Impact Factor (SJIF): 6.092 E-ISSN: 2583-1615

International Journal of Research in Academic World

Received: 19/July/2024 IJRAW: 2024; 3(8):189-192 Accepted: 25/August/2024

Enhancing Data Privacy within Criminal Justice System in India: The Case for a 'Privacy by Design' Framework in the Digital Era

*[1]Neha Agarwal

*[1]Research Scholar (UGC-SRF), Faculty of Law, Osmania University, Hyderabad, Telangana, India.

Abstract

The legislature's adoption of a criminal procedure model not only encourages a thoughtful examination of the standards for applying criminal sanctions but also sheds light on what those standards should ideally be. A noticeable movement away from the 'due process model' towards the more prevalent 'crime control model' is unfolding in India. This profound shift is reflected in the overarching goal of criminal laws, which increasingly emphasize crime prevention over procedural fairness, frequently leading to the erosion of individual privacy rights. This development, along with the stigmatizing impact of the criminal procedure, underscores the need for reforms in the criminal justice system by establishing safeguards and oversight mechanisms to regulate the power of the state and its agencies. In line with this, the paper seeks to explore the implications of the Criminal Procedure (Identification) Act, 2022 on the fundamental right to individual privacy and the potential conflicts that may emerge between the legislation's goals and its practical application. The paper offers a critical examination of the provisions of Act-2022 through the lens of fundamental principles of the criminal justice system and the constitutional right to privacy. To tackle these legal challenges, the concluding section of the paper recommends strategies to address privacy concerns in the digital age by integrating a 'Privacy by Design' framework into Act-2022.

Keywords: Data privacy, privacy-by-design, criminal identification, due-process model, proportionality test, judicial construct

1. Introduction

1.1. Emerging Trends in Privacy Jurisprudence under Criminal Justice System

Criminal justice systems typically oscillate between two models: the Due Process Model, which emphasizes fairness and adherence to legal procedures, and the Crime Control Model, which prioritizes truth-finding and proving guilt [2]. The Criminal Procedure (Identification) Act, 2022 (Act-2022) replaced the Identification of Prisoners Act, 1920 [3], after significant debate in Parliament and reflects a shift from the Due Process model to the Crime Control model. Designed to enhance investigations through modern technology, the Act broadens the powers of law enforcement and the judiciary. However, concerns have emerged regarding inadequate data protection safeguards, potential misuse by the state to suppress dissent, and fears of an evolving surveillance state. In promoting the Crime Control model under the guise of law enforcement, the state risks infringing on individual rights, a core principle of the Due Process model. This calls for a reassessment of current legal frameworks to strike a balance between protecting privacy and addressing legitimate state interests like crime prevention and prosecution. The Supreme Court's recent dismissal of a public interest litigation challenging the constitutionality of Act-2022 further underscores the need for this discussion [4].

1.2. Nexus between Criminal Identification and Data Privacy

Governments and law enforcement frequently use 'measurements' for purposes like identifying suspects or victims. However, without strong constitutional and legal privacy protections, this practice risks infringing on individual privacy. Best international practices suggest obtaining consent when possible, requiring court orders before sample collection, fully informing individuals, and segregating samples. This paper highlights the significant privacy concerns associated with collecting measurements from individuals, exacerbated by vague criminal laws and courts' tendency to expand rather than clarify legal ambiguities [5]. These issues risk disproportionately burdening individual privacy rights. Current provisions under the Code of Criminal Procedure, 1973 (CrPC) and the Act-2022 lack clarity regarding which entities, beyond law enforcement, are permitted to collect, manage, and store bodily samples, and for what purposes. Moreover, these entities are not legally required to follow standardized procedures, seek consent, or inform individuals about the collection and use of their measurements.

The Supreme Court has recognized that data privacy, including biometric and other personal data, falls under the right to privacy guaranteed by Article 21 [6]. The collection

*Corresponding Author: Neha Agarwal

and handling of measurements intrude upon individual privacy, particularly concerning sensitive personal data such as biometric, and behavioral information managed by the state. This requires that the state protect such data from both internal and external breaches throughout criminal proceedings, from investigation to trial and beyond. While recognizing the necessity of these powers in criminal justice, it is vital to establish clear safeguards to ensure that such authority is exercised in line with principles of justice. In light of Edward Snowden's revelations about the state's tendency to bypass accountability when granted extensive data collection powers, it is crucial to explore ways to safeguard personal data privacy within the framework of constitutional protections against state intrusion [7].

2. Constitutional Conundrums of Privacy in Criminal Proceedings

2.1. Ramifications of Criminal Procedure on Fundamental Right of Individual Privacy

While the Act-1920 allowed for basic identification techniques like fingerprints and photographs for arrested individuals, Act-2022 significantly expands the scope of 'measurements' to include iris scans, retina scans, handwriting analysis, palm prints, and various physical and biological samples [8]. This broader definition suggests the potential creation of detailed personal profiles from the collected data. A particularly contentious aspect of Act-2022 is its requirement for digital or electronic storage of these measurements for seventy-five years without established procedural safeguards [9]. These provisions clearly violate Supreme Court guidelines [10], which state that the lack of precise guidance makes a law arbitrary, leading to excessive and disproportionate infringements on privacy. Moreover, the Act's vague integration of 'behavioral attributes' could be interpreted broadly, potentially extending to testimonial measurements and their compulsory collection [11]. This interpretation conflicts with the Supreme Court's ruling in *Selvi v. State of Karnataka* [12], which protects privacy and the right against self-incrimination under Article 21 and Article 20(3) of the Constitution of India respectively.

2.2. Paradigm of Proportionality Test to Assess Privacy Infringements by the Act-2022

In *Puttaswamy-I* [13], the Supreme Court established a four-pronged proportionality test to address concerns about state encroachments on privacy. This test outlines a right to privacy by allowing reasonable restrictions under the following criteria:

i). The action must be legally sanctioned (legality prong);
ii). It must serve a legitimate purpose in a democratic society (suitability prong);
iii). The level of interference must be proportionate to the need (necessity prong); and
iv). There must be safeguards to prevent misuse (balancing prong).

Evaluating Act-2022 against this test is crucial to ensure its legitimacy and compliance with the Rule of Law and Constitutionalism, thereby limiting state discretion. If any of the four criteria are not complied, the Act may face constitutional challenge and be declared invalid. While Act-2022 fulfills the legality prong by legislating for crime investigation and prevention, it fails to meet the other three criteria.

It fails the suitability prong due to the Act's failure to differentiate among convicts, detainees, and individuals under Section 117 of the Code of Criminal Procedure leads to an excessive invasion of privacy, lacking reasonable connection to the nature of the offense or investigative needs. This is similar to the European Court of Human Rights' ruling in *Gaughran v. The United Kingdom* [14], which found that indiscriminate retention of personal data, such as DNA profiles and photographs, was an undue intrusion on privacy and not justified in a democratic society. The Act's broad application to all individuals, regardless of the offense's severity or their relevance to an investigation, and its lack of provisions for data deletion timelines or specific purposes for data use, result in disproportionate privacy invasions [15]. These issues make the Act's encroachments on privacy unjustifiable in relation to its stated objectives, failing the necessity prong. Further, the Act fails to specify the purposes for which collected measurements can be used and allows for indiscriminate collection, processing, and storage by various agencies without procedural safeguards or regard for the offense's nature or established guilt. Consequently, it does not reasonably justify privacy intrusions, lacking balance between individual rights and state interests, and thus fails the balancing prong.

3. Critical Evaluation of the Act-2022 on the Touchstone of Right to Privacy and Fundemental Criminal Law Principles

3.1. Impact on Rules Legality and Adjudication Legality

Criminal law upholds the Rule of Law through two principles of legality: Rules Legality and Adjudication Legality [16]. Rules Legality includes fair notice, prevention of over-deterrence, and exclusive criminalization power for the legislature, while Adjudication Legality ensures uniform application and adjudication of violations [17]. Ambiguous laws can lead to arbitrary enforcement and discretionary abuse by the executive, highlighting the need for clear legal standards to prevent individual biases in law enforcement and judicial processes.

The Act-2022 undermines the principles of legality by failing to provide fair notice to those whose measurements are being collected. Unlike the withdrawn DNA Technology (Use and Application) Regulation Bill, 2019, which required consent or a Magistrate's approval for collecting measurements, Act-2022 removes this safeguard with few exceptions. Additionally, the Act-2022 allows for excessive discretion in enforcing criminalization by using non-mandatory language like 'may' instead of 'shall,' and extends authority to compel both biological and non-biological samples [18]. Additionally, the Act-2022 grants broad discretionary authority to Magistrates to order measurements from individuals for investigations or proceedings under any law, contrasting sharply with Clause 21(3) of the DNA Bill, which limited collection to arrested individuals with reasonable cause [19]. By removing the requirement for reasonable cause and allowing measurements from any individual, the Act-2022 fails to adhere to the legality doctrine and the Rule of Law.

3.2. Lack of Procedural Safeguards and Violation of Principle of Limited Delegation

The Act-2022 exhibits excessive delegation of power by leaving critical provisions undefined and allowing the executive to set rules, contrary to limited delegation as established by administrative law principles and judicial standards [20]. According to the Supreme Court, while

legislative delegation is permissible, it must not result in the executive performing legislative functions [21]. The Act fails to provide clear legislative guidance or procedural safeguards for the Governments in rule-making [22]. It permits the governments to regulate all aspects of measurement handling, from collection to destruction, through their rules, and allows officers or Magistrates to collect measurements without specifying the criteria for what constitutes expediency [23]. This lack of defined standards and constraints on authority undermines privacy protections.

3.3. Reverse Burden of Proof and Violation of Principle of Presumption of Innocence

The principle of presumption of innocence holds that a defendant is presumed innocent until proven guilty and that those asserting claims must fulfil the burden of proof [24]. This principle faces scrutiny when reverse burdens are imposed, raising questions about whether they violate the presumption and if such violations are justifiable [25]. The Act-2022 undermines this principle by permitting the collection of measurements from any individual without linking it to a crime, arrest, or magisterial order, and disregards the requirement for proving mens rea. Additionally, it infringes on privacy rights by allowing enforcement of measurement collection against resistant individuals according to unspecified rules.

3.4. Missing *Mens rea* and Violation of Principle of Fair Labelling

The principle of proportionality in criminal law links innocence with both blamelessness and the appropriate mental state, advocating for a proportional mens rea framework to ensure fairness and safeguard innocence [26]. This approach requires procedural safeguards to match the severity of offenses with appropriate sentencing [27]. The Act-2022 violates these principles by criminalizing resistance to measurement as obstruction of a public servant, without a proportional or principled sentencing approach and lacking differentiation between offense severity and individual circumstances [28]. It also breaches the Fair Labelling principle by failing to clearly distinguish between different types of offenses and individuals affected.

4. Suggestions for Integration of 'Privacy by Design' Paradigm in the Act-2022

To address the stigmatizing and coercive aspects of the criminal process, this paper advocates for integrating procedural safeguards through a 'Privacy by Design' framework [29], linking data protection law with Act-2022. This approach aims to balance privacy rights with legitimate state interest of the law enforcement, enhancing privacy protections in criminal identification procedure.

a) **Accountability Framework:** To enhance privacy and address legislative shortcomings, India should implement an Accountability framework within its criminal procedure for individual identification. This framework designates entities handling personal data as 'data fiduciaries,' requiring them to meet stringent privacy and security standards under the newly enacted data protection law [30] and shift the onus of proof onto the state in cases of breaches, thus reinforcing accountability and trust between the state and its citizens.

b) **Strict Liability:** Data fiduciaries will face strict liability for unlawful handling of personal data, regardless of the harm's immediacy, based on tort principle of strict liability [31]. Law enforcement and others involved must process data solely for legitimate purposes, with penalties for breaches proportional to the severity and sensitivity of the data, and state must prove compliance. The Data Protection Board of India will adjudicate privacy breaches under Act-2022, though officers acting in good faith will be shielded from legal action [32].

c) **Vertical Application of Law:** The Act-2022 shall integrate core privacy principles, as recommended by Justice A.P. Shah's expert group, to guide stakeholders on their rights and responsibilities, especially in complex technological contexts [33]. These principles, including "collection limits, purpose specification, storage restrictions, disclosure controls, transparency, and security", will be enforceable against the state and its agencies as enunciated by courts under Article 12, with consent required except for specific offenses, where judicial approval will be necessary for data collection.

d) **Limitations on Exemptions to State and its Agencies:** The proposed framework allows state exemptions for sovereignty, public order, law enforcement and compliance with judicial orders, enabling non-consensual data processing. To ensure oversight and prevent misuse, a retired judicial officer, appointed in consultation with the Data Protection Board of India, should authorize or restrict state agency actions based on case specifics [34].

e) **Participation Rights for Data Privacy:** The Act-2022 shall adopt a rights-based approach, ensuring individuals have inviolable set of digital rights to protect their data, including correction, deletion, the right to be forgotten, and grievance redressal. This framework will enhance fundamental rights and uphold individual liberty and dignity in the digital realm.

f) **Policy Measures to Complement Constitutional and Legal Safeguards:** Measures such as establishing a Regulatory Board for oversight, accrediting and evaluating measurement-handling agencies, creating standardized guidelines for data management by the NCRB, ensuring ongoing training for law enforcement officers, developing legal standards for different types of measurements, setting guidelines for data deletion requests, and restricting access and dissemination of measurement data, needs to be simultaneously undertaken.

Conclusion

The Act-2022 diverges from the 'Due Process Model' and fails the proportionality test, reflecting a shift towards Inquisitorial techniques and a focus on crime suppression that undermines fundamental criminal law principles and more importantly the fundamental right to data privacy under Article 21 of the Constitution. To address this, the 'Privacy by Design' approach is suggested, emphasizing on individual autonomy and privacy towards data empowerment and data justice in the digital age. Shifting away from this approach, except in extreme cases like subversive activities against state or terrorism, could undermine the criminal justice system and lead to excessive state control over data privacy of individuals.

References

1. The Criminal Procedure (Identification) Act, 2022 (Act 11 of 2022).
2. Herbert L. Packer, "Two Models of Criminal Process" 113 *University of Pennsylvania Law Review* 1 (1964).

3. The Identification of Prisoner's Act, 1920 (Act of 33 of 1920).
4. Awstika Das, "Supreme Court Refuses to Entertain Challenge to Law Allowing Collection of Prisoners' Biometrics", *Live Law*, Feb. 12, 2024.
5. Stephen F. Smith, "A Judicial Cure for the Disease of Over-criminalization" 135 *Heritage Foundation Legal Memo 1 (2014)*
6. *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others,* (2019) 1 SCC 1.
7. Shankar Narayan, "Criminal Identification Bill Follows Similar Unsuccessful, Discriminatory Laws Elsewhere', *The Wire*, Apr. 11, 2022.
8. [1] *Supra* note 3, s. 2(a) and s. 5; *supra* note 1, s. 2(b).
9. *Id.,* s. 4(2).
10. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
11. National Law University, Delhi, "An Analysis of the Criminal Procedure (Identification) Act, 2022" (September, 2022), at 7.
12. (2010) 7 SCC 263.
13. *Justice K.S. Puttaswamy (Retd.) v. Union of India,* (2017) 10 SCC 1.
14. ECLI: CE: ECHR: 2020: 0213JUD004524515.
15. *Supra* note 1, s. 4.
16. *Supra* note 1 at 335.
17. *Id.* at 375, 378-379.
18. *Supra* note 1, s. 4(1) and s. 3.
19. *Id*., s. 5.
20. *Hamdard Dawakhana v. Union of India*, AIR 1960 SC 554, p.33.
21. *In Re: The Delhi Laws Act*, 1912, AIR 1951 SC 332.
22. *Supra note 1,* s.4, s.8.
23. *Id*., s.8.
24. Jerome Hall, "Nulla Poena Sine Lege", 47 *Yale Law Journal* 165, 192-193 (1937).
25. Victor Tadros and Stephen Tierney, "The Presumption of Innocence and the Human Rights Act*",* 67 *Modern Law Review* 402, 404 (2004).
26. Stephen F. Smith, "Proportional Mens Rea", 46 *American Criminal Law Review* 127 (2009).
27. Andrew Ashworth, *Principles of Criminal Law* 109 (Oxford University Press, UK, 6th ed., 2009).
28. *Supra note 1,* s.6.
29. Neha Agarwal, "Deciphering Right to Informational Privacy in India: A Comparative Analysis of DPDP Bill, 2022 and DPDP Act, 2023" 3(5) *International Journal of Research in Academic World* 10-11 (2024).
30. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 4-10.
31. *Rylands v. Fletcher*, (1868) LR 3 HL 330.
32. *Supra note 1,* s.7.
33. Committee of Experts under Chairmanship of Justice A.P. Shah, "Report of the Group of Experts on Privacy*"* (October, 2012), 21.
34. Neha Agarwal, *Right to Privacy and Data Protection in India: From a Judicial Construct to Legislative Reality* (2024) (Unpublished Ph.D. dissertation, Osmania University), at 287.