Page 1190 - 1203 **DOI:** *https://doij.org/10.10000/IJLMH.1110404*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 4

2025

Through the Eye of the State: Biometrics, Surveillance and the Evolution of Liberty in India's Criminal Justice System

PANKAJ SHARMA[1] AND DR. SHIV KUMAR KURREY[2]

ABSTRACT

This piece critically examines the constitutional and philosophical implications of the Criminal Procedure (Identification) Act, 2022. This piece contends that while the Act strengthens the evidentiary and identification power of the state, it threatens to upset the precarious balance between state power and liberty. Based on the Puttaswamy privacy doctrine, Foucault's surveillance theory, and comparative law perspective, this piece critiques whether liberty is compatible with a digitalized criminal justice system.

I. INTRODUCTION

Contextualizing the Emergence of Biometric Technologies

Over the last two decades, biometric technologies have evolved from being tools of civilian identification to being instruments of law enforcement, national security, and population control.[3] Fingerprints, face recognition, iris scans, voice prints, and DNA profiling entered the widening biometric regime worldwide.[4] It happened in India with the explosion of the Aadhaar project, which has emerged as the world's biggest biometric database, encompassing more than 1.3 billion residents.[5] It was first implemented for disbursing welfare, and Aadhaar's architecture unwittingly sanctioned state-sponsored biometric surveillance.[6]

The installation of predictive policing software, smart CCTV networks, and automatic facial recognition systems (AFRS) is a transition from traditional policing to techno-governance.[7] In this, the body of the citizen is no longer merely a subject of law but a variable of ongoing identification and data accumulation.[8] Biometrics ensure precision and swiftness—but at what constitutional cost?

[1] Author is a Research Scholar at Govt J Yoganandam Chhattisgarh College Raipur (C.G), India.
[2] Author is an Assistant Professor at Govt J Yoganandam Chhattisgarh College Raipur (C.G), India.
[3] Usha Ramanathan, Aadhaar: A Tool of Surveillance, 46 Econ. & Pol. Weekly No. 50 (2011).
[4] Reetika Khera, Aadhaar and Food Security in India, 106 World Dev. 104–13 (2018).
[5] Unique Identification Authority of India, Annual Report 2021–22.
[6] N. McCarthy & J. Higgins, Biometrics and Welfare in India, 15 J. Dev. Stud. 82–98 (2019).
[7] Amnesty Int'l, Automated Injustice: How AFRS Undermine Human Rights in India 12–34 (2021).
[8] Internet Freedom Found., Surveillance Reforms in India: Need for Oversight 8–22 (2023).

 [ISSN 2581-5369]

Overview of the Criminal Procedure (Identification) Act, 2022

Passed by Parliament in April 2022, the Criminal Procedure (Identification) Act, 2022 superseded the colonial Identification of Prisoners Act, 1920.[9] The new Act greatly expands the types of "measurements" that law enforcement officers may obtain from an individual, including fingerprints, palm prints, iris and retina scans, photos, behavioral patterns, and even DNA.[10] It makes it permissible to take not only from convicts, but from those arrested, detained, or even merely called for an offence under any law.[11]

Above all, it enables information to be stored digitally for 75 years, and enables police officers at any level of rank (not just magistrates) to approve collection.[12] It removes the right of refusal, on grounds of informed consent, privacy, rights of the body, and against self-incrimination under Article 20(3).[13]

Research Question

The general question of this paper is:

Can a surveillance-hungry state maintain constitutional freedom in a time of widening biometric surveillance?

This paper contends that while technological progress is beneficial to the criminal justice system, their disproportionate or unregulated use undermines the very foundation of liberty, privacy, and dignity guaranteed under the Indian Constitution, referring specifically to the case of K.S. Puttaswamy v. Union of India (2017).[14]

II. STATE SURVEILLANCE IN INDIAN CRIMINAL LAW: HISTORY

India's jurisprudence shows a uniform pattern of state control over the bodies of Indians in the name of the imperative of law and order. The legal machinery of surveillance has evolved over the decades—from colonial policing to post-colonial digital surveillance.[15] Here is a chronology of this continuum of history:

[9] Identification of Prisoners Act, 1920, No. 17, Acts of Parliament, 1920.
[10] Criminal Procedure (Identification) Act, 2022, supra note 1, § 2(b).
[11] Id. § 2(e).
[12] Id. § 3(1).
[13] India Const. art. 20(3).
[14] K.S. Puttaswamy, supra note 2.
[15] Indian Police Act, 1861, No. 1, Acts of Parliament, 1861.

 [ISSN 2581-5369]

Table: Evolution of Bodily Surveillance Laws in India

Year	Law / Framework	Key Provisions	Surveillance Techniques	Significance
1861	**Indian Police Act, 1861**	Gave colonial police wide powers of arrest, search, and preventive detention	Physical inspections, manual records	Legalized colonial control post-1857 rebellion; no citizen safeguards
1920	**Identification of Prisoners Act, 1920**	Allowed collection of **fingerprints, footprints, and photographs** from convicts and certain categories of arrestees	Manual biometric recording	Introduced bodily surveillance as legal evidence; discretionary and limited
1973	**Code of Criminal Procedure, 1973 (CrPC)**	Section 53, 53A, and 54 authorized medical examination of accused; Section 311A allowed for handwriting/signature samples	Semi-voluntary bodily and biological evidence	Balanced with judicial oversight but lacked provisions for DNA or digital storage
2000	**Information Technology Act, 2000**	Introduced digital signatures, electronic surveillance, and cyber-policing	Online tracking, metadata monitoring	Focused on cybercrime but became gateway for non-physical surveillance
2009–Present	**Aadhaar (UIDAI project)**	Collected biometric and demographic data for ID creation	Fingerprints, iris scans, facial image	Created world's largest biometric ID base; initially voluntary, later linked to welfare and bank accounts
2018	**AFRS (Automated Facial Recognition System)**	No legislation; implemented through police databases	Real-time facial scanning and matching with criminal records	Lacks statutory framework or judicial oversight
2022	**Criminal Procedure (Identification) Act, 2022**	Allows **compulsory** collection of biometric and biological samples, even from non-convicts; retention for 75 years	Fingerprint, iris, DNA, handwriting, behavioural traits	Most expansive identification law; criticized for lacking proportionality, consent, and judicial safeguards

Main Continuity and Development Characteristics

Voluntary to compulsory: Earlier provisions allowed suspects to refuse, but the 2022 Act takes away such a safeguard. From scarce data to full-body profiling: What began with fingerprinting has become full biometric capture. From judicial control to executive discretion: Power has moved from magistrates to police officers. From temporary storage to digital permanence: Retention periods have lengthened from days/weeks to decades.

This development shows a clear path of the state normalizing appropriation of the body and control of information, frequently in the absence of protection. The Identification Act, 2022 therefore comes across as a reflection of the state's quest for an all-knowing, all-seeing system of enforcement.

III. THEORETICAL OUTLINE: SURVEILLANCE AND THE SELF

To comprehend the philosophical aspects of the Criminal Procedure (Identification) Act, 2022, it is necessary to examine how surveillance operates in connection with ideas of the self, freedom, and the power of the state. The section dialogues with the major theoretical explanations—Foucaultian panopticism,[16] Benthamite utilitarian legitimacy of surveillance, and Ambedkarian democratic accountability—to utilize as a collectivity of analytical perspectives to interpret the implications of the law.

Foucault's "Panopticon"

French philosopher Michel Foucault's critique in 'Discipline and Punish' reinterprets Jeremy Bentham's Panopticon not merely as an architectural design but as a metaphor for modern disciplinary power. The Panopticon—where the watchtower can see all the cells without being observed—creates a condition of continuous visibility that guarantees automatic obedience. Foucault argues that with such a setup, the subjects learn to internalize the observation and discipline themselves.

The Identification Act represents this rule of internalized observation. By instituting the possibility of permanent measurement, profiling, and storage in biometric databases, it alters the sense of bodily autonomy.[17] It makes citizens permanent suspects, especially those from marginalized communities. The potentiality of being watched becomes an instrument of control.

[16] Foucault, supra note 5, at 200–25.
[17] Id. at 209.

 [ISSN 2581-5369]

Bentham's Utilitarianism and Justification of Surveillance

Jeremy Bentham, the Panopticon's designer, justified surveillance as a rational and efficient way of maximizing the common good. Public safety and deterrence justified public intrusion into personal privacy from a utilitarian perspective. The utilitarian doctrine of 'the greatest good for the greatest number' was the basis of that acceptance.[18]

But the concern with the Identification Act is that the balance may be tipped too far towards state utility at the expense of individual rights. Utilitarian justification of any and all intrusion is possible without proper safeguards. A utility-based criminal justice system has the danger of legitimizing coercion without proportion.

Ambedkar's Vision of State Accountability

Dr. B.R. Ambedkar, contrary to Bentham and Foucault, demanded democratic and moral accountability of state power. His vision for the Indian Constitution was that while the state should be empowered, it should yet be subject to the rule of law and civil liberties.

Ambedkar dreaded the emergence of 'hero worship' and untrammelled executive power. In his address to the Constituent Assembly, he cautioned against an executive-dominated state becoming tyrannical in the absence of constitutional checks. He envisioned a system of justice that ensured the dignity of the weakest, that is, Scheduled Castes and Adivasis.

Against this background, the Identification Act has to be tried against Ambedkar's normative values—does it safeguard the marginalised,[19] or subject them to greater state intrusion without recourse? Does it strengthen the judiciary as a check, or consolidate power in the hands of the police? These are the questions crucial to deciding whether the Act is in the spirit of the Indian Constitution.

IV. RIGHT TO PRIVACY AND COMPARATIVE STUDY

Indian Constitutional Jurisprudence Post-Puttaswamy

The historic judgment in K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, was a constitutional milestone in India. The Supreme Court was headed by a bench of nine judges who ruled unanimously that the right to privacy is a constitutional right under Part III of the Constitution and is enshrined in Articles 14, 19, and 21. The judgment brought privacy to a natural, inalienable, and intrinsic right relating to individual freedom and dignity.

In its broadest meaning, perhaps the most important achievement of the ruling was the

[18] Bentham, supra note 6, at 60.
[19] B.R. Ambedkar, Constituent Assembly Debates, Vol. IX 132–45 (1949).

 [ISSN 2581-5369]

establishment of "informational autonomy," or the idea that individuals should be responsible for the acquiring, storing, processing, and forwarding of personal information. State interests of even security or convenience only can invade privacy only after they have overcome the constitutional hurdle, the court determined.

The court created a three-stage test of proportionality for any interference by the state with privacy:

1. Legality – The interference must be authorized by law.
2. Necessity – It must be required for a legitimate state purpose.
3. Proportionality – The test should be the least intrusive to achieve the goal and should possess proportion between the state's interest and the rights of the individual.[20]

Referring this test to the Criminal Procedure (Identification) Act, 2022, grave doubts arise:

- Legality: The Act is a validly enacted legislation. Legality, however, is not enough.
- Necessity: The State must establish why further biometric gathering from not only convicts but even suspects and detainees is necessary. The Act supplies no cogent or narrowly tailored basis.
- Proportionality: The Act allows for 75-year retention, broad collection powers like from those who have not yet been convicted, and lacks clear redressal or deletion policies. This fails the test of being the least restrictive means.[21]

Apart from this, Article 20(3) of the Constitution safeguards an accused from being compelled to be a witness against oneself. Although the Supreme Court in State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808, believed that fingerprints and physical evidence are not testimonial, DNA, retina, and behavioural profiling are on the cusp between physical and mental indicators. Judicial examination of the Identification Act under Articles 20 and 21 is hence constitutionally necessary.

International Comparative Perspective

1. United Kingdom: Protection of Freedoms Act, 2012 In the UK, the Protection of Freedoms Act, 2012 has been enacted to roll back excessive DNA profile and biometric data retention after the S. and Marper v. UK case (ECtHR, 2008). Characteristics are:

- Compulsory erasure of biometric information in case the person is not convicted.

[20] K.S. Puttaswamy, supra note 2, ¶¶ 98–109.
[21] Criminal Procedure (Identification) Act, 2022, supra note 2.

- Independent oversight by the Biometrics Commissioner.
- Time-limited retention: DNA and fingerprints must be preserved under specific conditions and for a limited period.
- NOTE: India's Identification of Living Persons Act, however, allows retention of information for 75 years without any obligation of review, and no independent review committee.

2. European Union: GDPR and Biometric Data The General Data Protection Regulation (GDPR) classifies biometric data as "sensitive personal data" under Article 9 and mandates:

- Transparent and constructive consent to processing,
- Purpose limitation and data minimisation
- Right of erasure or right to be forgotten,
- Right of information and access to information.
- Any collection of biometric data for use by the police is covered by EU Directive 2016/680 on processing personal data by competent authorities. India does not have such protections in place.

3. United States: Maryland v. King (2013) In Maryland v. King,[22] The Supreme Court upheld taking DNA from arrestees for violent offenses but stressed heavily proportionality and reasonableness under the Fourth Amendment. The Court equated DNA with fingerprinting but spoke of procedural restraint and protection of privacy.[23] The most important lesson American jurisprudence has to offer is conditional approval: biometric collection is only allowed subject to judicial review, specified use, and due process.[24]

Synthesis: Where Does the Indian Law Stand? In global constitutional democracies, biometric collection is permitted but strictly regulated. The Indian Identification Act, although comprehensive in nature, lacks:

- Judicial or quasi-judicial oversight
- Time-sensitive data destruction procedures,
- Consent-based collection or exemptions for vulnerable groups

[22] Protection of Freedoms Act, 2012, c. 9, § 25 (UK).
[23] GDPR, Regulation (EU) 2016/679, art. 9(1).
[24] Maryland v. King, 569 U.S. 435 (2013).

 [ISSN 2581-5369]

Transparency or public accountability mechanisms. In its fusion of a colonial logic of suspicion of criminality with current technological capabilities, the Act is an unprecedented meeting of biometric power within the police. Conclusion of the Chapter Despite the fact that the Puttaswamy judgment created a robust constitutional framework of privacy in India, acts like the Identification Act, 2022 attempts to reverse its protections unless rigorously scrutinized. A comparative analysis from around the world underscores the need to place guardrails—through amending legislation, data protection laws, and by the courts—preventing surveillance from becoming sovereignty's most dangerous tool.

V. CONSTITUTIONAL ISSUES, JUDICIAL INTERPRETATIONS, AND DIGNITY PHILOSOPHY

Basic Rights Involved: Articles 21, 14, and 20(3)

The Criminal Procedure (Identification) Act, 2022, in essence, raises serious constitutional issues. It has the potential to violate Article 21 (right to life and liberty), Article 14 (equality before the law and equal protection of the laws), and Article 20(3) (protection against self-incrimination).[25]

Under Article 21, privacy as a right has been enshrined as a fundamental right after K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1. The blanket authorization of the Act to collect biological and biometric data — even from individuals who are not convicts but only accused, detained, or even summoned — amounts to an infringement of the principle of informational autonomy, a central tenet of the Puttaswamy judgment. There is no need for judicial sanction in most situations, and also no facility for consent or after-collection redress.

Article 14 is also involved since the law grants broad and arbitrary discretion to executive authorities. The Act allows for disproportionate treatment of persons — for example, a person arrested for a bailable and minor offence can still have their biometric profile retained for 75 years, even if never convicted. This contravenes the principle of non-arbitrariness, a fundamental of Article 14 as enunciated in E.P. Royappa v. State of Tamil Nadu, (1974) .

The most contentious article, however, is Article 20(3): "No person accused of any offence shall be compelled to be a witness against himself." Historically, the courts have read this provision to safeguard against testimonial compulsion. In State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808, the Supreme Court held fingerprints, handwriting, and physical specimens to not be testimonial in nature.

[25] India Const. arts. 14, 15, 21, 20(3).

 [ISSN 2581-5369]

But today's technological environment is much more intricate. Biometric information like DNA profiles, iris scans, voice samples, and even behavioural traits (such as gait or typing habits) could contain profound personal, family, or genetic details — rendering them arguably testimonial in effect, if not in form. Accordingly, the identification process can incidentally disclose evidence of identity, prior conduct, or hereditary tendencies, hence raising stark concerns regarding self-incrimination in the digital world.[26]

Until the courts re-examine the reach of "testimonial" in light of contemporary biometrics, the Act exists within an area of constitutional susceptibility.

VI. THE PHILOSOPHICAL QUESTION: STATE, DATA, AND DIGNITY

Beyond legality, there is the more profound question: what manner of relationship between the State and the citizen's body should exist in a democratic republic?

Historically, liberal constitutionalism is rooted in the notion that the State's purpose is to safeguard individual liberty, rather than to anticipate, list, and regulate it. However, statutes such as the Identification Act bespeak a paradigm shift—from the concept of the body as rights-holding to the body as data-providing.[27]

This transition indicates a more profound philosophical crisis. As Michel Foucault has so eloquently put it, surveillance is not simply a matter of watching; it is a matter of moulding behaviour, internalizing control, and disciplining bodies. Under constant scrutiny—or the threat of it—liberty is converted into performance. People start to behave not by free will, but by perceived notions of compliance.

In addition, the Ambedkarite understanding of democracy cautions against untrammeled executive authority. Dr. B.R. Ambedkar notoriously feared that India would slip into authoritarianism if democratic institutions were turned into means of domination instead of guardians of rights. Constitutional morality was seen by him as the ultimate guarantor against state encroachment, particularly for the historically disadvantaged.

Today, as biometric tracking targets tribal people, Dalits, undertrials, and the poor in a disproportionate way, we are forced to ask ourselves: Is the State performing its constitutional role of empowering them, or returning to its old colonial habit of suspicion? If those same people that Ambedkar referred to as the "depressed classes" become mere biometric registrations in police computer records, then the dignity Article 21 pledges is rendered an

[26] E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.
[27] Solove, Daniel J., A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).

 [ISSN 2581-5369]

empty shell.[28]

The philosophical paradox is this: Can freedom endure in perpetual surveillance?

Can the citizen remain free if their body becomes a permanent site of registration, analysis, and storage?

If freedom is to have any meaning in the digital republic, it must be freedom from algorithmic suspicion, biometric profiling, and bodily invasion—except in the strictest constitutional oversight. Without this, we risk building a "republic of control", not justice.

VII. CONCLUSION AND RECOMMENDATIONS

The Criminal Procedure (Identification) Act, 2022, even though brought forward to reform criminal justice and take advantage of advancements in technology, poses a significant constitutional issue. While the state definitely needs efficient tools to investigate crime and maintain public safety, such tools cannot at the expense of fundamental freedoms, human dignity, and procedural fairness under the Indian Constitution. The Act's sweeping and wide-ranging provisions point to essential gaps that need to be filled to maintain the fragile equilibrium between state security concerns and personal freedom.

The accompanying table highlights the key issues that involve constitutional, ethical, and procedural issues. The law's broad jurisdiction, extending collection of biometric data to detainees, suspects, and even those summoned on mere suspicion without charges, threatens to infringe upon the integral right to liberty enshrined in Article 21. Lack of consent procedures and provision of data retention for a record 75 years without meaningful review or deletion procedures reflect a perilous inclination towards perpetual surveillance, undermining both the doctrine of informational autonomy and the right to equality under Article 14. Additionally, executive-led authorization of data collection without judicial oversight puts at risk the separation of powers and the right to natural justice. The differential effect of such surveillance on marginal groups, including minorities, Dalits, and tribal populations, introduces an added dimension of injustice, endangering the constitutional promises of substantive equality and access to justice.

With these multi-pronged issues, there is a compelling necessity for judicial action to bring the Identification Act under the strictures of constitutional analysis. The Supreme Court is bound to use the proportionality test discussed in the landmark judgment in Puttaswamy, requiring any action of the state impinging upon privacy to be legal, necessary, and

[28] S. and Marper v. U.K., App. Nos. 30562/04 & 30566/04 (ECtHR 2008).

 [ISSN 2581-5369]

proportionate. Though the Act meets the threshold of legality due to the legislative process of Parliament, it lags on necessity and proportionality. The inability of the law to explain why current forensic and identification processes are inadequate, combined with its overreach in data scope and retention, makes it constitutionally susceptible. Judicial review via a Public Interest Litigation or direct constitutional challenge is essential to protect citizens' rights and avoid the entrenchment of permanent biometric surveillance databases.

Legislative and institutional reforms need to be implemented to restore constitutional balance. The definition of "measurements" must be tightly circumscribed, excluding sensitive cognitive, genetic, or behavioral information unless it is accompanied by rigorous judicial warrant. A consent model, with reasonable exceptions, would have to be implemented to avoid unwarranted intrusion, particularly in minor offenses. Furthermore, data storage has to be strictly time-limited, with automatic deletion procedures for acquitted suspects and those in petty crimes, together with redressal mechanisms for review and appeal. The authority to sanction intrusive biometric gathering must be with judicial or quasi-judicial powers and not just that of police officers, especially in delicate situations involving vulnerable groups. Establishing an independent Biometric Oversight Authority would increase transparency and accountability, as it would provide for regular audits and reporting on the use of biometric data to the public. In addition, ensuring legal aid and educating people about their rights and choices after collection is crucial to maintain access to justice, particularly for marginalized communities. Special protection is required to avoid exploitation of biometric technology in socio-economically weaker or tribal areas, where systemic injustices tend to be increased. Finally, India needs a holistic "Surveillance Regulation and Accountability Code" that brings together and oversees all facets of state-sponsored biometric and data activities. A code of this nature should incorporate the suggestions of Justice B.N. Srikrishna Committee on privacy and data protection, incorporating principles of accountability, transparency, and user rights. It will need to include sunset provisions, impose privacy impact assessments prior to installing any surveillance tool, and incorporate rights such as data portability and the right to be forgotten. This system would make sure that surveillance is always a tool of the state, not a weapon turned against its people.[29]

The long-term success of any constitutional democracy is not based on the use of power, but rather in its careful restraint. The age of cyberspace creates new challenges; unfettered control over bodies and information threatens to create an internal colonialism—a hidden, omnipresent, and possibly permanent one. It is important to remember that Sardar

[29] Justice B.N. Srikrishna Committee Report on Data Protection (2018).

 [ISSN 2581-5369]

Vallabhbhai Patel, who is usually credited with centralizing India's political union, realized the need for a disciplined but responsible state. Following his vision involves creating a biometric system of governance based on constitutional morality, safeguarding rights while facilitating security, and maintaining the dignity of all individuals.

Issue	Observation	Constitutional/Legal Risk
Overbroad scope	Applies to detainees, suspects, and even those merely summoned	Violates Art. 21 – liberty and proportionality
Absence of consent	No requirement of voluntary participation or awareness	Violates informational autonomy under Puttaswamy
Extended retention period	75 years of data storage regardless of outcome of trial	Arbitrary, lacks proportionality – Art. 14
No deletion or review mechanism	Even acquitted individuals' data may be retained indefinitely	Violates right to be forgotten; lacks remedy
Executive control, no oversight	No requirement for magistrate's approval in many cases	Violates separation of powers and natural justice
Risk of profiling/misuse	Disproportionate application on minorities, Dalits, and tribals	Undermines Art. 15 & 21 (substantive equality)
No legal aid or post-collection rights	Marginalized individuals unable to challenge state action	Denial of access to justice – Art. 39A, 21

 [ISSN 2581-5369]

VIII. BIBLIOGRAPHY

1. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
2. State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808.
3. E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.
4. Maryland v. King, 569 U.S. 435 (2013).
5. S. and Marper v. United Kingdom, ECtHR, App. No. 30562/04 and 30566/04 (2008).
6. Criminal Procedure (Identification) Act, 2022 (India).
7. Identification of Prisoners Act, 1920 (repealed).
8. Indian Police Act, 1861.
9. Code of Criminal Procedure, 1973 (India).
10. Information Technology Act, 2000.
11. Protection of Freedoms Act, 2012 (UK).
12. General Data Protection Regulation (GDPR), EU Regulation 2016/679.
13. EU Directive 2016/680 on processing of personal data for law enforcement purposes.
14. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
15. Justice B.N. Srikrishna Committee Report on Data Protection, 2018.
16. Jeremy Bentham, *The Panopticon Writings*, ed. M. Bozovic (Verso, 1995).
17. Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. A. Sheridan (Pantheon, 1977).
18. Michel Foucault, *Security, Territory, Population* (Palgrave Macmillan, 2009).
19. B.R. Ambedkar, *Annihilation of Caste* (Navayana, 2014).
20. B.R. Ambedkar, *The Essential Writings of B.R. Ambedkar*, ed. Valerian Rodrigues (Oxford University Press, 2002).
21. Gautam Bhatia, *The Transformative Constitution* (HarperCollins India, 2019).
22. Justice K.S. Puttaswamy (Retd.) v. Union of India – Supreme Court Judgment Summary.

 [ISSN 2581-5369]

23. Tal Z. Zarsky, "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making," *Science, Technology, & Human Values*, 2016.

24. Solove, Daniel J., "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, 2006.

25. Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

26. Usha Ramanathan, "Aadhaar: A Tool of Surveillance," *Economic and Political Weekly*, Vol. 46, No. 50, 2011.

27. Reetika Khera, "Aadhaar and Food Security in India," *World Development*, Vol. 106, 2018.

28. Justice A.P. Shah Committee Report on Privacy, 2012.

29. Law Commission of India, Report No. 271: *Human DNA Profiling – A Draft Bill for the Use and Regulation of DNA-Based Technology*, 2017.

30. National Crime Records Bureau (NCRB), *Crime in India Reports*, various years.

31. K.K. Mathew, *Democracy, Equality and Freedom* (Eastern Book Co., 1978).

32. Madhav Khosla, *India's Founding Moment* (Harvard University Press, 2020).

33. Laurence Tribe, "The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier," 1991.

34. Lawrence Lessig, *Code: And Other Laws of Cyberspace* (Basic Books, 1999).

35. Pratap Bhanu Mehta, "The Inner Conflict of Constitutionalism: Judicial Review and the Basic Structure," in *India's Living Constitution*, ed. Zoya Hasan et al., 2002.

36. Richard A. Posner, "Privacy, Surveillance, and Law," *The University of Chicago Law Review*, Vol. 75, 2008.

37. India Justice Report, Tata Trusts and Centre for Social Justice, 2022.

38. Amnesty International Report, *Automated Injustice: How Automated Facial Recognition Systems Undermine Human Rights in India*, 2021.

39. Internet Freedom Foundation (IFF), *Surveillance Reforms in India: Urgent Need for Oversight*, 2023.

40. UN Human Rights Council, *The Right to Privacy in the Digital Age*, A/HRC/27/37, 2014.

*****

 [ISSN 2581-5369]