right of the individual to privacy and self-determination.[52] Application of biometric data should, then, be under scrutiny with care for ethical acceptability. It shall ensure that data collected is limited to necessity and for a valid purpose, provided on a voluntary basis.

6.2 Safeguards to Prevent Misuse: Legal and Technological Measures

(a) Comprehensive Data Protection Legislation

For a country like India, a comprehensive data protection law is an immediate requirement. The legal vacuum in this respect has given adequate scope for amounts of ambiguity in how biometric data would be treated. The Personal Data Protection Bill (PDPB) has a crucial opportunity here to set up standards around the collection, storage, and usage of data. This covers:

- Consent-based Collection: PDPB mandates that any collection of personal or biometric data must be done on a principle of informed consent. In other words, this means individuals must know for what purpose their data is collected, how it is going to be treated, and for how long the data needs to be maintained. Similarly, exceptions to the above would also be very strict in nature; for example, criminal investigations might require the collection of data, but this too should be done with stringent oversight and checks so that arbitrary or excessive collection of data does not occur.

---

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5347846 (Accessed: 12 December 2025).

[52] Satyajeet Panigrahi (2025) *Fingerprinting Freedom: A Case of Over-Policing Under the Criminal Procedure (Identification) Act, 2022,* Rethinking police for a better future, *available at:* https://doi.org/10.1007/978-3-031-83173-7_15

- Data Minimisation Principle: The collection of data should not be more than required for the purpose. Hence, fingerprinting can be thus justified in identification of criminal cases, while in the case of DNA or iris scan, it can be performed so far as such is strictly necessary and proportionate.
- Retention limits and data deletion: The second most important pledge in PDPB is regarding retention limits-data is to be destroyed once its purpose is served. For instance, if biometric data is collected in a criminal investigation and the person is acquitted, then that data has to be completely deleted from police databases.[53]

(b) Judicial Oversight and Accountability Mechanisms

One of the major legal protective measures involves judicial control of the collection practice of biometric data, particularly when sensitive personal information is at issue.

- Court Authorization for the Collection of Biometric Data: In the case of biometric data collection, the police should get a court order at least in non-serious cases or where such collection may amount to the violation of the rights of privacy. This would ensure that arbitrary collection does not take place, and it is collected only when it is absolutely necessary.[54]
- Periodic Judicial Reviews: In addition to court orders, judicial review of data collection practices must be undertaken to secure accountability in this regard. Periodic audits of the collection, storage, and usage of biometric data by law enforcement agencies prevent abuse and ensure that the standards of the law are upheld. These may also include reviews of data retention time and the respect for privacy rights amongst individuals.

(c) Independent Oversight Bodies

The other important legal safeguard would be the setting up of autonomous monitoring bodies at the level of a DPA, for instance. It

---

[53] Ankit Yadav (2024), *An Analytical Study Of Criminal Procedure (Identification) Act 2022 With Special Reference To Human Rights Perspective,* Indian Journal of Legal Review, *available at:* https://ijlr.iledu.in/wp-content/uploads/2024/09/V4I2169.pdf (Accessed: 12 December 2025).

[54] Paul Scott (2022) *Authorising Crime: The Covert Human Intelligence Sources (Criminal Conduct) Act 2021,* The Modern Law review, *available at:* https://doi.org/10.1111/1468-2230.12751

would serve as a watchdog to verify how far the collection and use of biometric data have gone, by investigating every case that might be perceived as abuse.

- Oversight-regulatory: the DPA may be tasked with verifying that law enforcement agencies abide by the laws on data protection regarding data processing, storage, and destruction. It could also be involved in the oversight of compliance with the limits on retention and data minimization.
- Complaints and Grievances: There are provisions that allow individuals whose biometric data has been collected to file complaints with the DPA when they feel their rights have been breached. The DPA could also act as an arbiter in disputes relating to improper use of data and, therefore, offer a key avenue of legal redress and compensation where data has been misused.[55]

6.3 Technological Safeguards: Security Measures and Data Management Protocols

Apart from the legal framework, there must be safeguards in the form of technologies to prevent this sensitive biometric data from falling into the wrong hands and being misused. Since biometric data is sensitive by nature, breaches or unauthorized access may have seriously far-reaching consequences in the long run.

(a) Data Encryption and Secure Storage

Among such critical technological safeguards is encryption, to be implemented to protect biometric information both during storage and in transit. End-to-end encryption needs to be implemented necessarily so that from the very time of collection of data, it cannot be decrypted until it has to be by the authorized personnel.

- Encryption both in transit and at rest: biometric data transmitted from devices to databases, other devices, or enforcement agencies and while stored in databases should be encrypted. This would mean an extra layer of security in case the data is

[55] Mahalakshmi V (2025) *Admissibility Of Fingerprint Recognition Evidence In Indian Criminal Trials: An Ict And Legal Perspective,* Indian Journal of Legal Review, *available at:* https://ijlr.iledu.in/wp-content/uploads/2025/11/V5I1366.pdf (Accessed: 12 December 2025).

intercepted or accessed because it would not be readable without a proper key for decryption.[56]

- Secure Cloud Storage Solutions: The future of law and order is inextricably linked to cloud storage, and it becomes imperative that the cloud platforms being used to store biometric data are continuing to meet the best standards for security. Zero-knowledge encryption models, wherein only an entity owning the data is able to access decryption keys, are to be considered when sensitive biometric information is stored.

(b) Access Control Mechanisms

Besides encryption, access control mechanisms are needed to ensure that such biometric data is accessible only to duly authorized personnel of the law enforcement agencies, on a need-to-know basis to limit exposure and reduce the possibility of misusing sensitive data.

- Role-Based Access Controls (RBAC): The RBAC can restrict access to biometric data by the role and clearance level of the personnel concerned. A good example would be a case whereby a minor case is being handled, perhaps by a local police officer; he should not have any access to the national biometric databases. It could also block access to brief periods and withdraw permissions once the investigation is closed.[57]
- Audit Trails: The second important part of any access control system is the audit trails. The systems can monitor and record every access event, leaving a trail of who and why people have accessed the data. Audit trails introduce another further element of accountability through the checking and documenting of any misuse or unauthorized access, adding to ease in holding individuals or agencies responsible.[58]

---

[56] SS Dari et al (2025) AI-Powered Criminal Identification in India: Evaluating Human Rights Concerns in Automated Identification Systems, SGS-Humanities and Management, *available at*: https://spast.org/index.php/sgshm/about (Accessed: 12 December 2025).

[57] Jeremy Horder (2024) *Corporate criminal liability under the Economic Crime and Corporate Transparency Act 2023,* Legal Studies, *available at:* https://doi.org/10.1017/lst.2024.46

[58] *Ibid*.

(c) Data Breach Notification Protocols

This would involve prompt notification of breaches where data is compromised, thus the affected individual can promptly take immediate action. Breaches of biometric data, given the permanency of the information involved, require prompt notice in order to mitigate injury.

- Data Breach Notification Laws: There is a dire need for stringent data breach notification mechanisms in India, through which law enforcement agencies and other data controllers should notify the concerned individual and regulatory authorities about such breaches within a stipulated timeframe. This is not only about transparency but gives the person affected an opportunity to take some mitigation measures.
- Containment and Response Plans: Besides notification, the controller shall have a well-structured response plan to contain the breach in order not to cause further damage and also to secure the breached data. Where there is any lapse in securing the biometric data or any undue delay in notifying the incident, it shall attract penalties by regulatory authorities upon the agencies concerned.

6.4 Need for Ongoing Dialogue and Collaboration

As technology is developing, so too are the risks and ways that the data can be used or misused. In this respect, there is a dire need for continuous dialogue and collaboration between all key stakeholders to ensure that legal and technological safeguards remain robust and adaptive to new challenges.

(a) Collaboration Between Legal Authorities and Law Enforcement Agencies

It requires a constant interaction between the courts and legislatures on one hand and law enforcement agencies on the other as to how best the gathering of biometric data should be done within constitutional limitations. The courts must engage in periodic reviews of the proportionality and necessity of such data collection practices so that such practices do not violate the individual's rights to privacy and civil liberties. Law enforcement agencies for their part should

engage in discussing the best practices for data protection and be open about how they treat the data they collect.[59]

(b) Ethical Input from Ethicists and Privacy Advocates

Such involvement of ethicists and privacy advocates in the policy-making process will ensure respect for human dignity, autonomy, and privacy. It would even be more instructive to see these kinds of stakeholders help guide the ethical implications of using the data in profiling, predictive policing, or mass surveillance, and their impacts, which could run contrary to the very idea of not having vulnerable groups targeted disproportionately in data collection practices.[60] Their input may shape policies that align with broader human rights standards.

(c) Technological Collaboration for Security and Innovation

This calls for collaboration between technologists, privacy experts, and policy thinkers in developing robust security measures since technologies in biometric data are changing over time. Indeed, the newest emerging technologies, such as AI and machine learning, have large potential to either protect or compromise privacy, depending on how they will be used. Through the ongoing dialogue, the stakeholders will be able to think of ways by which the development of PETs, such as differential privacy or anonymization techniques, can reduce risks associated with large-scale collection of data.[61]

6.5 Recommendations for Strengthening Safeguards

The collection and use of biometric data under laws such as the Criminal Procedure (Identification) Act, 2022 raise significant privacy concerns, necessitating the introduction of robust legal and technological safeguards.

(a) Implementation of the Personal Data Protection Bill (PDPB)

The PDPB lays down a comprehensive legal regime for data privacy and, ipso facto, biometric data. Indeed, a suite of protections are

---

[59] Martin Zieger (2025) *Ethical and legal reflections on secondary research using genetic data acquired for criminal investigation purposes,* Forensic Science International: Genetics, *available at:* https://doi.org/10.1016/j.fsigen.2024.103178

[60] *Ibid*.

[61] Utkina (2023) *Digital identification and financial monitoring: New technologies in the fight against crime,* Scientific journal of polonia university, *available at:* http://doi.org/10.23856/5842

called for in the Bill to be absolutely necessary for ensuring the gathering and utilization of biometric data in a manner that is ethical. Provisions requiring strengthening under the PDPB are:

- Consent Requirements: Section 11 of the PDPB requires that no processing of personal data may be carried out except with the consent of the data principal, meaning thereby the individual to whom the data pertains. This must be balanced quite sensitively by law enforcement agencies collecting biometric data with public safety.[62] Consent should be obtained where possible. While there might be some exemptions under the law for purposes that relate to law enforcement, when consent is not possible, any necessary oversight mechanisms must be stringent.
- Data Minimization: Section 6 of the PDPB is a proponent of data minimization wherein personal data shall be collected only to the extent that is directly relevant and necessary for a particular purpose. Such a principle has to be applied when collection of biometric data takes place under the Criminal Procedure Identification Act, 2022, where law enforcement agencies may collect minimum possible biometric data in relation to their processing over crime investigation. Examples are DNA gathering and compilation of retinal images, to which persons should not be subjected in less serious crimes since that will amount to a lack of proportionality.
- Retention limitation: Section 9 provides for data retention under the PDPB as personal data shall be retained only for such duration as is necessary to achieve the purpose for which it was collected. This should be followed strictly in the case of biometric data, making sure that this kind of data is deleted the moment use is no longer justified. The retention limit of the biometric data collected within the purview of the Criminal Procedure Identification Act, 2022, is explicitly to be amended in order to prevent indefinite storage and resulting perpetual surveillance[63].

Amendment Recommendation: Modify Section 4 of the Criminal Procedure Identification Act, 2022, to incorporate express provisions on data minimization and limits on retention that shall be in

[62] Digital Personal Data Protection Act 2023.

[63] The Criminal Procedure Identification Act, 2022.

accordance with the principles laid down by the PDPB. Lay down an explicit scheme that classifies both the nature of biometric data to be collected for different classes of offenses, as also the duration that such data is to be retained.

(b) Judicial Oversight and Regular Audits

One of the strongest checks against abuse of biometric data is judicial oversight. The Criminal Procedure Identification Act, 2022, as it stands, confers blanket powers for collection of biometric data on enforcement agencies. This works as a recipe for abuse in the absence of a strong system of oversight. For this purpose, judicial oversight, supported by routine audits, is essential to ensure that such collection of biometric data is necessary and proportionate and that it complies with constitutional safeguards of privacy.

- Court Orders for Data Collection: According to Section 3 of the Criminal Procedure Identification Act, 2022, biometric data may be collected from persons convicted or accused of certain crimes. Avowedly, however, this shall be with the approval of the judiciary in cases involving offenses that are not serious in nature.[64] Adequate law enforcement agencies must be directed to seek a court order for such collection; it will ensure that the data collection is necessary and proportionate to the nature of the offense. This will also align the law with the principle of proportionality emphasized in the *Puttaswamy judgment* (2017) recognizing the right to privacy as a fundamental right under Article 21 of the Indian Constitution.[65]
- Judicial Audits: In addition to judicial oversight at the point of collection, periodic judicial audits are necessary for oversight sharing, storage, and use of biometric data to ensure continued accountability and compliance with the legal standards. Section 8 of the Criminal Procedure Identification Act, 2022 may be reworked so as to make routine audits requisite by a specific judicial body working for the assurance of law enforcement agencies regarding the protection of data by the laws and guidelines.

---

[64] Melina (2025) *Exploring algorithmic governance: The AI act and new realities for criminal justice and fundamental rights,* New Journal of European Criminal law, *available at*: https://doi.org/10.1177/20322844251338627

[65] *Ibid*

Amendment Recommendation: Amend Section 3 of the Criminal Procedure (Identification) Act, 2022 to require judicial authorization for the collection of biometric data in non-serious offenses. Additionally, insert a provision under Section 8 for mandatory periodic judicial audits to review the use and handling of biometric data.

(c) Mandatory Data Breach Notifications

Since biometric data is immutable, its breach may have long-term effects, unlike breaches of passwords or any other personal identifier that can be changed. It is, therefore, very important to bring in a strong data breach notification regime in India, especially with regard to sensitive biometric data.

- Breach Notification: Although Section 25 of the PDPB mandates the data fiduciary - that is, the entity collecting or processing data - to report data breaches to the Data Protection Authority, in the case of breaches of biometric data, there is an urgent need to make the law even more strict through notices to the concerned individuals and the relevant authorities immediately. In this way, the affected individual will get a chance to take precautionary measures regarding one's identity, such as fraud or misuse.[66]
- Non-compliance Penalty: There must be strict penalties against late reporting of the breach of data. Though the PDPB, under Section 57, provides a penalty against non-compliance with the law, in cases of sensitive biometric data breach, this needs to be enhanced. This would ensure that the enforcement of the law, along with other agencies, pays due priority to the security of data and prevention of breach.

Amendment Recommendation: Amend the PDPB to strengthen the requirements under Section 25 for immediate reporting of biometric data breaches, both to affected individuals and to the Data Protection Authority. Ensure that the penalties under Section 57 for non-compliance are stringent enough to deter lax data protection practices.

---

[66] Vagmita Tiwari (2024) *Analysing Genetic Privacy Under The Lens Of Indian Criminal Justice System,* Indian Journal of Legal Review, *available at:* https://ijlr.iledu.in/wp-content/uploads/2024/07/V4I2102.pdf (Accessed: 12 December 2025).

(d) Establishment of an Independent Data Protection Authority (DPA)

It, therefore, calls for the establishment of an independent Data Protection Authority with main mandate in regulating collection, processing, and use of biometric data. The DPA will work as a regulatory enforcement body and also as a grievance redressal mechanism for data protection laws.

- Regulatory Oversight: The DPA should investigate breaches, audit data collection practices, and impose penalties for violations in the law on data protection. The DPA would be important, especially with respect to processing biometric data under the Criminal Procedure Identification Act 2022, to ensure that such law enforcement agencies apply the principles of data minimization, retention limits, and secure storage.[67]
- A grievance redress mechanism should be provided in the DPA, whereby an appeal against misuse or improper collection against every individual with respect to his or her biometric data will be allowed. This will give them the opportunity to contest against the law enforcement agencies with appropriate forms of remedies for privacy violations.[68]

Amendment Recommendation: Ensure that the provisions under Chapter X of the PDPB, which deal with the establishment of the DPA, are strengthened to grant the authority sufficient power to regulate and oversee the collection and use of biometric data by law enforcement agencies.

(e) Strengthening Technological Safeguards

Apart from the legal safeguards, technological protection becomes imperative to prevent unauthorized access and misuse of such biometric data. While biometric identifiers are sensitive in nature, such as fingerprints and retinal scans, or even DNA, it is the latter that requires adequate data security on the part of law enforcement.

- Encryption of Biometric Data from End to End: Biometric data shall be encrypted from creation to storage. It ensures that when collected, data is encrypted right up to its storage point, and it can

[67] The Criminal Procedure Identification Act 2022.

[68] Ankit Srivastava et al., (2022) *Impact of DNA evidence in criminal justice system: Indian legislative perspectives,* Egyptian Journal of Forensic Sciences, *available at:* https://doi.org/10.1186/s41935-022-00309-y

only be decrypted by authorized persons. This encryption secures biometric data against unauthorized access during transmission and storage, reducing the possibility of data breach.[69]

- Access Control: Biometric data shall be made available by using role-based access control. This shall grant access only to the person who really needs it, thus ensuring that the data is kept safe and secure. In addition, multi-factor authentication shall be required for all access to biometric databases, further adding security.
- Audit Trails: Accountability would be achieved by introducing audit trails in order to log access to biometric data. These trails show who has accessed the data, when it was accessed, and for what purpose. In case the information is misused or accessed without proper authority, the audit trails would facilitate an investigation into the matter that leaves a paper trail of activity for investigation and appropriate action.
- Periodic Security Audits: It is highly impotant for periodic security audits regarding the systems hosting the biometric data. Such audits shall point out the vulnerabilities and arrange for their compliance to up-to-date security standards. Section 8 of the Criminal Procedure Identification Act, 2022 should include a provision by way of amendment that there must be mandatory security audits by an independent authority.[70]

Amendment Recommendation: Amend Section 8 of the Criminal Procedure (Identification) Act, 2022 to require regular security audits of biometric data systems. Ensure that law enforcement agencies implement end-to-end encryption, access controls, and audit trails, and that these measures are updated regularly to keep pace with technological advancements.

7. Conclusion

NDP, therefore, offers transformational benefits in this rapidly changing digital environment due to its efficiency-improving nature while processing data close to their generation source, which is fast assuming criticality given the exponential growth in data volume. However, the integration of NDP technologies is equally fraught with

---

[69] *Ibid*.

[70] The Criminal Procedure Identification Act, 2022.

very grave concerns about privacy, especially regarding sensitive biometric data collection required under such laws as the Criminal Procedure Identification Act, 2022. Efficiency and security benefits of the NDP, in fact, have to be balanced against the imperatives of protection of privacy and civil liberties in their most traditional forms. Clearly, biometric data is sensitive and permanent and would raise peculiar risks of misuse and unauthorized access. There is a potential risk from unregulated data collection practices, like mass surveillance and erosion of civil liberties, and this requires stringent legal and technological controls.[71] These would come through legislation, one of them being the Personal Data Protection Bill, which lays down guidelines toward meeting this objective by consent-based data collection, minimization of data, and limits on retention. Secondly, judicial oversight, periodic audits, and even the establishment of a DPA will be very important legal interventions to ensure that the use of biometric data is transparent and accountable. Technologically, too, there are safeguards: encryption end-to-end, mechanisms of access control, and audit trails to protect the biometric data against breaches and misuse. These steps need to be revised on a regular basis as technology is still evolving to be able to handle these emerging threats. While the security of biometric data and the protection of privacy are-engaged, both legally and technologically in their continuous processes of evolution-the future challenges emanating from artificial intelligence, machine learning, and advanced surveillance technologies through ongoing dialogue and collaboration between lawmakers, technologists, ethicists, and civil society. The legal frameworks in this respect would have to evolve to match up with new technological capabilities, ensuring that no impairment of individual rights is caused. The integration of NDP technologies into practices of collection of biometric data has huge potentials but nevertheless needs to be done with care.

In balancing appropriately between innovation and the protection of privacy, India can leverage the benefits of NDP while upholding its constitutional values. A sustainable collaborative approach would

---

[71] Victor Shevchuk et al., (2022) *Criminalistic methodics of crime investigation: Current problems and promising research areas,* Revista Jurídica Portucalense, *available at:* https://doi.org/10.34625/issn.2183-2705(32)2022.ic-14

mean that the practices pertaining to data management are efficient and, at the same time, respectful of fundamental rights. Only then will watchfulness ensure that technological advancement today does not come with a cost in the form of privacy and security for tomorrow.