

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 8 | Issue 4
2025

© 2025 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Between Data and Dignity: Reimagining Biometric Justice for Backward Regions in India with Special Reference to Chhattisgarh

PANKAJ SHARMA¹ AND DR. SHIV KUMAR KURREY²

ABSTRACT

This paper critically investigates how the Criminal Procedure (Identification) Act, 2022 impacts marginalized and backward populations in India, with a case focus on Chhattisgarh. It argues that technology-based laws, if imposed without context-sensitive application, deepen structural injustice. Using the lens of Rawlsian equity and Ambedkarite social democracy, the paper offers a human dignity-centered model for implementing biometric laws in underdeveloped regions.

I. INTRODUCTION

Tech-Centric Legislation and Criminal Justice

The Indian legal environment in recent years has seen a speeding up of transition towards technology-based law enforcement systems. The center of this shift is the Criminal Procedure (Identification) Act, 2022, which exponentially increases the power of the state to gather, retain, and use biometric³ and behavioral information from individuals caught up in criminal proceedings. Seized by the state as a means of technologizing policing and enhancing rates of conviction, the Act represents a wider trend in India's criminal justice system: the integration of technological aids into legal processes without due regard for the social and regional inequalities they engage with.

Chhattisgarh: Tribal Population, Digital Divide, and Under-Policing

These inequalities are nowhere more apparent than in backward and tribal-majority states like Chhattisgarh. Having a sizable Adivasi population, entrenched poverty, and traditionally sparse state presence in the interior areas, Chhattisgarh is a challenging field for the enforcement of surveillance-based laws.⁴ The geography of the state is characterized by digital exclusion, poor legal literacy, and stressed policing systems typically found in conflict

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 Criminal Procedure (Identification) Act, No. 11 of 2022, Acts of Parliament, 2022 (India).

⁴ Shoshana Zuboff, *The Age of Surveillance Capitalism* 153–60 (2019).

areas as a result of the persistent Naxalite insurgency. Therefore, the implementation of a data-heavy and discretion-laden law such as the Criminal Procedure (Identification) Act can potentially reinforce systemic biases and worsen pre-existing vulnerabilities among already marginalized groups.

Research Question: Is Biometric Justice Possible?

This paper therefore poses a basic question: Does biometric justice have the possibility of being made equitable in settings where social, economic, and infrastructural lagness compromises fundamental legal safeguards? In particular, it is seeking to understand how the implementation of the 2022 Act impacts traditionally marginalized communities of Chhattisgarh and if a dignity-based, rights-oriented framework can assist in the more equitable enforcement of such legislation.⁵ By engaging with Rawlsian accounts of justice and Ambedkarite conceptions of social democracy, the article attempts to reimagine what ethical biometric governance can be in areas where law and technology have routinely been used as weapons of domination instead of freedom.

II. SOCIO-LEGAL CONTEXT OF CHHATTISGARH

Chhattisgarh, separated from Madhya Pradesh in 2000, has one of India's largest tribal populations, who make up about 30% of the state's population. The state continues to be economically backward, with chronic poverty, illiteracy, and lack of access to healthcare, education, and judicial facilities. These intersect to create a highly unequal socio-legal context, where marginalization is both systemic and multilayered.⁶

Caste, Poverty, Illiteracy, and Naxalism

The overlap of caste-based discrimination, endemic poverty, and low literacy further exacerbates the vulnerability of Chhattisgarh's Adivasi and Dalit populations. Further added to this mix is the historical occurrence of Naxalite activism in the tribal regions, creating increased militarization, suspicion of the local populace, and confrontational policing culture. Police frequently view entire villages as suspected populations, and security actions in so-called "Red Corridor" areas have seen frequent human rights abuses.

Excessive Rate of False Arrest, Custodial Assault, and Undertrial Crisis

The criminal justice system of Chhattisgarh is characterized by an excessively high rate of false arrests and long pretrial detentions, especially of tribal youth. Human rights

⁵ Soumyabrata Dey, *Police and Tribal Communities in Chhattisgarh: An Uneasy Relationship*, 47 Soc. Change 589 (2017).

⁶ Kumar, Rajiv, *Policing and Tribal Societies in India: A Study of Chhattisgarh* 59–61 (2018).

organizations and government commissions have documented repeated cases of custodial torture, trumped-up charges under strict laws such as the Unlawful Activities (Prevention) Act (UAPA), and the recording of coerced confessions. The under trial crisis is especially acute — numerous accused spend years behind bars without trial, thanks partly to a dearth of legal aid, inadequate investigation, and judicial logjam.⁷

Disproportionate Impact of Invasive Laws on Adivasis

Against this background, enforcement of the Criminal Procedure (Identification) Act, 2022 is of grave concern. The statute provides for the collection of behavioural and biometric data from suspects who are merely accused of crimes, with minimal procedural protections. In a society where illiteracy and fear are endemic, the line between consent and coercion is easily crossed. The Adivasi population, which usually does not enjoy access to counsel or knowledge of their rights, are most vulnerable to such intrusive surveillance practices. The Act, when enforced in such circumstances, risks becoming another instrument of state excess — one that subverts constitutional assurances of equality, freedom, and dignity.

It is therefore crucial to grasp Chhattisgarh's socio-legal context prior to judging the justice implications of biometric legislation.⁸ It is amidst such overlapping layers of marginality that the promise—or danger—of technological legality needs to be assessed.

III. ANATOMY OF THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

The Criminal Procedure (Identification) Act, 2022 represents a drastic increase in the scope of data collection by Indian law enforcement agencies. Substituting the colonial-era Identification of Prisoners Act, 1920, the new legislation empowers the police and prison authorities to acquire extensive amounts of biometric and behavioral information from individuals subjected to criminal investigations. Though the Act is articulated in terms of modernization and scientific policing, its provisions pose fundamental questions about state power versus individual rights—particularly when invoked against socially marginal groups.

Provisions: Extent of "Measurements" and Who Are Targeted

The Act considerably expands the scope of "measurements" to cover fingerprints, palm prints, iris and retina scans, photographs, physical and biological samples, and even behavioral traits like handwriting and signatures. Crucially, it sanctions collection of data not only from convicted individuals but also from those who are arrested for any offence—even if not charged—or those who are merely detained under preventive measures. The coverage under

⁷ Amnesty Int'l, "Denied: Failures in Police Accountability for Torture and Ill-Treatment in India" (2017).

⁸ Harsh Mander & Satendra Singh, Dignity, Rights, and Inclusion: Reflections from India 110–115 (2020).

preventive detention laws and the broad discretion placed in the hands of authorities make the Act eligible for invocation by quite vast sections of the population, especially in areas like Chhattisgarh that are prone to conflict or over-policed.⁹

Absence of Consent Safeguards and Excessive Discretion to Police

Perhaps the greatest concern regarding the Act is the lack of formal consent safeguards. While it enables magistrates to direct the collection of data even from individuals who do not give consent, there are no procedural safeguards clear enough to guarantee voluntariness, particularly for illiterate and marginalized individuals. Further, the law affords disproportionate police discretion, allowing the police to collect and retain sensitive personal information without strong controls or independent scrutiny. In real life, it can result in coercive collection of information, particularly in areas where awareness of legal rights is low and fear of authority is prevalent.¹⁰

Issues of Implementation in Backward Regions

In backward areas such as Chhattisgarh, where the infrastructure of laws is generally weak and public perception of the judiciary is shaky, implementation of such a far-reaching regime of surveillance is fraught with danger. The digital divide—reflected in poor internet connectivity,¹¹ low levels of technological literacy, and weak data protection mechanisms—means that biometric systems are likely to make mistakes, leave people behind, and be abused. Moreover, with informal policing being so widespread, there is a real risk that biometric data will be used to profile whole communities instead of helping to solve individual cases.

The Act's wide reach, minimal procedural safeguards, and reliance on opaque data practices raise pressing concerns about its potential misuse in socially and economically backward regions. A critical assessment of its structure reveals that without meaningful reforms and context-sensitive implementation, it may serve more as a tool of control than of justice—especially for the most marginalized.

IV. PHILOSOPHICAL FOUNDATION: DIGNITY, EQUALITY, AND LEGAL PERSONHOOD

Understanding the implications of the Criminal Procedure (Identification) Act, 2022 in

⁹ Criminal Procedure (Identification) Act, § 2(1)(b).

¹⁰ Janaki Nair, *Women and Law in Colonial India* 88–92 (2009).

¹¹ Jon Truby, *The Right to Privacy and Biometric Identification in Developing Countries*, 41 Hum. Rts. Q. 652, 656 (2019).

marginalized regions like Chhattisgarh requires a normative framework rooted in constitutional values. This section draws on two foundational traditions of justice theory—John Rawls' liberal egalitarianism and Dr. B.R. Ambedkar's social democracy—to argue that any law, particularly one involving bodily and data-based surveillance, must center the dignity and equality of the individual as a legal person.

Rawls' "Difference Principle"

John Rawls, in *A Theory of Justice*, maintains that social and legal disparities are only acceptable if they serve to the advantage of the worst off in society. Referred to as the "difference principle," this suggests that any use of state power—such as biometric policing—should be judged on its effect on the most disadvantaged.¹² Transposing this to Chhattisgarh, where Adivasis, Dalits, and the poor are disproportionately victimized by policing excesses, the Identification Act does not pass the Rawlsian test. Instead of empowering the marginalized, the law can further drive them away and criminalize them under datafication with no safeguards.

Ambedkar's Writings on Justice and State Neutrality

Dr. B.R. Ambedkar's vision of justice was not merely legal but profoundly social. For Ambedkar, the Constitution was an instrument for attaining liberty, equality, and fraternity—principles which needed to be converted into lived experiences. He cautioned against state tyranny over the citizen, particularly in the case of Dalits and Adivasis who were victims of state and caste violence throughout their history.¹³ From this Ambedkarite perspective, biometric legislation—when utilized without participatory consent mechanisms, accountability, and redress—constitutes an extension of the caste and class-based state surveillance, unfulfilling the emancipatory potential of the Constitution.

Dignity as a Lived Constitutional Value (Article 21)

Article 21 of the Indian Constitution provides a right to life and personal liberty, a right that has been widely interpreted by the Supreme Court to encompass the right to privacy, bodily autonomy, and dignity.¹⁴ In *Justice K.S. Puttaswamy v. Union of India* (2017), the Court reiterated that privacy is a part of dignity, and that any intrusion would have to pass the test of necessity, proportionality, and procedural fairness. The Identification Act's ambiguously worded standards, its absence of safeguards, and its open-ended data retention provisions are

¹² John Rawls, *supra* note 4.

¹³ B.R. Ambedkar, *State and Minorities* (1947).

¹⁴ *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

antithetical to this constitutional jurisprudence. For populations in Chhattisgarh already struggling to make claims of personhood within the legal system, the lack of mechanisms based on dignity within the Act reifies structural invisibility and disposability.

Overall, a philosophical critique based on Rawls and Ambedkar forces us to reimagine biometric justice not as technocratic or neutral procedure, but as an intensely political act. It needs to be informed by the moral requirement of safeguarding the dignity, equality, and legal rights of the most vulnerable—concerns that are not currently reasonably secured by the existing law.

V. DIGITAL JUSTICE AND THE EXCLUSION DILEMMA

The story of Indian digital justice has come to focus more and more on technology solutions to structural issues. As much as digital technology holds out the possibilities of efficiency, transparency, and accountability, in practice, it enlarges inequality when applied in areas characterized by infrastructural lack and social marginalization. In Chhattisgarh specifically, the application of biometric systems under the Criminal Procedure (Identification) Act, 2022 stands the risk of solidifying a fresh pattern of digital exclusion that resonates from earlier injustices hidden behind pretenses of modernization.¹⁵

Biometric Mismatch, Infrastructure Gaps, Digital Illiteracy

Perhaps the most critical operational issue with biometric systems is their error-proneness—fingerprint and iris mismatches in particular, higher among manual laborers, elderly populations, and malnourished individuals. These mismatches have the potential to result in wrongful identification, wrongful arrests, and denial of bail or legal rights.¹⁶ In rural Chhattisgarh, where the availability of electricity, internet, and digital literacy is uneven, these technological dependencies become obstacles instead of bridges to justice. The application of biometric devices in sparsely connected or linguistically isolated communities calls into question procedural fairness as well as technological reliability.

Lessons from Aadhaar and Welfare Exclusions

The experience of Aadhaar offers a cautionary lesson. Although brought in as a welfare-promoting tool, Aadhaar-based exclusion from food rations, pensions, and subsidies has been well-documented—mainly from the tribal and rural groups. The exclusions were not because of non-eligibility but because of authentication failures, system glitches, or unawareness.

¹⁵ Ramesh Thakur, South Asia and the Challenge of Data Governance, Asia-Pac. Rev. 29, 31 (2020).

¹⁶ Anjali Singh, Biometric Data and Marginalized Communities: A Comparative Perspective, S. Asian J. Hum. Rts. 9 (2021).

Concomitant trends might occur under the Identification Act, where non-compliance or technical mistakes at the data-gathering stage might result in criminal profiling or exclusion from procedural safeguards, effectively punishing the individual for bureaucratic failure.

Why Technological Legality ≠ Social Legitimacy

The emphasis of the law on legality—i.e., what the state can do under the law—should not blind us to the deeper issue of legitimacy: whether the law, as practiced, protects and honors the dignity of the people it concerns.¹⁷ In areas such as Chhattisgarh, where there is long-standing suspicion of the police and state institutions, legal requirements by themselves cannot produce compliance and trust. Legitimacy demands community engagement, informed consent, and openness—none of which are institutionally inculcated in the Criminal Procedure (Identification) Act. A biometric surveillance top-down imposition without infrastructural preparedness or cultural sensitization generates what scholars describe as a "techno-legal vacuum"—a condition in which laws are there on paper but subvert justice on the ground.

Therefore, though digital justice seeks to democratize access and efficiency, in practice, it threatens to create a new class of digitally dispossessed. Lacking sensitivity to local realities and social context, technological legality could in fact undermine the very basis of democratic governance and constitutional morality.

VI. RIGHTS-BASED CRITIQUE OF THE ACT

While the Criminal Procedure (Identification) Act, 2022 is couched in terms of improving criminal justice efficiency, a closer look from a constitutional and rights-oriented viewpoint indicates grave danger to individual freedom, particularly for vulnerable sections. Lacking sufficient procedural mechanisms, the law undermines fundamental constitutional rights, especially where legal illiteracy, institutional discrimination, and social exclusion run deep, as in states like Chhattisgarh.

Right Against Self-Incrimination (Article 20(3))

Article 20(3) of the Indian Constitution ensures that "no person accused of any offence shall be compelled to be a witness against himself."¹⁸ The courts have also made a distinction between testimonial and nontestimonial evidence like fingerprints or body samples. The widening ambit of "measurements" under the 2022 Act obfuscates this distinction. The addition of biological samples, handwriting, behavioral characteristics, and even DNA is

¹⁷ Sheila Jasanoff, *The Ethics of Invention: Technology and the Human Future* 76–80 (2016).

¹⁸ India Const. art. 20, cl. 3.

likely to raise serious doubts regarding whether or not the collection can be deemed coercive or incriminatory. Without informed consent and legal representation, people—particularly from uncivilized communities—might be forced to furnish proof that can be used against them in contravention of the spirit of Article 20(3).

Procedural Safeguards Missing for Backward Classes

The Act has no specific provisions for differential treatment or special safeguards for such vulnerable groups of persons as Scheduled Tribes (STs), Scheduled Castes (SCs),¹⁹ and economically weaker sections. In a state like Chhattisgarh, where all these communities constitute a significant percentage of such persons targeted by the criminal justice system, such an omission is stark. There is no informed consent in a language known to the accused, no provision for mandatory legal assistance prior to biometric data collection, and no independent oversight provisions. All these lacunae make the Act procedurally arbitrary and discriminatory in operation, though facially neutral in terms.

Role of Legal Aid and Judicial Scrutiny

Legal aid organizations in rural and tribal regions of Chhattisgarh are poorly funded and overburdened. Under such a scenario, the silence of the Act regarding the right to counsel at the data collection point is a serious omission. The lack of judicial oversight in the approval or review of collection, storage, and use of biometric information makes abuses more likely. In contrast to search and seizure activities, which are warrant- or oversight-dependent, biometric extraction according to this legislation may be conducted with minimal accountability. This increases police discretion further and provides scope for targeting arbitrarily or in revenge—especially in Naxal-hit zones or in zones under suspicion from the state.²⁰

A rights-oriented interpretation of the Act thus makes it clear that its design enshrines state authority at the expense of individual agency and procedural justice. The onus of compliance lies overwhelmingly with the least capable of contesting it: the poor, the illiterate, the tribal, and the underrepresented. In the absence of effective legal protections, autonomous monitoring, and context-aware administration, the Criminal Procedure (Identification) Act, 2022 infringes the constitutional principle of equality before law and the right to life with dignity.

VII. COMPARATIVE FRAMEWORKS

To analyze and reimagine India's biometric justice framework—particularly as implemented

¹⁹ Charu Gupta, Gender, Caste and Religious Identities: Resurgent Conflicts in India 151–55 (2018).

²⁰ Arun Mukherjee, Digital Justice: Technology, Law, and Access in Rural India, Int'l J. L. & Tech. 4 (2022).

in backward areas such as Chhattisgarh—it is helpful to gaze beyond the country's shores.²¹ Comparative lessons from the Global South underscore how various legal cultures have reacted to state surveillance, data extraction, and technological policing. Specifically, the South African jurisprudence and Latin American policy resistance provide competing visions that position community dignity, participatory government, and human rights at the forefront of biometric regulation.

South Africa's Ubuntu-Based Privacy Jurisprudence

The constitutional order of South Africa is rooted in the African philosophy of Ubuntu, with its focus on shared humanity, dignity, and communal responsibility. The South African Constitutional Court has formally acknowledged dignity and privacy as fundamental rights closely tied to the historical experiences of racialized surveillance under apartheid. In judgments like *MEC for Education: Kwazulu-Natal v. Pillay* and *Justice Alliance v. President of the Republic*, the court has invalidated state conducts that breached individual dignity in the interest of state efficiency.²²

This Ubuntu-based strategy is as opposed to the Indian model where surveillance legislation such as the Identification Act is made effective with little public discussion or cultural construction. In downtrodden zones such as Chhattisgarh, an Ubuntu-based jurisprudence would prioritize the right of community to dignity and self-determination over their body and data—something India's technocratic legal paradigm seriously misses.

Latin America's Rebellion Against Extractive State Policies on Data

Latin American nations, especially Brazil, Argentina, and Colombia, have witnessed increased opposition against biometric and surveillance regime expansion—popularly termed as "data extractivism." Activists and legal scholars, in drawing on the experience of authoritarianism and social inequalities in these countries, have contended that state acquisition of biometric data from marginalized groups mirrors colonial control and dispossession logics. Civil society organizations in these nations have highlighted prior informed consent, participatory policy-making, and data sovereignty as especially important for Indigenous and Afro-descendant peoples.

For India, and tribal-majority states like Chhattisgarh, these movements highlight the need to position data governance as an issue of social justice rather than technological management.

²¹ *Justice Alliance v. President of the Republic*, [2011] ZACC 23 (S. Afr.).

²² Alicia Ely Yamin, *Power, Suffering, and the Struggle for Dignity: Human Rights Frameworks for Health* 121–28 (2016).

The biometric shift in criminal justice needs to be critically interrogated through the lens of appreciating the intersections of caste, indigeneity, and poverty with digital systems of domination.

These comparative frameworks illustrate that a fair biometric regime needs to move beyond legal formality and address the cultural, historical, and ethical aspects of surveillance. Ranging from Ubuntu's ethics of dignity and relational personhood to the data justice discourse in Latin America, the fundamental insight is this: biometric legislation needs to avoid reproducing the very exclusions they claim to address.

For India's backward areas, importing context-sensitive norms from these international experiments may drive us toward a more democratic, humane, and participatory model of biometric governance that safeguards not just national security, but constitutional morality as well.

VIII. TOWARDS A FRAMEWORK FOR ETHICAL BIOMETRIC GOVERNANCE

The pressing need to revisit the Criminal Procedure (Identification) Act, 2022—particularly in socially and infrastructurally lagging areas such as Chhattisgarh—requires a transition from surveillance-oriented legality to dignity-oriented justice. A framework of ethical biometric governance needs to balance law enforcement objectives with the lived experiences of historically marginalized communities. This section suggests a multi-pronged, participatory model based on democratic accountability, community empowerment, and constitutional values.

Community Consent Models

Consent is the basis for any moral application of biometric data. In remote regions, however, consent needs to transcend personal signatures or thumb prints—it needs to be collective, informed, and culturally situated. Borrowing from environmental law's "free, prior, and informed consent" (FPIC)²³ principle applied in tribal land purchases, the same principles can be extended to biometric governance. Prior to the deployment of biometric devices in tribal hamlets, district administrations must be obliged to consult gram sabhas or local community institutions to elucidate the law, its implications, and channels of redress. In the absence of such deliberative procedures, the state may perpetuate extractive modes of governance.

Role of Local Panchayats, NGOs, and Public Defenders

For ensuring accountability and accessibility, a decentralized monitoring system is critical.

²³ Ministry of Tribal Affairs, Govt. of India, Handbook on Free, Prior and Informed Consent (FPIC), 2019.

Local panchayats—already empowered under the PESA Act in Fifth Schedule areas such as Chhattisgarh—can function as watchdogs for the collection of biometric data. Civil society groups and legal aid clinics should be incorporated into the process formally to deliver real-time support, review of documents, and rights-awareness drives. Public defenders, especially in Naxal-affected areas, need to be trained and equipped to challenge illegal biometric extraction and data abuse in magistrate courts and High Courts.²⁴

State Responsibility in Implementation: Education, Review, Audit

The state has the sole responsibility for ensuring ethical use of biometric technology. This entails:

Digital and Legal Literacy Campaigns: The state has to invest in contact programs—through vernacular languages and community radio—to inform citizens about their biometric rights, the extent of the Identification Act, and redress mechanisms.²⁵

Independent Review Boards: There should be a state-level Biometric Oversight Committee with jurists, technologists, Adivasi leaders, and human rights defenders to audit biometric practices at regular intervals, hear complaints of misuse, and provide recommendations.

Annual Transparency Audits: Public reporting requirements on the collection, storage, access, and deletion of data will place pressure for legal behavior. Special categories must note the number of marginalized people impacted and the character of police action.

A moral biometric governance framework has to turn the existing power relation on its head, and center around the rights of the most disadvantaged. In a state such as Chhattisgarh—characterized by development lag, police excess, and adivasi resistance—any roll-out of a surveillance law has to cross higher standards of accountability, popular legitimacy, and constitutional compliance.²⁶

Finally, the future lies not in discarding technology, but re-politicizing it with participatory justice. Only in this way can India's biometric future be both effective and just.

IX. CONCLUSION

The movement towards a digitized criminal justice regime in India, as exemplified by the Criminal Procedure (Identification) Act, 2022, is profound and deeply problematic in terms of ethics and the constitution—especially in states like Chhattisgarh, where there is historical injustice, infrastructural backwardness, and tribal marginalization. This paper has attempted to

²⁴ Panchayats (Extension to Scheduled Areas) Act, 1996, No. 40, Acts of Parliament, 1996 (India).

²⁵ Law Comm'n of India, Report on Biometric Identification and Privacy Safeguards, No. 277, at 44 (2021).

²⁶ Niraja Gopal Jayal, *Citizenship and Its Discontents: An Indian History* 203–210 (2013).

prove that technology-driven laws, without a contextual and dignity-embracing orientation, have the potential to reaffirm, not rectify, structural disparity.

The prevailing discourse of biometric rule-making tends to favor state effectiveness and crime management over citizens' freedom and social justice. Yet, the prism of Rawlsian fairness and Ambedkarite social democracy discloses that it is not just procedure but outcome that is concerned with justice—particularly of the most disadvantaged. Understood in this way, surveillance legislation needs to be recast not only on the basis of legality, but on the basis of legitimacy, solidarity, and constitutional morality.²⁷

To that effect, special rules of implementation for backward and tribal areas need to be enacted. These could involve: compulsory consultations at the community level, added legal protections, culturally sensitive consent procedures, and regular scrutiny by independent, representative organizations. The aim cannot be to exclude such areas from technological reforms, but to make them ensure technology follows justice—not vice versa.

This article invokes a turn toward what can be called "affirmative surveillance"—a rights-oriented, inclusive model of biometric rule in which the state's investigation arm is weighed against its responsibility to ensure dignity, curtail abuse, and empower the marginalized. Instead of perceiving biometric technologies as apolitical tools of law and order, policymakers need to see them as potent socio-political technologies that owe their legitimacy to their democratic moorings.²⁸

In short, the task is not merely one of regulating biometric data, but of situating it within a constitutional imagination of justice that upholds both human dignity and technological humility. Anything less would risk widening the gap between data and dignity—and forfeiting the promise of a future in which justice is not only digital, but also fundamentally democratic.

²⁷ *ibid*

²⁸ Upendra Baxi, *The Future of Human Rights* 212–214 (2008).

X. BIBLIOGRAPHY

1. Baxi, Upendra. *The Future of Human Rights*. Oxford University Press, 2008.
2. Balkin, Jack M. "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society." *New York University Law Review*, vol. 79, no. 1, 2004, pp. 1–55.
3. Baviskar, Amita. *In the Belly of the River: Tribal Conflicts Over Development in the Narmada Valley*. Oxford University Press, 1995.
4. Bhattacharya, Shuvendu. "Biometric Surveillance and the Right to Privacy in India." *Economic & Political Weekly*, vol. 52, no. 28, 2017.
5. Chandrachud, Abhinav. "The Aadhaar Judgment: Privacy, Surveillance, and the Indian Constitution." *The Indian Journal of Constitutional Law*, 2018.
6. Choudhury, Anindita, et al. *Law and Society in Modern India*. Routledge, 2017.
7. Cohen, Julie E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press, 2019.
8. De, Prabir. "Surveillance and the Marginalised: Challenges in India's Security Architecture." *Journal of Asian Security and International Affairs*, vol. 3, no. 1, 2016.
9. Dey, Soumyabrata. "Police and Tribal Communities in Chhattisgarh: An Uneasy Relationship." *Social Change*, vol. 47, no. 4, 2017.
10. Ganguly, Sumit. *India's Foreign Policy: Retrospect and Prospect*. Oxford University Press, 2015.
11. Gandhi, Raj. "Digital Identity and Exclusion: A Case Study of Aadhaar in India." *Harvard Law & Policy Review*, 2020.
12. Gupta, Charu. *Gender, Caste and Religious Identities: Resurgent Conflicts in India*. Routledge, 2018.
13. Haggerty, Kevin D., and Richard V. Ericson. *The New Politics of Surveillance and Visibility*. University of Toronto Press, 2006.
14. Harris, John. *Enhancing Human Dignity: A Framework for Ethical Biometric Use*. Cambridge University Press, 2021.
15. Jasanoff, Sheila. *The Ethics of Invention: Technology and the Human Future*. W.W. Norton & Company, 2016.

16. Jayal, Niraja Gopal. *Citizenship and Its Discontents: An Indian History*. Harvard University Press, 2013.
17. Joseph, Mathew. "Constitutional Morality and the Promise of Equality." *Economic & Political Weekly*, vol. 54, no. 9, 2019.
18. Kaur, Ravinder. *The Indian Media: Decoding the Role of Digital Surveillance*. Sage Publications, 2019.
19. Khanna, Rajiv. "The Criminal Procedure (Identification) Act, 2022: A Rights-Based Review." *Indian Journal of Human Rights*, 2023.
20. Kumar, Rajiv. *Policing and Tribal Societies in India: A Study of Chhattisgarh*. Oxford University Press, 2018.
21. Law Commission of India. *Report on Biometric Identification and Privacy Safeguards*, 2021.
22. Mander, Harsh, and Satendra Singh. *Dignity, Rights, and Inclusion: Reflections from India*. Routledge, 2020.
23. Menon, Nivedita. *Recovering Subversion: Feminist Politics Beyond the Law*. University of Illinois Press, 2015.
24. Mukherjee, Arun. "Digital Justice: Technology, Law, and Access in Rural India." *International Journal of Law and Technology*, 2022.
25. Nair, Janaki. *Women and Law in Colonial India*. Kali for Women, 2009.
26. Nussbaum, Martha C. *Creating Capabilities: The Human Development Approach*. Harvard University Press, 2011.
27. Pal, M., and S. Rao. "Biometric Surveillance and Privacy Concerns in India." *Journal of Information Policy*, 2019.
28. Rajagopal, Balakrishnan. *International Law from Below: Development, Social Movements and Third World Resistance*. Cambridge University Press, 2003.
29. Sen, Amartya. *The Idea of Justice*. Harvard University Press, 2009.
30. Singh, Anjali. "Biometric Data and Marginalized Communities: A Comparative Perspective." *South Asian Journal of Human Rights*, 2021.
31. Thakur, Ramesh. "South Asia and the Challenge of Data Governance." *Asia-Pacific Review*, 2020.

32. Truby, Jon. "The Right to Privacy and Biometric Identification in Developing Countries." *Human Rights Quarterly*, vol. 41, no. 3, 2019.
33. Veeraswamy, Lakshmi. "Technology, Law, and Social Exclusion: The Case of Aadhaar." *Journal of Social Inclusion Studies*, 2018.
34. Walker, Margaret Urban. *Moral Understandings: A Feminist Study in Ethics*. Oxford University Press, 2007.
35. World Bank. *Digital Divides and Socioeconomic Inequality in India*, 2022.
36. Yamin, Alicia Ely. *Power, Suffering, and the Struggle for Dignity: Human Rights Frameworks for Health and Why They Matter*. University of Pennsylvania Press, 2016.
37. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. PublicAffairs, 2019.
