International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 10-11-2025, Accepted: 09-01-2026, Published: 24-01-2026
Volume 12, Issue 1, 2026, Page No. 171-175

Identify the problem: Issues with the Criminal Identification Act 2022, with special reference to right to be forgotten, and ai surveillance technologies

Kumar Ankit[1], Aman Singh[2]
[1] Assistant Professor of Law, Ramaiah College of Law, Bengaluru, Karnataka, India
[2] Research Scholar, Faculty of Laws, Banaras Hindu University, Varanasi, Uttar Pradesh, India

Abstract
The new Criminal Procedure Identification Act 2022, widened the scope of data that had earlier been collected under the Identification of Prisoners Act 1920. This act further authorises the collection and storage of biological samples and behavioural attributes of arrested, under-trial, or any other person for 75 years. This act is alleged to violate the right to be forgotten embedded in the right to privacy. Moreover, there is no data protection law in India, and thus the data collected by the agencies may be misused in the absence of such a law. Furthermore, there is no specific agency in India for collecting and storing data. In addition to it, the data collected under this act may in the future be fed into AI for the profiling of criminals. The use of AI for the purpose of profiling has several discrepancies while generating the outcomes and thus infringes on several basic rights. This paper deals with the problems in implementing the Criminal Procedure Identification Act 2022 and suggests a way forward.

Keywords: Right to be forgotten, identification, privacy, AI, profiling, data, surveillance

Introduction

The new Criminal Procedure Identification Act 2022 has been introduced for the collection of data, including biological samples and behavioural attributes, of arrested, under-trial, or any other person (with the permission of a magistrate) for 75 years. A person not below the rank of head warden has been authorized to collect the data. The new act has replaced the old "Identification of Prisoners Act, 1920, and has widened the scope of data collected. The National Crime Records Bureau has been empowered to collect, store, and destroy the data.

With the advancement in technologies, forensic evidence has become more advanced, giving rise to the need for the collection of biological data to make the investigation procedure smooth. But with the collection, storage, and use of such data, the privacy concern has been triggered in the absence of data protection and privacy legislation, as there is a risk of such data being misused without providing any remedy to the person whose data is being collected.

As per the Criminal Procedure Identification Act 2022, such data may be used for investigative purposes, which may lead to the use of AI in the future for predicting offenders and profiling people more likely to commit such offences. AI is based on machine learning, and there is a lack of human intervention in the outcome provided by AI, making it prone to giving biased and discriminatory results. Further chapters would deal with the problems of implementing the act and using the data to feed the AI.

Privacy Concerns Regarding The New Criminal Procedure (Identification) Act, 2022 With Special Reference To The Right To Be Forgotten, And Ai Surveillance Technologies

The new Criminal Procedure (Identification) Act (hereinafter the Act) replaces the previous Identification of Prisoners' Act 1920, moving towards the modernization of forensics and diversifying the scope of data collection, preservation, and processing. While posed to be developmental in nature by including newer and more accurate technology for measurements and records, there are several issues, from constitutional validity to incompatibility with international covenants to which India is a signatory. However, in this chapter, we focus on the blatant procedural and privacy issues that have surfaced from the act and how it goes against the right to be forgotten, intrinsic to the fundamental right to life as well as the right to life itself.

What Is Right To Be Forgotten?

The jurisprudential origin of the Right to Be Forgotten can be traced back to the 2014 CJEU judgement [1], which became the origin of the whole spectrum of online privacy and data protection and paved the way for the 2016 GDPR guidelines and data protection becoming a fundamental right under the European Convention on Human Rights.

It establishes that any data that has been collected from an individual (a data subject) should be removed once the purpose for which it was collected is served, hence the term "forgotten" [2], like when the sentence has been completely served or the accused has been acquitted, as well as instances wherein the dignity of the victims is to be safeguarded, such as cases of rape or sexual abuse of children. The key here is to give due respect to the individual's privacy and grant them autonomy over their data that is accessed, collected, and processed by someone else, for these days human beings live two lives: one in the world and another online. And the internet does not forget, and it does not let humans forget [3].

In India, the concept of the "right to be forgotten" is not in the form of a statutory provision but rather a development of judicial jurisprudence recognised in the landmark case of K. S. Puttasswamy v. UOI [4]. It has been revered as an intrinsic aspect of the Right to Life, wherein the term "life" means more than mere bodily existence but also to live with dignity. The apex court has said that it is one of the most

basic human rights, so fundamental that even the government has no authority to violate it, even if the individual in question is subjected to incarceration.

How Does The Act Violate The Right To Be Forgotten?

The Act blatantly violates the above-mentioned principles and goes against the tenet of innocence until proven guilty. It defines "measurements" under Section 2(1)(b) consisting of various elements from finger, palm, and foot impressions to signatures and even behavioural patterns, and the very vaguely listed and most problematic "physical and biological samples," which not only brings in an aspect of the potential use of implicit force in the collection or processing of the data but is also in violation of the right to self-incrimination.

All this data is to be stored for 75 years, irrespective of the individual's acquittal or concluded sentence, as per Section 4(2) [5], and thus jeopardises the privacy of the individual. Moreover, the fact that all this data is to be collected from such a wide array of people (accused, under-trials, etc.) and with the least possible authorization makes it draconian, apart from being unconstitutional.

There is no differentiation between necessary and unnecessary data and no stratification when it comes to the levels of data sensitivity, which leaves the scope of data collection very open-ended. There is also no provision to keep a check on the way the data is processed after it is collected because we have no data protection act in India as of now, and even if we did, there would need to be changes made in the prospective data protection law to also include the post collection processing of the collected data and make it challengeable and maintain the claim of the aggrieved individual to get the discrepancy allied because on perusal of section 10 [6] (Indian Data Protection Bill, 2022) of the Indian data protection bill, we see that any maintainable challenge and/or removal of the collected data is based on its lawful "collection" only and is silent on its post - collection processing which has the most potential for misuse and can be violative of the individual's privacy.

There is inherent vagueness imbibed in this legislation, for example, in Section 5 [7] (The Criminal Procedure (Identification) Act, 2022), which allows the magistrate to authorise the taking of measurements from "any" individual, someone who is not even a suspect in the instant investigation. The collection of DNA samples gives way to further profiling and can give away even more sensitive information, such as one's medical statistics or data about relatives completely uninvolved in the investigation, without getting them involved. In the judgement in K.S. Puttaswamy v. UOI [8], the principles of GDPR were propounded as useful guidance with context for the Indian legal framework. Although the Indian data protection bill has attempted to incorporate the said principles, it is still in the pipeline, has no enforceability, and thus has no way to keep the methods of the act in check.

The Act is not in tune with the principle of limitation, or the "limitation test", a derivative of the GDPR, which emphasises the purposeful aspect of data collection [9]. The principle in essence promotes transparency, legal certainty, and predictability; however, there is no specific and legitimate purpose that has been made certain for the vast array of data collection that the Act authorises ("an officer in charge of a police station," "any officer not below the rank of head constable," and "prison officers not below the rank of head warder") [10] (Jasserand, 2018).

While the act is allegedly collected for the purpose of "criminal investigation", it has the ability to affect any individual and has no precise procedural legitimization or definition, with rampant usage of vague terminology and open-ended statements, as well as a violation of the "Storage Limitation Principle" provided in Article 5(1)(e) of the GDPR [11], which says that the personal data that is collected is to be stored for no longer than what is necessary for the fulfilment of the purpose for which it was to be processed. As per Section 4 of the NCRB Act, it has been authorised to collect and process the whole array of sensitive records made in pursuance of the Criminal Identification Act despite the infrastructural shortcomings, and that too for 75 years, irrespective of acquittal or completion of the sentence.

When we put together the process of collection, the lowered level of authorization, the variety of data to be collected, the gross disregard for the varied sensitivity various "measurements" have, the unnecessarily long time for which it is collected (and that too even if the person is acquitted), as well as from whom all the measurements can be taken, in tandem with lacking privacy protection statutes and a data protection bill stuck as a draught for years, as well as the glaring potential for misuse and violative practising, we have what one truly can call a "recipe for disaster."

Infrastructural And Feasibility Issues With The Criminal (Procedure) Identification Act, 2022

The Criminal Procedure (Activation) Act 2022 (the Act) diversifies the array of data collection, moves forward from the mere collection of signatures and photographs under the Identification of Prisoners Act 1920, and marks a move towards a modern forensic criminal justice system. While the ideal may be modernization and betterment of the criminal justice system in India, the proper implementation of the Act would require extensive infrastructural changes and legislative reforms because, although modernization and technological developments sound good on paper, there needs to be adequate guidelines and infrastructure so that enforcement is smooth, fruitful, and just. The NCRB of India has been given responsibility for the accrual and recording of the "measurements" as defined in the Act. The broadened scope of "measurements" to be recorded as mentioned in Section 2(1)(a) of the Act extends beyond the erstwhile purpose and functioning of the NCRB.

Capacitive Shortcomings Of The Ncrb: The Act has expanded the scope of measurement and data collection incorporating physical and biological samples along with any other crime-specific "examinations" as listed under Section 53 and Section 53-A [12]. The NCRB was not established with this purpose; it was made as a repository of criminal information that was collected under the previous prisoner's identification laws of 1920. However, there has not been adequate upgradation done in the NCRB to facilitate the new incorporations. Basically, the Act is ahead of its time, at least in India, lacking what we can call "future proofing."

The feasibility of such record maintenance would require a major revamp of the NCRB, considering the current capacitive limitations. The NCRB is archival in its purpose as well as functioning; it has no protocol for collection of the long list of measurements that the current Act authorises. Considering the limited infrastructure and capacity of the central as well as state forensic science labs

along with the wider scope of measurements that will have to be made now, as "anyone" can be made to submit measurements, we see the inherent lack in the qualifications of the NCRB for handling such diversity and quantity of data [13].

Moreover, all data that the NCRB is supposed to collect will be stored for 75 years. The capacitive shortcomings would not only cause privacy and security concerns regarding the very sensitive nature of the collected data, but also sub-par quality of the samples if they are not stored as per the required medical standards for proper preservation to avoid inaccuracies. The measurements that are to be collected shall aid various investigative processes where the margin for error has to be as low as possible. In the landmark judgement of Puttaswamy v. UOI, the Supreme Court has emphasised the 99.7% and not absolute accuracy of biometrics and has elucidated how even such a small margin of error becomes dangerous when affecting a big population. The collection of biological samples is at the core of the current Act, and thus the above-mentioned capacitive inadequacies can cause serious issues from inaccurate accusations and profiling.

Inadequacy Of Guidelines Concerning Collection, Preservation And Processing: Having the new Act at hand, India still lacks the proper guidelines for the lawful, proper, and just implementation of the gargantuan database to be formed. We have no definitive protocols pertaining to the consensual and secure handling of data, nor do we have any dedicated data protection authority that can keep a check on the authority responsible for the enforcement of the data and sample-related provisions, which in this case is the NCRB. We need an independent public body that can ensure lawfulness in the processing and preservation aspects of the collected data and keep a check on the concerned authority so that the citizens stay protected.

In various countries where extensive profiling and data collection and processing are done, there are dedicated and specialised independent bodies to ensure transparency and safeguard against any potential breach. The USA has the "Privacy Office of the Department of State" as well as the 1974 "U.S. Privacy Act'' [14] protecting individual privacy, as well as several state laws such as the "California Consumer Privacy Act" [15], the US equivalent of the EU's GDPR. The GDPR has extensive, comprehensive, and concrete stratification and differentiation when it comes to the levels of data sensitivity and the collections and processing therein. There is systemic categorization like "special data," wherein more attention and scrutiny are given to the safety provisions because of higher levels of sensitivity.

Not only do we lack definitive guidelines and an independent authority for keeping a check, but the Act is widely vague, which makes certain aspects open-ended and potent for abuse. There are no boundaries for the collection of data, and the autonomy of the individual are given little importance or consideration, if any. The Act compels any accused or under-trial person under "any law" to submit to the measurement procedure, violating the Supreme Court mandate against the "forcible conveyance of personal knowledge that is relevant to facts in the issue", and thus Article 20(3) [16] of the Constitution of India as well as Article 21 [17] (Justice K.S.Puttaswamy(Retd) vs Union Of India, 2017).

Indeed, the Act intends to modernise the forensic database, ideally making convictions more accurate. However, the Act seems to be ahead of the present infrastructural and capacitive limitations. While a revamp is very much due, it must be done right! Right by the law, right by the people, and, of course, right by the nation; a complete transformation with immediate effect makes headlines, but fixing smaller problems and pre-requisite preparation before bringing such legislation leads to better implementation and safer citizens.

Future Use Of Data Collected For Investigation With Reference To Ai

The Alan Turing Institute has defined AI as a model that works on algorithms performing functions that were earlier considered to be performed by human beings by applying their reasonable minds. Further, the European Union draft AI Act elaborates the definition under Section 3 stating that it is software based on machine learning working on logic, knowledge, and statistics fed into it that can be used to generate outputs like prediction, recommendation, or decision [18] (Dai & Ke, 2022).

AI improves its intelligence by self-induced machine learning, not by human rules. AI develops by using a huge database embedded with human bias, which is unforeseen sometimes [19]. The technologies pick up the prejudicial values and patterns prevalent in society as they are, without the influence of any moral compass, and purely mathematical algorithms dealing with raw data and statistics can actually showcase an increment of those very same discriminatory practices and inequalities existing in society when they yield results from the raw data they were fed, lacking socio-legal perspectives.

AI has been discussed on different levels since the early 1950s. However, with the progress in data analysis techniques and the availability of data, AI has transformed a lot in recent times. Despite gaining popularity, there is still no universal definition accepted; however, commonly, it is considered that AI focuses on "mimicking human thought" [20] and thus it has the capacity to do tasks falling within the capacity of human beings.

Use Of Ai In Criminal Justice System: Ai Has been frequently used in the present scenario not only for profiling people but also for profiling geographic areas to predict, firstly, the likelihood of the person recommitting the offence and, secondly, the areas where there are more chances of crime being committed. The use of AI for the above-mentioned purposes is classified as "high risk" under the EU's Draft AI Act. The use of AI for the above-mentioned purpose infringes on the basic rights of the individual, namely equality before the law, non-discrimination, etc.

The use of AI has been objected to by European Union members, especially for the purpose of the predictive policing system that is provided under Article 5 of the AI Act. Predictive policing uses AI to identify the person who is more likely to commit the offence and also to identify the areas where the offence is more likely to be committed. The use of AI for this purpose violates the principles of equality and the rule of law, which will be further discussed in this chapter ("AI Act," 2022) [21].

Hungary uses facial recognition technology for surveillance by collecting and storing data nationwide and naming it the 'Dragonfly Project'. The use of this technology is

problematic as it raises several ethical and legal issues. Moreover, Hungary and Poland used an app named "Home Quarantine App" during the pandemic to keep a check on people through facial recognition technology to ensure that they remained in quarantine for the necessary duration.

The Minister of Justice in Ireland, Helen McEntee, has granted numerous powers to Garda Siochana, allowing them to use facial recognition technology for identifying criminals. This technology would be fed into CCTV, which would identify criminals. The Irish Council of Civil Liberties has raised concern regarding mass and discriminatory surveillance [22] ("Facial-Recognition Technology Will Turn Gardaí into Roaming Surveillance Units – The Irish Times,"). However, the legislation is targeting to build safeguards such as data protection, which would curb the infringement of the right to privacy.

In a similar context, the data that is to be collected as per the Criminal Procedure Identification Act 2022 by the NCRB may in the future be used to feed the data to such AI for the purpose of investigation and profiling that may raise the concern regarding right to privacy and discrimination.

Although the use of AI in the criminal justice system would improve public safety and help in the investigation of crimes committed by facial recognition, detection of individuals, etc [23]. But at the same time it should be handled with caution to avoid the infringement of fundamental rights.

Complication In Using Ai In Criminal Justice System: The Rule Of Law Embodies The Right To equality, and thus the public officials making the decision must be accountable. Using AI for the purpose of investigation may cause difficulty in determining whom to hold liable for the violation of rights due to the outcome provided by AI as it uses a system that does not have human intervention and is based on "black box" reasoning [24]

The only option left is to make the manufacturer and designer liable, but even they could not be made completely liable for the algorithms derived by the AI as it works on the machine learning system. Moreover, even the members of the European Union are aware about the complications of using AI, especially regarding the discriminatory and biased results provided by it [25].

The AI system misclassified people belonging to certain races, communities, etc., and thus it is required to counter such problems by avoiding algorithm-created discrimination and bias [26]. Human oversight is required to enhance data security and protect personal data. The resolution further demands a permanent ban on the recognition of human features in public spaces as it raises privacy concerns.

Biased Outcome of AI: AI Are Often Trained Based on the historical, institutional, etc. data collected and are thus more likely to discriminate based on races, communities, and geographical areas. These discriminations are so inherited in the algorithms that the results are prone to being biased [27]

The Criminal Procedure Identification Act authorises the agency to collect the data of prisoners and other people that may in the future be used to set the algorithms of the AI for investigation purposes. India has a diverse culture and geographical areas, and thus discrimination based on culture, race, and geographical area is likely to happen in this country.

For example, the north eastern people have similar facial structures, it is more likely to happen that if in case there are a greater number of people whose data has been collected and fed in AI belongs to North Eastern states, such people would be scrutinized more compared to others.

AI System Shall Be Designed To Be Non-Discriminatory: The USA has COMPAS, a risk assessment tool that was designed to predict the people who are more likely to re-commit the offence. The USA media found that 77% of the people belonging to the black community were at high risk of re-committing the offence [28]. Thus, it signifies that the AI based outcome is discriminatory in nature and requires human intervention.

In Denmark, AI is used to classify neighbors based on their education, crime rates, second generation migrants (the population of second-generation migrants in Denmark is 50%), etc., and the neighbors so classified are differently treated and are given higher punishments if they commit a crime. This indicates that the use of such an AI system needs to be regulated [29].

Conclusion

The Criminal Procedure (Identification) Act, 2022, has many prerequisites. Privacy and illegal profiling are important issues. This bill exceeds the existing capacitive, infrastructural, and legal limits in multiple respects.

India needs to pass the Data Protection Bill with significant purposive and substantive changes, especially to Section 10 of the Right to be Forgotten, and make it more process-oriented and protect against illicit data processing after (lawful) collection from the individual. The Act requires a thorough and definitive set of standards and limitation clauses to limit the use of acquired data and prevent arbitrariness and force in measurement reporting.

The EU's GDPR, various American Judgements, and European jurisprudence regarding data and privacy must be used to comprehensively stratify data on the basis of varying sensitivity, which the existing Act lacks. The NCRB must be monitored by an established, public and independent Data Protection Authority with regards to the data it collects as per the Act. Before it can handle the enormous range of data and samples the Act requires it to gather, preserve, and process, the NCRB needs an infrastructural makeover.

The introduction of AI to the data collected in the procedure of data processing, making of database, statistical generation, etc. must have human intervention to avoid the inherent bias and prejudices from getting magnified by the sociologically and morally unaware AI systems. They are highly mathematical in nature and solely result – oriented which is not a desirable situation when it comes to law enforcement and criminal justice systems. Human intervention and an authority to socio – legally examine the data is mandatory.

This Act comes a bit ahead of its time, at least ahead of the preparations that need to be made before this can become even remotely enforceable. Unless the changes suggested are made (at least), there shall arise numerous issues of data security, qualitative maintenance of the samples collected and most importantly non – arbitrary and just enforcement of law, without sacrificing rights of the Indian citizen.

References

1. Google Spain SL v. Agencia Espalona de Protection de Datos, Case No. C-131/12, Court of Justice of European Union (CJEU) May 13, 2014).

2. EU's General Data Protection Bill, 2018, Pub. L. No. 2016/679, Art. 17(1)(a), 2018.
3. JE McNealy. The Emerging Conflict between Newsworthiness and the Right to Be Forgotten, SSRN Scholarly Paper, Rochester, NY, 2012. https://papers.ssrn.com/abstract=2027018.
4. Justice K.S. Puttaswamy (Retd.) v. Union of India AIR 2018 SC 1841 (India), 2017.
5. The Criminal Procedure (Identification) Act 2022, § 4(2).
6. Indian Data Protection Bill, 2022, § 10, 2023.
7. GS Bajpai, S Beweja, Questioning the feasibility of the Criminal Procedure (Identification) Act, 2022.
8. Supra N. 4.
9. Supra N. 2.
10. C Jasserand. Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation? [SSRN Scholarly Paper]. Rochester, NY, 2018. https://papers.ssrn.com/abstract=3230347.
11. General Data Protection Regulation, 2016, Art. 5(1)(e).
12. The Code of Criminal Procedure, 1973, Act No. 2 of 1974, § 53 (1974).
13. Supra N. 7
14. Office of Privacy and Civil Liberties, Privacy Act of 1974. (2014, June 16), 2023. https://www.justice.gov/opcl/privacy-act-1974.
15. California Consumer Privacy Act (CCPA) (2018, October 15), (Retrieved May 4, 2023), from State of California, Department of Justice, Office of the Attorney General website: https://oag.ca.gov/privacy/ccpa.
16. Selvi v. State of Karnataka, AIR 2010 SC 1974.
17. Supra N. 4.
18. CP Dai, F Ke. Educational applications of artificial intelligence in simulation-based learning: A systematic mapping review. Computers and Education: Artificial Intelligence,2022:3:100087 https://doi.org/10.1016/j.caeai.2022.100087.
19. S Poole, The big idea: Should we worry about artificial intelligence? The Guardian, 2021. Retrieved From https://www.theguardian.com/books/2021/nov/29/the-big-idea-should-we-worry-about-artificial-intelligence.
20. AI audit framework on ICO agenda, (2023, April 5). Retrieved 2023, from Pinsent Masons https://www.pinsentmasons.com/out-law/news/ai-audit-framework-on-ico-agenda.
21. AI Act: EU must ban predictive AI systems in policing and criminal justice (2022, March 1), Retrieved May 4, 2023, from Fair Trials website: https://www.fairtrials.org/articles/news/ai-act-eu-must-ban-predictive-ai-systems-in-policing-and-criminal-justice/.
22. Facial-recognition technology will turn gardaí into roaming surveillance units – The Irish Times. (n.d.). Retrieved May 4, 2023, from https://www.irishtimes.com/opinion/2023/04/18/facial-recognition-technology-will-turn-gardai-into-roaming-surveillance-units/.
23. Using Artificial Intelligence to Address Criminal Justice Needs. (n.d.). Retrieved May 4, 2023, from National Institute of Justice website: https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs.
24. Emily Binchy, Advancement or Impediment AI and the Rule of Law, 2022 Retrieved from Advancement-or-Impediment-AI-and-the-Rule-of-Law.pdf. (n.d.).
25. EP Resolution on AI in Criminal Law and Policing. (n.d.). Retrieved May 4, 2023, from https://eucrim.eu/news/ep-resolution-on-ai-in-criminal-law-and-policing/.
26. Ibid
27. Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act, (n.d.). Retrieved May 4, 2023, from European Digital Rights (EDRi) website: https://edri.org/our-work/civil-society-calls-on-the-eu-to-ban-predictive-ai-systems-in-policing-and-criminal-justice-in-the-ai-act/.
28. Mattu, J Angwin, Machine Bias (May 23, 2016). Retrieved May 4, 2023, from ProPublica website: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
29. Automating Society 2019. (n.d.). Retrieved May 4, 2023, from AlgorithmWatch website: https://algorithmwatch.org/en/automating-society-2019/.