INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

FROM IDENTIFICATION TO SURVEILLANCE: A CONSTITUTIONAL CRITIQUE OF THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

AUTHORED BY - SAKSHI SHARMA
5th Year law student
Himachal Pradesh National Law University, Shimla

ABSTRACT

The Criminal Procedure (Identification) Act, 2022[1] (operationalised in 2023) marks a significant extension of the State's power to collect, store, and process personal and biological data of individuals involved with the criminal justice system. By replacing the Identification of Prisoners Act, 1920[2], the new regime authorises the collection of a sizeable range of "measurements", including fingerprints, palm-prints, footprints, photographs, iris and retina scans, physical and biological samples, behavioural attributes, and other biometric data. Section 349[3] of the Bharatiya Nagarik Suraksha Sanhita, 2023 (corresponding to Section 311A of the CrPC, 1973) further strengthens this structure by empowering investigative authorities to compel accused persons to provide such measurements during the course of investigation.

This paper thoroughly examines the privacy ramifications of these provisions in light of the constitutional right to privacy laid down in *Justice K.S. Puttaswamy v. Union of India* (2017)[4]. It argues that the breadth of data authorised to be collected, coupled with the wide discretionary powers conferred upon the police and prison authorities, raises grave concerns regarding arbitrariness, over-criminalisation, and surveillance-oriented governance. The retention of measurements for a period of seventy-five years by the National Crime Records Bureau (NCRB), irrespective of the nature of the offence, acquittal, or discharge, further escalates the risk of perpetual stigmatisation and misuse.[5]

Applying the four-fold proportionality test- legality, legitimate aim, rational nexus, necessity, and balancing, the paper contends that while crime prevention and effective investigation make

[1] *The Criminal Procedure (Identification) Act, 2022*, No. 11 of 2022, India.
[2] *Identification of Prisoners Act, 1920*, Act 33 of 1920 (repealed).
[3] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s. 349.
[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[5] PRS Legislative Research, **"The Criminal Procedure (Identification) Bill, 2022",** Legislative Brief (2022).

ISSN: 2582-6433

up legitimate State objectives, the manner adopted under the Act fails to satisfy the requirements of minimal intrusion and narrow tailoring. The absence of robust procedural safeguards, independent oversight, data minimisation norms, purpose limitation, and effective remedies against abuse erodes the constitutional balance between individual liberty and collective security.[6] By placing the Act within comparative international practices and Indian constitutional doctrine, the paper ultimately questions whether the Criminal Procedure (Identification) Act, 2023 represents a shift from investigatory necessity to preventive surveillance, thereby threatening the core values of dignity, autonomy, and personal liberty under Article 21 of the Constitution.

RESEARCH QUESTIONS

Primary Research Question

1. Whether the Criminal Procedure (Identification) Act, 2023 and Section 349 BNSS infringes the fundamental right to privacy under Article 21 of the Constitution by permitting excessive, intrusive, and long-term collection and retention of personal data?

Secondary Research Questions

2. What is the scope and nature of "measurements" permitted under the Criminal Procedure (Identification) Act, 2023, and how does it differ from the colonial framework under the Identification of Prisoners Act, 1920?
3. Whether the powers conferred upon the police and prison authorities under the Act and Section 349[7] BNSS suffer from arbitrariness due to the absence of clear standards, judicial oversight, and procedural safeguards?
4. To what extent does the compulsory collection of biometric and biological data establish a reasonable nexus with the stated objectives of criminal investigation and prevention?
5. Whether the retention of measurements for seventy-five years by the NCRB satisfies the constitutional requisite of proportionality, necessity, and data minimisation?
6. How does the Act address concerns of misuse, data breaches, and secondary use of personal data in the absence of a comprehensive data protection apparatus?

[6] National Crime Records Bureau, Ministry of Home Affairs, Government of India (statutory role under CPI Act, 2022).
[7] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s. 349 (corresponding to s. 311A CrPC).

ISSN: 2582-6433

7. Whether individuals who are acquitted, discharged, or not formally charged have adequate legal reliefs for deletion or destruction of their data?
8. How does Indian jurisprudence on bodily integrity, self-incrimination, and privacy (Articles 20(3) and 21) interact with compulsory identification measures?
9. Whether the Criminal Procedure (Identification) Act, 2023 represents a paradigm shift from evidence-based investigation to preventive surveillance, and what are its long-term ramifications for civil liberties in India?

INTRODUCTION

The Criminal Procedure (Identification) Act, 2022[8] authorises law-enforcement agencies to collect a wide range of identifiable and biometric information from individuals for the purpose of criminal investigation. The Act repealed the colonial-era Identification of Prisoners Act, 1920 and substantially broadened both the class of persons from whom such data may be obtained and the nature of information that may be collected. The constitutional validity of the Act has been questioned, and multiple petitions challenging its provisions are presently pending before the Delhi High Court and the Madras High Court.

In furtherance of the statutory framework, the Central Government notified the Criminal Procedure (Identification) Rules[9], 2022 in September 2022. These Rules lay down the procedural safeguards and modalities governing the collection, storage, preservation, sharing, and destruction of records containing such identifiable information. Together, the Act and the Rules mark a significant shift in India's criminal justice and investigative architecture, raising concerns relating to privacy, proportionality, and data protection.

The relevance of this legislative development has been further reinforced by the enactment of the **Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). Section 349**[10] **of the BNSS** vests Magistrates with sweeping authority to direct any person to provide measurements or other identifiable information for the purposes of investigation or proceedings under the Code. When read alongside the Criminal Procedure (Identification) Act, 2022, this provision effectively consolidates and amplifies the State's power to compel the extraction of personal data, raising

[8] Ministry of Home Affairs, *The Criminal Procedure (Identification) Act, 2022* (Act No. 11 of 2022), Gazette of India, Extraordinary, Part II, Section 1.
[9] Ministry of Home Affairs, *The Criminal Procedure (Identification) Rules, 2022*, Gazette of India, Extraordinary (September 2022).
[10] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s. 349 (corresponding to s. 311A CrPC).

ISSN: 2582-6433

serious concerns regarding judicial discretion, absence of express limitations, and the adequacy of safeguards against abuse.

This research paper analyses the evolving statutory framework governing the collection of identification of data in India, analysing the Criminal Procedure (Identification) Act, 2022 and the Criminal Procedure (Identification) Rules, 2022 in conjunction with Section 349 of the BNSS, 2023. It seeks to evaluate the ramifications of these provisions on fundamental rights, particularly the right to privacy and personal liberty, and to assess whether the current legal framework strikes an appropriate balance between investigative efficiency and constitutional protections.

KEY FEATURES

The enactment of the **Criminal Procedure (Identification) Act, 2022** represents a decisive departure from the limited and custodial framework of the **Identification of Prisoners Act, 1920**, reflecting the State's increasing reliance on scientific and technological tools for criminal investigation. The 2022 Act considerably expands both the **scope of persons** subject to compulsory identification and the **range of data** that may be collected, thereby recalibrating the balance between investigative necessity and individual autonomy.

A central provision of the Act is **Section 2(b)**[11]**,** which mandates the taking of "measurements" from specified categories of individuals. The statutory definition of "measurements" under the Act is extraordinarily broad and technologically expansive. It includes **finger impressions, palm-print impressions, foot-print impressions, photographs, iris and retina scans**, as well as **physical and biological samples and their analysis**. Significantly, it also encompasses **behavioural attributes**, such as signatures and handwriting, and extends further to cover **any examination referred to under Sections 53**[12] **and 53A of the Code of Criminal Procedure, 1973**.

The inclusion of **biological samples** within the ambit of mandatory measurements has far-reaching implications. Bodily samples are not limited to superficial identifiers but potentially extend to **blood, saliva, semen, hair, DNA profiles, and other bodily fluids**, all of which carry deeply personal and sensitive information. This expansion is strengthened by **Section 53**

[11] *Criminal Procedure (Identification) Act, 2022*, s. 2(b).
[12] *Code of Criminal Procedure, 1973*, ss. 53 & 53A.

ISSN: 2582-6433

of the CrPC, which authorises a police officer to request a registered medical practitioner to conduct a medical examination of an arrested person where such examination may afford evidence of the commission of an offence. Judicial interpretation of Section 53 has already recognised the permissibility of extracting **blood samples and DNA** for investigative purposes, thereby providing a statutory bridge between criminal procedure and forensic science.

More debatable, however, is the Act's inclusion of **"behavioural attributes"**[13]**,** a term that remains **undefined** within the statute. The absence of a precise legislative definition introduces significant loopholes and opens the door to expansive executive interpretation. In the absence of express exclusions, this undefined category arguably brings within its ambit **forensic psychological and neuroscientific techniques,** such as **narco-analysis, brain mapping, and polygraph examinations**. Although the Supreme Court in *Selvi v. State of Karnataka* (2010)[14] held the involuntary administration of such techniques to be unconstitutional[15], the breadth of the statutory language under the 2022 Act raises serious concerns about indirect legitimisation through subordinate legislation or investigative practice.

These concerns are further enlarged when the Criminal Procedure (Identification) Act, 2022 is read alongside **Section 349 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS).** Section 349 empowers a Magistrate to direct any person to provide measurements or identifiable information for the purposes of investigation or proceedings, without prescribing clear substantive or procedural limitations. The combined operation of Section 2(b) of the 2022 Act and Section 349 of the BNSS effectively vests **wide and potentially untrammelled discretion** in both the executive and the judiciary, raising questions about proportionality, necessity, and the sufficiency of safeguards against misuse.[16]

The notification of the **Criminal Procedure (Identification) Rules, 2022** has further operationalised this framework by prescribing the procedures for collection, storage, sharing, and retention of such data. However, concerns continue to exist regarding **data retention periods, oversight mechanisms, informed consent, and destruction of records**, especially in cases of acquittal or discharge. In light of India's evolving privacy jurisprudence post *Justice*

[13] Supreme Court of India, interpretation of "testimonial compulsion" under Article 20(3).
[14] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[15] *Nandini Satpathy v. P.L. Dani*, (1978) 2 SCC 424.
[16] Law Commission of India, **185th Report on Review of Criminal Justice System** (relevant discussion on scientific investigation).

ISSN: 2582-6433

K.S. Puttaswamy v. Union of India, the expanded identification regime warrants careful constitutional evaluation.

TAKING OF MEASUREMENTS UNDER THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

Section 3[17] of the Criminal Procedure (Identification) Act, 2022 constitutes the substantive provision authorising the compulsory taking of measurements from a wide category of individuals. Under this provision, the obligation to provide measurements extends not only to convicted persons, but also to arrested individuals and persons detained under preventive detention laws. The scope of the provision is further expanded to include persons directed to furnish security for good behaviour or maintenance of public peace under Section 117 read with Sections 107–110 of the Code of Criminal Procedure, 1973[18]. The inclusion of such pre-emptive and preventive categories where guilt has neither been established nor even formally alleged in many cases marks a substantial departure from traditional criminal procedural safeguards.[19]

While the proviso to Section 3 provides limited protection by exempting persons arrested for minor offences from compulsory extraction of biological samples, this exemption is narrowly framed and expressly excludes offences against women or children and offences punishable with imprisonment of seven years or more. As a result, the exception does little to mitigate the overarching breadth of the provision, particularly in light of the expansive definition of "measurements" under the Act.

The Criminal Procedure (Identification) Rules, 2022 bring forth a conditional safeguard by providing that, in certain cases, measurements shall not be taken unless the individual has been formally charged or arrested in connection with another offence. However, these safeguards are regulatory in nature and remain subordinate to the wide enabling power conferred by the parent statute. Their efficacy is therefore contingent upon executive discretion rather than enforceable statutory limitations.

[17] *Criminal Procedure (Identification) Act, 2022*, s. 3.
[18] *Code of Criminal Procedure, 1973*, ss. 107–110 & s. 117.
[19] *Joginder Kumar v. State of U.P.*, (1994) 4 SCC 260.

ISSN: 2582-6433

PERSONS AUTHORISED TO TAKE MEASUREMENTS

The Act authorises police officers and prison officers to take measurements. The Rules further widen this category by permitting an authorised user, any person skilled in taking such measurements, a registered medical practitioner, or any other person authorised for this purpose to collect the data. An "authorised user" is defined as a police or prison officer granted access by the National Crime Records Bureau (NCRB) to the centralised database of measurements. This decentralised authorisation structure, coupled with the absence of clear accountability mechanisms, broadens the risk of misuse and arbitrary application.

COMPULSION, USE OF FORCE, AND CRIMINALISATION OF RESISTANCE

The coercive character of the statutory framework becomes apparent when Sections 5 and 6[20] of the Act are read together. Section 5 mandates that the person to whom an order relates "shall allow" the measurements to be taken in accordance with the prescribed directions. Section 6 goes a step further by authorising the use of lawful force where an individual resists or refuses to comply. More significantly, Section 6(2) criminalises such resistance by making it an offence under Section 221 of the Bharatiya Nyaya Sanhita, 2023[21].

This combination of compulsory compliance, authorised use of force, and penal consequences for resistance raises grave constitutional concerns[22]. The framework effectively leaves individuals with no meaningful choice, thereby undermining the principle of voluntary consent and eroding the protection of bodily autonomy and personal liberty guaranteed under Article 21 of the Constitution[23].

CONSTITUTIONAL CONCERNS: ARBITRARINESS, PROPORTIONALITY, AND NEXUS

The statutory scheme suffers from a palpable lack of proportionality and reasonable nexus between the means employed and the objectives sought to be achieved. While the stated aim of the Act is to ease accurate identification and efficient investigation, the indiscriminate inclusion of arrested persons, preventive detainees, and individuals involved in peace-bond

[20] *Criminal Procedure (Identification) Act, 2022*, ss. 5 & 6.
[21] *Bharatiya Nyaya Sanhita, 2023*, s. 221.
[22] *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 SCC 608.
[23] *Sunil Batra v. Delhi Administration*, (1978) 4 SCC 494.

ISSN: 2582-6433

proceedings reflects an overbroad and undifferentiated approach. The absence of offence-specific thresholds, judicial oversight at the stage of collection, and clear exclusions for intrusive techniques renders the law at risk to challenge on grounds of manifest arbitrariness under Article 14.[24]

In Justice *K.S. Puttaswamy v. Union of India (2017)*[25], the Supreme Court held that any infringement of the right to privacy must satisfy the test of legality, legitimate aim, necessity, and proportionality. The wide ranging powers under Sections 3, 5, and 6 of the 2022 Act raise serious doubts as to whether the requirement of least restrictive means is met. Similarly, in *Selvi v. State of Karnataka (2010*)[26], the Court categorically held that involuntary administration of techniques such as narco-analysis, polygraph tests, and brain mapping violates personal liberty and the privilege against self-incrimination. The undefined and elastic nature of "measurements" under the Act risks indirectly bypassing this constitutional protection.[27]

Earlier, in *State of Bombay v. Kathi Kalu Oghad (1962)*[28], the Supreme Court differentiated physical evidence from testimonial compulsion. However, the contemporary expansion of measurements to include biological and behavioural data capable of revealing intimate personal information blurs this distinction and necessitates a re-examination of earlier jurisprudence in light of modern privacy standards.

COLLECTION, STORAGE, AND RETENTION OF MEASUREMENT RECORDS: ROLE OF THE NCRB

Section 4 of the Criminal Procedure (Identification) Act, 2022[29] endows the National Crime Records Bureau (NCRB) with extensive and centralised authority over the collection, processing, storage, dissemination, and destruction of records of measurements.[30] Sub-section (1) mandates the NCRB, in the interests of prevention, detection, investigation, and prosecution of offences, to collect such records from State Governments, Union Territory Administrations, and other law-enforcement agencies, to store and preserve them at the national level, to process the data alongside relevant crime and criminal records, and to share and disseminate the

[24] *Modern Dental College v. State of Madhya Pradesh*, (2016) 7 SCC 353.
[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (four-fold proportionality test).
[26] *Selvi v. State of Karnataka*, (2010) 7 SCC 263, ¶¶ 200–225.
[27] PRS Legislative Research, **"Key Issues and Analysis: Criminal Procedure (Identification) Bill, 2022"**.
[28] *State of Bombay v. Kathi Kalu Oghad*, AIR 1961 SC 1808.
[29] *Criminal Procedure (Identification) Act, 2022*, s. 4.
[30] Ministry of Home Affairs, Functions of NCRB (official mandate).

ISSN: 2582-6433

information with any law-enforcement agency, in a manner to be prescribed.

This provision effectively creates a centralised national repository of sensitive personal data, embodying biometric, biological, and behavioural information of a vast segment of the population, including individuals who may never be convicted of any offence. The breadth of the data flows authorised under Section 4 particularly the power to share records with "any law enforcement agency" without explicit statutory safeguards raises grave concerns regarding purpose limitation, access control, and oversight.[31]

RETENTION PERIOD AND THE QUESTION OF PROPORTIONALITY

Section 4(2) provides that records of measurements may be retained in digital or electronic form for a period of seventy-five years from the date of collection. Such an extended retention period is extraordinary by any comparative standard and the same has profound implications for the right to privacy and informational self-determination. While the proviso requires destruction of records in cases where a person without prior conviction is released without trial, discharged, or acquitted subject to exhaustion of legal remedies, this safeguard is diluted by the discretionary power vested in courts and Magistrates to direct otherwise for reasons to be recorded in writing.

The statutory design thus normalises long-term surveillance by default, making deletion the exception rather than the rule. The absence of offence-based differentiation, periodic review mechanisms, or mandatory data minimisation principles renders the retention framework vulnerable to challenge on grounds of disproportionality.

PRIVACY AND DATA SECURITY CONCERNS

The Act is strikingly silent on specific technical and organisational safeguards to prevent unauthorised access, data breaches, profiling, or misuse of the stored information. Given the nature of the data involved-biometric identifiers, biological samples, and behavioural attributes, the risks associated with data compromise are exceptionally high. Unlike passwords or identification numbers, biometric and biological data are immutable, and any neglect may result in permanent harm, including identity theft, surveillance, and profiling.

[31] PRS Legislative Research, **"Data Retention and Privacy Concerns under CPI Act"**.

ISSN: 2582-6433

In Justice *K.S. Puttaswamy v. Union of India (2017)*[32], the Supreme Court recognised informational privacy as an inherent facet of Article 21 and held that any State action involving collection and retention of personal data must satisfy the tests of legality, legitimate aim, proportionality, and procedural safeguards against abuse. The indefinite-like retention period of seventy-five years, coupled with vague data-sharing provisions, raises serious concerns as to whether these constitutional thresholds are met.

Further, in *Anuradha Bhasin v. Union of India (2020)*[33], the Court emphasised the necessity of procedural safeguards and periodic review when fundamental rights are curtailed. The absence of statutory review mechanisms under Section 4 undermines this requirement.

INTERFACE WITH THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023[34]

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) introduces a panoramic framework governing the processing of digital personal data, anchored in principles such as lawful purpose, data minimisation, storage limitation, and security safeguards. While the DPDP Act provides exemptions for processing of personal data by the State for purposes of law enforcement and public order, such exemptions are not absolute and are intended to operate subject to necessity and proportionality.

The Criminal Procedure (Identification) Act, 2022, however, neither expressly incorporates DPDP standards nor provides an internal mechanism to ensure compliance with data protection principles. The seventy-five-year retention rule appears strenuous to reconcile with the DPDP Act's emphasis on retention only for as long as necessary to fulfil the stated purpose. This normative dissonance risks creating a parallel data regime in which sensitive personal data collected for criminal justice purposes remains largely covered from contemporary data protection safeguards.[35]

[32] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (informational privacy).
[33] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[34] *Digital Personal Data Protection Act, 2023*.
[35] Justice B.N. Srikrishna Committee Report on Data Protection (2018).

ISSN: 2582-6433

INTERFACE BETWEEN THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022 AND SECTION 349 OF THE BNSS, 2023

The **Criminal Procedure (Identification) Act, 2022** and **Section 349 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)** operate together to significantly widen the State's power to collect personal and sensitive information from individuals involved in the criminal justice process. When read in isolation, each provision appears to serve a procedural or investigative purpose. However, when read together, they create a structure that confers **wide and largely unregulated discretion** on the State.

The Criminal Procedure (Identification) Act permits the compulsory collection, storage, and long-term retention of "measurements," a term that includes biometric, biological, and behavioural data. The Act applies not only to convicted persons, but also to arrested individuals, preventive detainees, and even persons against whom no formal charge has been proved. It further allows the use of force to obtain such data and criminalises resistance, while authorising retention of the collected data for up to **seventy-five years**.[36]

Section 349 of the BNSS strengthens and legitimises this framework by empowering a **Magistrate to order any person to provide measurements or identifiable information** for the purposes of investigation or legal proceedings. Crucially, this power is not accompanied by clear statutory limits, objective criteria, or mandatory safeguards. The provision does not require the Magistrate to judge the **necessity or proportionality** of the order, nor does it distinguish between minor and serious offences or between accused and non-accused persons. Together, these provisions create a situation where the **executive collects and stores sensitive personal data,** while the **judiciary authorises its extraction**, without either being subject to clearly defined restrictions. The absence of offence-specific thresholds, judicial review mechanisms, or express exclusions for intrusive techniques allows the State to exercise surveillance-oriented powers in a routine and normalised manner.

This combined operation raises serious constitutional concerns. It weakens the principle that constraints on personal liberty and privacy must have a **reasonable nexus with the objective sought to be achieved.** Instead of adopting a targeted and need-based approach, the legal

[36] Law Commission of India, **277th Report on Wrongful Prosecution (Miscarriage of Justice)**.

ISSN: 2582-6433

framework authorises broad and standardised data collection, even where the investigative value of such information is minimal.[37]

In effect, the Criminal Procedure (Identification) Act, 2022 provides the **significant power to collect and retain personal data**, while Section 349 of the BNSS supplies the **procedural authority to compel compliance.** The lack of meaningful safeguards at either stage results in a concentration of power that risks arbitrariness and undermines the constitutional guarantees of privacy, dignity, and personal autonomy.

INTERACTION OF COMPULSORY IDENTIFICATION MEASURES WITH ARTICLES 20(3) AND 21[38]

Indian constitutional jurisprudence has consistently attempted to balance the State's interest in criminal investigation with the individual's rights to bodily integrity, protection against self-incrimination (Article 20(3)), and personal liberty and privacy (Article 21). Compulsory identification measures lie at the interplay of these competing interests.

Under Article 20(3), the Supreme Court in *State of Bombay v. Kathi Kalu Oghad (1962)*[39] held that the prohibition against self-incrimination applies only to testimonial compulsion and not to the collection of physical evidence such as fingerprints, handwriting, or footprints. This judgment provided early constitutional legitimacy to compulsory identification techniques. However, the Court's reasoning was based on the limited and non-intrusive nature of identification methods prevalent at the time.

The scope of this rational was revisited in *Selvi v. State of Karnataka (2010)*[40], where the Court distinguished between mere physical identification and techniques that intrude into the mental privacy of an individual. The involuntary administration of narco-analysis, polygraph, and brain-mapping tests was held to violate Articles 20(3) and 21, as such techniques compel a person to disclose personal information and thoughts. This judgment underscored that not all forms of scientific evidence collection are constitutionally permissible.

With respect to Article 21, the Court has progressively recognised bodily integrity and

[37] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press).
[38] *Constitution of India, 1950,* art. 20 & 21
[40] *Selvi v. State of Karnataka*, (2010) 7 SCC 263, ¶¶ 200–225.

ISSN: 2582-6433

privacy as essential parts of personal liberty. In *Maneka Gandhi v. Union of India (1978*)[41], the Court established that any procedure affecting personal liberty must be just, fair, and reasonable. This standard applies equally to modern and latest identification measures involving bodily and biological data.

Further, in ***Ritesh Sinha v. State of Uttar Pradesh (2019)***[42]**,** the Court permitted compulsory voice samples for investigation, but emphasised the need for **legal backing and procedural safeguards,** reflecting judicial caution against unrestrained investigative powers.

Although The Criminal Procedure (Identification) Act, 2022 does **not of itself violate Article 20(3)** as long as it is confined to non-testimonial physical evidence. However, its **open-ended scope** and interaction with behavioural and biological data raise serious concerns under **Article 21**, particularly in relation to bodily integrity, privacy, and proportionality. The constitutional validity of the Act will ultimately depend on how narrowly courts interpret its provisions and whether adequate procedural safeguards are read into its operation.

COMPARATIVE CONSTITUTIONAL AND INTERNATIONAL HUMAN RIGHTS PERSPECTIVES ON BIOMETRIC DATA COLLECTION

Comparative constitutional jurisprudence and international human rights standards treat **biometric and biological data** as **highly sensitive personal information**, requiring enhanced statutory protection when used in criminal justice systems. A consistent theme across jurisdictions is the emphasis on **necessity, proportionality, purpose limitation, and independent oversight** and monitoring.

In the **European Union**, biometric data is classified as *"special category data"* under the **General Data Protection Regulation (GDPR)**[43]**.** Its processing for law-enforcement purposes is authorised only where it is **strictly necessary,** supported by clear legal authority, and accompanied by strong safeguards, including limited retention periods and independent supervisory oversight. The **European Court of Human Rights (ECtHR)** in *S. and Marper v. United Kingdom* (2008)[44] held that the indefinite retention of fingerprints and DNA profiles of

[41] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[42] *Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1.
[43] General Data Protection Regulation (EU) 2016/679, Art. 9.
[44] *S. and Marper v. United Kingdom*, (2008) 48 EHRR 50.

ISSN: 2582-6433

unconvicted persons infringes the right to privacy under Article 8 of the European Convention on Human Rights.

In the **United Kingdom**, police powers to collect biometric data are regulated under the **Police and Criminal Evidence Act (PACE)** and subsequent legislation, which prescribe offence-based thresholds, judicial or independent authorisation, and mandatory destruction of data for persons not convicted, subject to narrow and limited exceptions. This framework reflects a rights-sensitive approach that balances crime control with individual liberty.

At the international level, instruments such as the **International Covenant on Civil and Political Rights (ICCPR)**[45] and the **UN Human Rights Committee's General Comments** recognise privacy as a fundamental right and caution against arbitrary or disproportionate data collection and its retention.[46] These standards stress that biometric databases must not result in blanket surveillance or discriminatory practices.

LONG-TERM IMPLICATIONS OF THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022 ON CIVIL LIBERTIES IN INDIA

The Criminal Procedure (Identification) Act, 2022 has the potential to significantly reshape the relationship between the State and the individual in India's criminal justice system. While the objective of improving investigation and identification is legitimate, the manner and mode in which the Act expands State's power raises serious long-term concerns for civil liberties.

1. **Normalisation of Surveillance**

   The Act institutionalises large-scale collection and long-term retention of biometric and biological data, including from individuals who are arrested, detained preventively, or never convicted. Over time, this may lead to the normalisation of surveillance and monitoring, where intrusive and personal data collection becomes a routine aspect of law enforcement rather than an exceptional measure justified by necessity.

2. **Erosion of the Presumption of Innocence**

   By authorising the collection and storage of sensitive personal data from non-convicted persons, the Act undermines the foundational criminal law principle of presumption of innocence. Individuals acquitted or discharged may continue to remain under digital

[45] *International Covenant on Civil and Political Rights*, Art. 17.
[46] UN Human Rights Committee, **General Comment No. 16**.

ISSN: 2582-6433

suspicion due to prolonged retention of their data.

3. **Chilling Effect on Personal Liberty and Dissent**

   The fear of long-term data retention and potential misuse may prevent individuals from exercising fundamental freedoms such as movement, association, and expression, particularly in politically sensitive contexts. Preventive detainees and persons involved in public order proceedings are especially vulnerable.

4. **Risk of Discrimination and Profiling**

   Centralised biometric databases can facilitate profiling of marginalised communities, leading to selective surveillance and discriminatory policing. In the absence of transparency and oversight, algorithmic or manual misuse or abuse of data may reinforce existing social biases.

5. **Weakening of Privacy Jurisprudence**

   If upheld without strict safeguards, the Act weakens the constitutional standards laid down in *Puttaswamy*, potentially creating a precedent where statutory authorisation alone is treated as sufficient to override privacy concerns.

SUGGESTED SOLUTIONS TO ADDRESS PRIVACY AND CIVIL LIBERTIES CONCERNS

1. **Narrowing the Scope of Persons and Data Collected**

   The Act should be amended to limit compulsory collection of biometric and biological data to grave and serious offences and convicted persons, with clear exclusion of minor offences and preventive detention cases. Behavioural and psychological examinations should be expressly excluded.

2. **Introducing Offence-Based and Necessity Tests**

   Mandatory application of a necessity and proportionality test before collecting sensitive data, with written reasons, would align the Act with Article 21 standards. Magistrates under Section 349 BNSS should be required to record detailed reasons as a legal mandate.

3. **Reducing Data Retention Periods**

   The seventy-five-year retention period should be replaced with graduated, offence-based retention limits, with automatic deletion upon acquittal, discharge, or lapse of a defined period.

ISSN: 2582-6433

4. **Strengthening Judicial and Independent Oversight**
   An independent oversight authority, possibly linked to the Data Protection Board under the Digital Personal Data Protection Act, 2023, should be formed to supervise access, sharing, and retention of biometric data.
5. **Clear Data Security and Accountability Standards**
   The law must prescribe mandatory cybersecurity framework, audit mechanisms, and penalties for data breaches or unauthorised access. Regular security audits of NCRB databases should be compulsory.
6. **Explicit Alignment with the Data Protection Act, 2023**
   The Criminal Procedure (Identification) Act should expressly incorporate principles of data minimisation, purpose limitation, and storage limitation from the DPDP Act, ensuring that law enforcement exemptions are narrowly interpreted.
7. **Right to Notice and Effective Remedies**
   Individuals should have a legal right to be informed when their data is collected, retained, shared, or destroyed, along with a clear and time-bound mechanism to seek deletion and compensation for misuse.

CONCLUSION

The Criminal Procedure (Identification) Act, 2022 represents a transformative moment in India's criminal justice system, marking a clear shift from traditional, offence-specific methods of identification to a data-intensive and technology-driven framework of policing. By replacing the colonial Identification of Prisoners Act, 1920, the legislation highlights the State's attempt to modernise investigative practices in response to evolving forms of crime. However, this modernisation has come at the cost of significantly expanding State power over the bodies, identities, and personal data of individuals, often without proportionate safeguards.

At the core of the Act lies an exceptionally broad concept of "measurements", extending beyond conventional physical identifiers to include biometric, biological, and behavioural data. This expansion blurs the classical distinction between physical evidence and deeply personal information capable of revealing intimate personal details about an individual's body, health, and behaviour. When applied not only to convicted persons but also to arrestees, preventive detainees, and individuals involved in peace-bond proceedings, the framework undermines the presumption of innocence and normalises intrusive data collection at preliminary stages of the criminal process.

ISSN: 2582-6433

The coercive nature of the statutory scheme is further accentuated by the combined operation of Sections 3, 5, and 6 of the Act and Section 349 of the Bharatiya Nagarik Suraksha Sanhita, 2023. Together, these provisions vest wide ranging discretion in police officers, prison authorities, and Magistrates to compel the extraction of measurements, authorise the use of force, and criminalise resistance. The absence of clearly articulated standards governing necessity, proportionality, and offence severity creates fertile ground for state arbitrariness, raising serious concerns under Articles 14 and 21 of the Constitution.

From a constitutional perspective, while the Act may not per se violate Article 20(3) insofar as it permits the collection of non-testimonial physical evidence, its open-ended language particularly with respect to behavioural attributes risks indirectly undermining the safeguards laid down in *Selvi v. State of Karnataka*. More critically, the Act's compatibility with Article 21 remains deeply contested. Post-*Puttaswamy*, bodily integrity and informational privacy are recognised as intrinsic to personal liberty, and any violation must satisfy the rigorous tests of legality, legitimate aim, necessity, proportionality, and procedural safeguards. The Act's indiscriminate application, prolonged data retention, and weak oversight mechanisms make it difficult to conclude that these constitutional thresholds are adequately met.

The role of the National Crime Records Bureau under Section 4 further amplifies these concerns. The creation of a centralised national repository with the authority to retain sensitive personal data for up to seventy-five years reflects a surveillance-oriented approach rather than a narrowly tailored investigatory tool. Comparative constitutional and international human rights standards, particularly from the European Union and the jurisprudence of the European Court of Human Rights, demonstrate that such continued retention, especially of data belonging to non-convicted persons is incompatible with modern privacy norms. In this light, India's framework appears out of step with global best practices.

The enactment of the Digital Personal Data Protection Act, 2023 offers a potential corrective, but the absence of explicit harmonisation between the two statutes risks creating a parallel regime in which law enforcement data remains insulated from meaningful data protection principles. Without express incorporation of data minimisation, purpose limitation, independent oversight, and effective remedies, the privacy guarantees recognised in constitutional jurisprudence remain largely theoretical.

ISSN: 2582-6433

In its present form, the Criminal Procedure (Identification) Act, 2022 signals a paradigm shift from evidence-based investigation to preventive and predictive surveillance. If left unchecked and without any constraints, this shift may have enduring consequences for civil liberties in India, including erosion of privacy, expansion of executive discretion, and gradual dilution of constitutional restraints on State power. The true test of the Act's constitutionality will therefore lie not merely in its stated objectives, but in how narrowly its provisions are interpreted, how robustly safeguards are implemented, and whether legislative and judicial institutions remain committed to preserving the delicate balance between collective security and individual freedom.

Ultimately, while the pursuit of effective criminal justice is both legitimate and necessary, it cannot be allowed to override the foundational constitutional values of dignity, autonomy, and liberty. A recalibrated framework anchored in proportionality, transparency, and accountability is essential to ensure that the march toward technological modernisation does not culminate in the erosion of the very rights the Constitution seeks to protect.