Page 2858 - 2873 **DOI:** *https://doij.org/10.10000/IJLMH.119381*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Right to Privacy: An Analytical Study of Justice D.Y. Chandrachud's Dissent in the Aadhaar Judgment

VAGHELA ABHIJEETSINH RANDHIRSINH[1] AND PRIYANKA TAKTAWALA[2]

ABSTRACT

Hon'ble Mr. Justice Dr. Dhananjaya Yashwant Chandrachud's dissent in the Aadhaar verdict offers a convincing examination of the ethical, legal, and constitutional implications of Bharat's biometric identification scheme. While the majority upheld the constitutionality of Aadhaar, his dissent challenges the basic assumptions of biometric accuracy, privacy, and government monitoring. He claims that the Aadhaar framework disproportionately affects marginalised individuals, leading to systematic exclusion and perhaps serving as a tool for state control rather than merely identification. His dissent exposes Aadhaar's reliance on unsupported claims about its efficacy and draws attention to its constitutional problems. He raises concerns about the basic right to privacy, data security vulnerabilities, and the unjust burden placed on individuals to verify their identity. In addition, he criticised the government for failing to demonstrate a sufficient state interest, which the proportionality test requires, making the mandatory nature of Aadhaar unlawful. This study critically examines Justice Chandrachud's dissent and its implications for digital governance, privacy jurisprudence, and constitutional interpretation. This study argues that his dissent is a crucial line of defence against the state's unchecked exploitation of technology to expand its power. By examining his assertions on exclusion, surveillance, and judicial excess, this study contributes to the broader discussion on digital rights and constitutional safeguards against governmental overreach.

Keywords*: Aadhaar Framework; Justice Chandrachud's dissent; Biometric Identification Scheme; Constitutional Implications; Right to Privacy; Data Security Vulnerabilities*.

I. INTRODUCTION

'Constitutional guarantees cannot be subject to the vicissitudes of technology'.

- **Hon'ble Mr. Justice Dr. D.Y. Chandrachud**[3]

[1] Author is a student at Unitedworld School of Law, Karnavati University, India.
[2] Author is an Assistant Professor at Karnavati University, Unitedworld School of Law, India.
[3] Chandrachud J., dissenting, paragraph 269, Justice K.S. Puttaswamy (retd.) & Another *vs.* Union Of India & Others, 2015 INSC 559

 [ISSN 2581-5369]

Bharat's legal debate on privacy, state authority, and digital governance underwent a sea change with the Aadhaar ruling. Even though the Supreme Court ruled in favour of the legitimacy of the Aadhaar Act, Justice Chandrachud's dissent is notable for its strong criticism of the government's biometric initiative. His opposition highlights the constitutional, moral, and practical shortcomings of Aadhaar and cautions against the degradation of basic rights in the sake of technological efficiency.

This study's goal is to examine Justice Chandrachud's dissent and evaluate its consequences for state surveillance, legal proportionality, and privacy law. This study attempts to draw attention to the weaknesses in Aadhaar's legal and structural framework and their wider effects on constitutional rights by critically analysing his claims. The dearth of academic discussion of the dissent as a fundamental criticism of Aadhaar represents a substantial research gap. Legal assessments have mostly concentrated on the majority decision, but little attention has been paid to how the dissent calls into question the legitimacy of Aadhaar from an ethical, legal, and factual standpoint. By situating the dissent within the larger context of constitutional law and human rights, this research aims to close that gap.

An examination of Aadhaar's operational shortcomings, legal underpinnings, and constitutional issues brought up in the dissent are all included in the study's purview. It also looks at how the Aadhaar ruling has affected discussions about digital identities throughout the world. The lack of factual data on post-judgment exclusions and the dynamic nature of Aadhaar's implementation are among the drawbacks, though, and might pose constitutional issues in the future. This study aims to critically assess Justice Chandrachud's dissent, contending that his logic serves as an essential check on the unbridled use of technology by the state. In order to place his dissent within Bharat's developing constitutional jurisprudence, the study analyses his arguments on privacy, data security, proportionality, and exclusion. According to the study, his dissent provides a foundation for future legal and legislative discussions about basic rights and biometric governance.

'Even in the absence of article 21 in the Constitution, the State has got no power to deprive a person of his life or personal liberty.'

- **Hon'ble Mr. Justice H.R. Khanna**

II. QUIRKY BIOMETRICS RELIANCE?

The majority ruling in the Aadhaar case takes many factual assumptions that either weren't sufficiently substantiated by evidence or those taken from a PowerPoint presentation made by the chairperson of the Unique Identification Authority of Bharat (UIDAI) before the court

during court proceedings[4]. Most people think monitoring is illegal and that profiling is bad. Based on its factual findings, however, it concludes that the Aadhaar framework does not support either one. Section 7 survives as an active law because the fundamental belief about biometric distinctiveness serves as its primary foundation[5]. Justice Chandrachud directly challenges the basic notion which underpins this approach. This section states there will be inevitable mistakes whenever biometrics are implemented. According to expert, simulation toes the uniqueness of fingerprints in forensic science due to a lack of absolute definitive evidence[6].

Just as many claim that Aadhaar collects little data, the majority also admits that data minimisation is a fundamental norm. The majority further affirms that the proposed proportionality requirement of law is met, but maintains that the *'uniqueness'* of biometric authentication delivers apposite recipients. The difficulty with their arguments isn't merely what the law requires of the Aadhaar system as the Justice Chandrachud had in mind; it is deeper than that and goes to their fundamental differences about the actual world the Aadhaar system operates in. This distinction must be understood because, while judges can make and change laws, the facts are out of judicial interpretation. For instance, this study disagrees about whether Justice Chandrachud or the majority is correct in sanctioning prior actions under Section 59 of the Aadhaar Act. But uniqueness of biometrics or of exclusion has to be only one thing, the other has to be wrong[7]. If its factual claims are invalid, the validity of the Majority's decision is seriously in doubt are false.

Justice Chandrachud differentiates himself from the other judges by using academic studies alongside the provisions in the Aadhaar Act that allow biometric information updates. Scientists have developed contradictory theories about biometric truth which ultimately impacts the judgment[8]. According to the Majority, the unique fingerprint-based system both functions flawlessly and promises elimination of duplicate entries. The fundamental premise in the course of majority arguments simplifies their case presentation. By being distinctive Aadhaar enables precise beneficiary identification which verifies both Section 7 and Section 139AA retention. Official circulars can substitute for discounting anecdotal evidence of exclusion because its

[4] Mehal Jain, "Live Law" *Live Law* (March 22, 2018) <https://www.livelaw.in/first-sc-allows-power-point-presentation-hearing-uidai-present-ppt-technicalities-aadhaar-2-30pm>.

[5] "Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)" (*Thales Group*) <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data>.

[6] Page M, Taylor J and Blenkin M, "Uniqueness in the Forensic Identification Sciences—Fact or Fiction?" (2010) 206 Forensic Science International 12 <https://doi.org/10.1016/j.forsciint.2010.08.004>

[7] "Biometrics and Privacy – Issues and Challenges – Office of the Victorian Information Commissioner" <https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/>.

[8] Kini A and Law L, "Live Law" *Live Law* (April 13, 2019) <https://www.livelaw.in/top-stories/jamaica-sc-declares-nids-unconstitutional-144256>.

validity remains unproven. Assessment dedicates more time to determining biometric authorizations' impact on public goals state containment use of invasive security instruments. According to Justice Chandrachud, technological systems carrying out biometric procedures have acknowledged their capacity to produce erroneous outcomes. The queries focus on both moral just and practical implications which occur when using biometric data for delivering essential services[9]. Justice Chandrachud's factual disagreements with the Court majority extend far past Aadhaar program regulations. The disputes expose critical matters about digital rights found within the Bharatiya constitution.

Protection of constitutional guarantees demands advanced understanding of technological interactions. The uniqueness assumption used by the majority creates a simplistic understanding of how the Aadhaar system solves benefit distribution and identification verification issues. Strict industrial enforcement by the State becomes possible without proper oversight when the court pronounces an unyielding support for Aadhaar's authentication system[10]. A democratic society stands responsible for prioritizing individual rights above all else so this situation is profoundly unsettling. According to Justice Chandrachud's dissent, the protection of constitutional rights becomes vulnerable when technological efficiency justifies their compromise thus maintaining continuous observation of governmental technology use becomes crucial[11].

III. UNSUBSTANTIATED EVIDENCE AND ITS AUTHORITY

Justice Chandrachud disagrees with the Majority's use of unsubstantiated statements presented before the court. Any legal decision must derive from verifiable facts specifically when addressing issues with big societal impacts and primary right protection. Upstanding legal structures need all significant facts to be thoroughly assessed before establishing their framework[12]. When a court rejects facts presented by petitioners this action threatens to undermine the validity of its legal decision. Justice Chandrachud emphasizes important problems regarding operating based on technologically imperfect systems in his dissenting

[9] Barton G, Lee NT and Resnick P, "Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms" *Brookings* (May 22, 2019) <https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>.

[10] "The Top 7 Dissents of Justice D.Y. Chandrachud - Supreme Court Observer" (*Supreme Court Observer*, November 25, 2024) <https://www.scobserver.in/journal/the-top-7-dissenting-judgements-of-justice-d-y-chandrachud/>.

[11] Law L, "Live Law" *Live Law* (September 26, 2018) <https://www.livelaw.in/breaking-aadhaar-project-wholly-unconstitutional-landmark-disssent-by-justice-chandrachud/>.

[12] Dixon P, "A Failure to 'Do No Harm' -- India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S." (2017) 7 Health and Technology 539 <https://pmc.ncbi.nlm.nih.gov/articles/PMC5741784/>.

 [ISSN 2581-5369]

judgment. The issue of flawed biometric system operation creates extensive concerns since this affects communities already facing challenges with accessing needed medical services. Alongside the Aadhaar program other uses of biometric data have raised ethical problems[13]. Sensor identification monitoring combines with law enforcement measures that determine access to essential services. The way technology is developing necessitates the legal enforcement of both moral integration systems and individual privacy measures[14]. Studies examining this relationship gain critical influence through Justice Chandrachud's dissent which appeared during the Aadhaar case proceedings. His factual disputes with the Majority make clear the importance of understanding technology boundaries in judgment making that relies on verifiable evidence. The Aadhaar ruling demonstrates why modern societies need persistent thought about technology ethics in relation to personal rights protection[15].

IV. SURVEILLANCE AND THE AADHAAR ACT

Comprehensive surveillance alongside profiling have become primary topics of debate during the discussion about the Aadhaar decision. Justice Chandrachud presents a clear opposite view from the legal views stated within the majority decision[16]. He considers the present Aadhaar framework enables efficient surveillance activities which include profiling operations. This study validates his position through presented legal rules combined with actual scenarios.

Regulation 17[17], grants requesting institutions specific authority to maintain biometric data for brief intervals. Under this rule unauthorized parties achieve access and surveillance abilities to target individuals creating quick concerns that it could be misused. In his dissent, Justice Chandrachud highlights that metadata enables the ability to track location and behaviour by following IP addresses. Security issues become worse because third-party suppliers have access to the Aadhaar database potentially creating vulnerability and abuse opportunities. He identifies connected Aadhaar databases as an essential concern regarding system security. When Aadhaar links to multiple systems it becomes the essential cohesive element which unites dispersed

[13] Pratt MK, "Biometric Privacy and Security Challenges to Know" (*Search Security*, November 19, 2024) <https://www.techtarget.com/searchsecurity/tip/In-biometrics-security-concerns-span-technical-legal-and-ethical>.

[14] "Using Technology Standards to Support Data Privacy - IEEE Digital Privacy" <https://digitalprivacy.ieee.org/publications/topics/using-technology-standards-to-support-data-privacy>.

[15] Karn R, "Constitutionalism in the Age of Technology" (*Taxmanagementindia.com (a Unit of MS Knowledge Processing Pvt. Ltd.)*, July 24, 2024) <https://www.taxmanagementindia.com/visitor/detail_article.asp?ArticleID=12819>.

[16] Yashawardhana, "Indian Constitution: A Living Document for the Digital Age - The Sunday Guardian Live" (*The Sunday Guardian Live*, January 25, 2025) <https://sundayguardianlive.com/opinion/indian-constitution-a-living-document-for-the-digital-age>.

[17] Kasiva KS &, "Regulation of Biometric Data under the DPDP Act" (*King Stubb & Kasiva*, November 2, 2023) <https://ksandk.com/data-protection-and-data-privacy/regulation-of-biometric-data-under-the-dpdp-act/>.

 [ISSN 2581-5369]

information regardless of whether systems belong to governmental entities or private organizations[18]. Aadhaar usage for any objective presents two main risks because information from multiple databases becomes linked. The logic demonstrates how information variables which were formerly unimportant build a fundamental connection. The court discovered evidence showing that Aadhaar enables intrusive life reconstruction which establishes its nature as a surveillance instrument.

According to Justice Chandrachud, the need to link Aadhaar to various programs creates potential identity-based discrimination. He illustrates his point with a compelling portrayal of a persons whose caste has been discriminated and performs manual scavenging[19]. After being rescued this person needs to associate their Aadhaar number with proper programs for benefit access. The link between individuals and manual scavenging functions through this requirement as a permanent registry creating more institutionalized prejudice and social shame. In principle Section 2(k) of the Aadhaar Act blocks sensitive race and religious data entry in the Central Identities Data Repository (CIDR) yet the current practice of Aadhaar database linking achieves identical outcomes according to Dr. Thondoo[20]. A spurious benefit delivery approach demands Aadhaar database matching which results in adding new value to previous administrative surveillance methods[21]. The fundamental disagreement about Aadhaar's design principles separates Justice Chandrachud from the majority which reasoned that profiling and monitoring do not occur in Aadhaar because no technical method exists to merge database components. Justice Chandrachud demonstrates in his views that Aadhaar's connection to multi-database platforms creates a large network of joined information databases which defeats the notion of data silos[22]. This contradiction about basic information stands above any distinction between multiple legal viewpoints. The outcome of this dispute carries important consequences because one interpretation of Aadhaar capabilities must be accurate. The core reasons supporting Aadhaar's legal position crumble when majority declarations about data silo inability to merge

[18] Nemitz P, "Constitutional Democracy and Technology in the Age of Artificial Intelligence" (2018) 376 Philosophical Transactions of the Royal Society a Mathematical Physical and Engineering Sciences 20180089 <https://doi.org/10.1098/rsta.2018.0089>.

[19] The Hindu Bureau, "Poverty, Caste-Discrimination at the Root of Manual Scavenging, Reveals Study" (*The Hindu*, January 7, 2023) <https://www.thehindu.com/news/national/tamil-nadu/manual-scavenging-study-reveals-poverty-caste-discrimination-at-its-roots/article66350006.ece>.

[20] Kumar A, "Policy for Protecting Personal Data of Aadhaar Number Holders" (2024) <https://www.creditaccessgrameen.in/wp-content/uploads/2024/05/CreditAccess-Grameen_Protecting_Personal_data_of_Aadhaar_Number_Holders_Policy_01-April_2024.pdf>.

[21] "Operation Model - Unique Identification Authority of India | Government of India" (*Unique Identification Authority of India | Government of India*) <https://uidai.gov.in/en/ecosystem/authentication-ecosystem/operation-model.html>.

[22] Bhatia G, "The Aadhaar Judgment: A Dissent for the Ages" (*Constitutional Law and Philosophy*, October 3, 2018) <https://indconlawphil.wordpress.com/2018/09/27/the-aadhaar-judgment-a-dissent-for-the-ages/>.

prove to be false. The factual dispute between Aadhaar stakeholders extends its effects throughout levels which surpass the boundaries of this specific digital identity program[23].

When one read Justice Chandrachud's dissent one shall appreciate how essential it is to develop advanced insights regarding technology engagement with constitutional rights[24]. Judicial decision-making requires evidence which becomes a major point in Justice Chandrachud's dissenting opinion. To maintain the strength of a legal framework all relevant information needs proper evaluation. The Majority weakens the integrity of their decision when they do not evaluate evidence presented by the petitioners. In a program with major abuse potential and high stakes Justice Chandrachud correctly highlights the critical need for rigorous evidence standards.

The ethical acceptability of using biometrics for verification purposes during the Aadhaar implementation process stands at the core of the program's political dispute. Detection defects in advanced technology result in substantial concerns according to the opposing stance presented by Justice Chandrachud during his dissenting statement[25]. As technology grows advanced citizens must evaluate the impacts of employing biometric information whether for public surveillance programs or law enforcement operations as well as service entry. The dissenting opinion of Justice Chandrachud in the Aadhaar case reveals how essential deep analysis of constitutional rights related to technology has become. Legal rulings need verifiable facts as base because factual disputes between Justice Chandrachud and the Majority show that technology has clear barriers[26]. The dispute between Justice Chandrachud and the Court's majority about profiling and monitoring Aadhaar drives wider disagreements which exist throughout current society.

V. EXAMINATION OF PRIVACY AND PROPORTIONALITY

A comprehensive evaluation of privacy rights through present-day technological development emerged as the main focus of legal scrutiny during the Aadhaar ruling dispute. The core disagreement between minority and the majority centres around their different views on the

[23] "Understanding Privacy in the Digital Age - IEEE Digital Privacy" <https://digitalprivacy.ieee.org/publications/topics/understanding-privacy-in-the-digital-age>.

[24] Pato JN and Millett LI, "Cultural, Social, and Legal Considerations" (*Biometric Recognition - NCBI Bookshelf*, 2010) <https://www.ncbi.nlm.nih.gov/books/NBK219893/>.

[25] Bhargava A and others, "Supreme Court Upholds the Constitutionality of Aadhaar Albeit Conditionally" (*Lexology*, October 1, 2018) <https://www.lexology.com/library/detail.aspx?g=2245f54a-6588-44d4-9f70-5fda69f2b3e4>.

[26] "Constitutionality of Aadhaar Act: Judgment Summary - Supreme Court Observer" (*Supreme Court Observer*, June 20, 2023) <https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/#:~:text=Chandrachud%20J's%20Dissenting%20Opinion&text=DY%20Chandrachud%20J%20delivered%20the,passed%20as%20a%20Money%20Bill.>.

proportionality of Section 7 of the Aadhaar Act and how to approach biometric data collection. This section carefully evaluates their claims and details their variable stands regarding both proportionality and privacy with effects on liberty rights.

In his dissent Justice Chandrachud establishes essential points regarding individual privacy concerns related to biometric data right at the start. Justice Chandrachud maintains our rights to biometric privacy cover iris scans along with fingerprints. This privacy concern handling by The Majority represents an opposite view from the basic stance of Justice Chandrachud's dissenting opinion. According to the majority decision people have no stronger privacy rights regarding their biometric data even though this information frequently has many reasons for collection. A failure to recognize self-determination rights as well as physical integrity value leads to problematic assessments. Justice Chandrachud uses his dissenting opinion to explain how biometric information contains powerful privacy elements which stems from both physical body integrity and personal information ownership rights. He stays clear of two crucial mistakes made by the majority; the Supreme Court misapplied the U.S. "*reasonable expectation*" doctrine while blending terms between "*minimal information collected*" and "*minimal privacy interference*"[27]. He maintains that the distinctive privacy element tied to biometric information remains unaffected regardless of how many times officials gather it. He claims the evaluation of Aadhaar system requires assessment based on this criterion and outlines major privacy violations which stem from three key factors which include procedural permission lessness in the Act alongside substantial dataset exposure and wide-reaching interpretations of biometrics[28]. Other privacy issues include customer challenges in updating their biometric content while lacking access to their record details.

VI. SECTION 7

Justice Chandrachud recognises that the Aadhaar Act, and in particular Section 7, seeks to achieve a valid State goal, i.e., the goal of enhancing benefit distribution efficiency requires a solution that advances past the core privacy issues. The program fails to pass the proportionality test because it ignores proper weighing between state-motivated goals against individual rights obligations[29]. According to Justice Chandrachud laid proportionality test requires states to

[27] "Expectation of Privacy" (*LII / Legal Information Institute*) <https://www.law.cornell.edu/wex/expectation_of_privacy>.

[28] "Security Guidelines for Use of Biometric Technology in E-Governance Projects" (Government of India, Ministry of Electronics & Information Technology, New Delhi-110003 2017) NeST-GDL-BIO.01 Version 1.0 <https://egovstandards.gov.in/sites/default/files/2021-07/Security%20Guidelines%20for%20use%20of%20Biometric%20Technology%20in%20e-Governance%20Projects.pdf> accessed January 29, 2025.

[29] Indulia B, "Aadhaar Act, 2016 Constitutional Not Violative of Right to Privacy; Linking of Aadhaar with Mobile

respect fundamental rights as they implement welfare programs through informed determination of the appropriate extent, they should interfere with privacy rights and corresponding access to dignity choices and fundamental benefits. The analysis shows three fundamental discrepancies in how Justice Chandrachud approaches proportionality compared to the rest of the court. The majority sees minimal violations that protect privacy and dignity so it keeps the threshold low for state interference. Justice Chandrachud emphasizes that privacy violations deserve serious acknowledgement because they should not be treated indifferently. According to his view, the government should offer compelling evidence to justify breaching privacy in similar situations. Furthermore, the Majority chooses to dismiss potential difficulties for fundamental rights access since it deems biometric authentication system flawless[30].

Aadhaar deployment provides entitlement benefits according to the majority judges who view this as an advantage compared to viewing it as a shortfall effect. Because the real risks from Aadhaar's deployment exceed its presumed benefits. The final step of the decision relies on an evaluation that demonstrates significant welfare gains against privacy damage because its system functions based on specific targeting which enables enhanced welfare programs.

VII. WELFARE AND GOVERNANCE

As part of his dissent, Justice Chandrachud argues that the State should establish proof regarding alternative non-intrusive biometric technology options[31]. Against the view of the Majority the dissenting judge asserted the petitioners' insufficient evidence proving alternative authentication procedures. Justice Chandrachud turns the burden on its head and demands the State establish why their infringement of individual rights exists. Justice Chandrachud reveals the new order, when he argues that through Aadhaar every citizen becomes a suspected criminal while State authorities lack reasonable grounds for investigations. Aadhaar proves to be unjustified against its intended purposes primarily because no reasonable assumptions or previous court rulings support it. The program suffers weaker validity due to the UIDAI's lack of responsibility and insufficient authentication failure procedures and the absence of adequate verification systems[32].

Phone Number, Bank Account Not Mandatory: SC | SCC Times" (*SCC Times*, May 21, 2019) <https://www.scconline.com/blog/post/2018/09/27/aadhar-act-2016-constitutional-not-violative-of-right-to-privacy-linking-of-aadha-with-mobile-phone-number-bank-account-not-mandatory-sc/>.

[30] "A PRIMER ON BIOMETRICS FOR ID SYSTEMS | Identification for Development" <https://id4d.worldbank.org/id-biometrics-primer>.

[31] U.S. Department of Homeland Security, U.S. Department of Justice, and White House Office of Science and Technology Policy, "BIOMETRIC TECHNOLOGY REPORT" (2024) <https://www.dhs.gov/sites/default/files/2024-12/24_1230_st_13e-Final-Report-2024-12-26.pdf>.

[32] "The Ryder Review" <https://www.adalovelaceinstitute.org/report/ryder-review-biometrics/>.

Justice Chandrachud advocates for a complete regulatory system for managing how biometric information is utilized. People express profound concerns about misuses and privacy rights deterioration based on the fact that Aadhaar does not clearly obligate rules for how to utilize the program in different contexts. A State bears moral duties to maintain rights protection and technical systems implementation must preserve privacy along with human dignity. Justice Chandrachud warns that errors in biometric systems create dangerous risks primarily for disadvantaged populations who need medical attention. Biometric data raises ethical dilemmas in multiple entities apart from the Aadhaar program[33]. The necessity of comprehensive judicial examinations of basic rights violations is strongly argued by Justice Chandrachud's disagrees.

Since biometric data collection admits[34] wide extent, the law needs to operate relentlessly while defending individual rights. Courts need to evaluate State arguments with special attention because power misuse can become a reality. The study by Justice Chandrachud advocates for a complete regulatory system for managing how biometric information is utilized. People express profound concerns about misuses and privacy rights deterioration based on the fact that Aadhaar does not clearly obligate rules for how to utilize the program in different contexts[35]. Aadhaar program faces opposite criticism because of moral consequences related to biometric data collection. A State bears moral duties to maintain rights protection and technical systems implementation must preserve privacy along with human dignity according to Justice Chandrachud's dissenting statement. He warns that errors in biometric systems create dangerous risks primarily for disadvantaged populations who need medical attention. Biometric data raises ethical dilemmas in multiple entities apart from the Aadhaar program[36]. The necessity of comprehensive judicial examinations of basic rights violations is strongly argued by Justice Chandrachud's dissent. Every argument raised at the state level needs strict examination due to potential power exploitation problems.

VIII. DISCRIMINATION

Justice Chandrachud that biometric technology often stands against the wrongly denial presented in the majority decision. The divergent understanding extends beyond interpretation

[33] Strom K, RTI International, and Police Executive Research Forum, "Research on the Impact of Technology on Policing Strategy in the 21st Century" (National Institute of Justice 2016) report 251140 <https://www.ojp.gov/pdffiles1/nij/grants/251140.pdf>.

[34] Smith M and Miller S, "The Ethical Application of Biometric Facial Recognition Technology" (2021) 37 AI & Society 167 <https://pmc.ncbi.nlm.nih.gov/articles/PMC8042627/>.

[35] Kindt EJ, *Privacy and Data Protection Issues of Biometric Applications* (2013) <https://doi.org/10.1007/978-94-007-7522-0>.

[36] Turley J and The George Washington University Law School, "ANONYMITY, OBSCURITY, AND TECHNOLOGY: RECONSIDERING PRIVACY IN THE AGE OF BIOMETRICS," vol 100 (2020) <https://www.bu.edu/bulawreview/files/2021/01/TURLEY.pdf>.

 [ISSN 2581-5369]

flexibility because it reflects fundamental disagreements about Aadhaar system capabilities together with their potential utility against disadvantaged population groups. The Connection Between Discrimination and Exclusion in a commentary shows how biometric authentication creates social justice problems which extend past technical system failures. According to his analysis, biometric devices produce a negative impact on exclusion which particularly harms disadvantaged and marginalized populations. The way the Aadhaar system operates produces fundamental injustices because marginalized groups suffer most from technical difficulties affecting biometric authentication.

He emphasis the "*digital poorhouse*" described by Virginia Eubanks to make his point[37]. The study conducted by Eubanks reveals that people who start from a position of disadvantage sustain a higher percentage of the adverse effects that result from technical solutions[38]. This core observation delivers power in Aadhaar as the system prioritizes raw biological measures that prove balanced disparities worse becoming a reality. Justice Chandrachud warns about inadequate adoption oversight of modern systems under which "*individual destinies must not rest upon weak technological solutions*" according to his final analysis[39].

Actual statistics found within the Economic Survey of 2016–17 and official reports from Andhra Pradesh experimental projects[40] reinforce his arguments. He strengthens his point by relying on findings from grassroots academics such as Jean Dreze and Reetika Khera to show how significantly many people have ended up unable to access services because of Aadhaar system requirements[41]. The Majority fails to address the exclusion problem seriously by only maintaining that alternate IDs should get recognition from the Attorney-General while using a Circular that supposedly solves these problems but ignores evidence-based analysis along with the court's own orders. By depending solely on promises of fair interpretation while ignoring fundamental biometric system structural issues the Majority undermines the validity of the Aadhaar Act. The dissent explains how technical problems requiring resolution should have come first before implementing the Aadhaar program[42]. He observes that connectivity problems

[37] Gordon F, "Virginia Eubanks (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: Picador, St Martin's Press" [2019] Law Technology and Humans 162 <https://doi.org/10.5204/lthj.v1i0.1386>.

[38] Zajko M, "Artificial Intelligence, Algorithms, and Social Inequality: Sociological Contributions to Contemporary Debates" (2022) 16 Sociology Compass <https://doi.org/10.1111/soc4.12962>.

[39] Sharma P and Law L, "Live Law" *Live Law* (August 1, 2022) <https://www.livelaw.in/top-stories/judicial-institutions-must-shed-the-resistance-to-adopting-new-means-of-technology-justice-dy-chandrachud-205278>.

[40] "Economy Economic-Survey-2016-2017 Statistics and Growth Figures Year-Wise of Andhra-Pradesh–Indiastat" <https://www.indiastat.com/andhra-pradesh-state/data/economy/economic-survey-2016-2017>.

[41] Khera R, "Impact of Aadhaar in Welfare Programmes" [2017] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.3045235>.

[42] Singh R and Jackson S, "Seeing like an Infrastructure: Low-Resolution Citizens and the Aadhaar Identification Project" (2021) 5 Proceedings of the ACM on Human-Computer Interaction 1 <https://doi.org/10.1145/3476056>.

within rural locations pose a major issue because many Bharti reside in these areas. A small number of mistakes creates consequences which reach into millions of affected lives.

Justice Chandrachud's remarks highlight an important idea. The State remains obligated to address issues which emerge prior to implementing a project after learning that exclusions will trigger right denials. He opposes the Aadhaar's continuous operation because fixes cover only known glitches whereas the Majority maintains Aadhaar is an ongoing project which solves emerging problems alongside existing ones. Hon'ble Mr Justice Chandrachud firmly opposes this belief when he declares "*you cannot be ironing out the glitches when Articles 14 and 21 are at stake*"[43]. His opposition is summed up in this statement: Using the most disadvantaged members of our society as experimental subjects is not acceptable when pursuing technical optimization. The extent of social welfare benefit provision failure is clear when he says "*no failure rate is acceptable*." Eating and other core human rights have an absolute barrier against being compromised. Families approaching poverty find they may die from starvation because of denied access to food. Any system that influences personnel needs to be constructed through principles of morality and ethics because it affects persons who are already marginalized.

IX. WANT FOR ACCOUNTABILITY

The ironic aspects of Justice Chandrachud's dissenting opinion become even stronger when observed against Bharat's legal framework as a whole. The Chief Justice first introduced the concept of human experimentation using persons against their will when he issued his ruling on passive euthanasia[44]. The majority decision in the Aadhaar case appears to have reversed its original stance against human trials by allowing highly effective technology to dominate individual rights safeguards. Through his dissent, Justice Chandrachud reminds the Court about its moral responsibilities when enforcing substantial legal provisions[45].

When deploying biometric systems organizations must maintain both authoritative oversight and be accountable for their operations according to his opposing political view[46]. The required framework needs protocols for managing rejected authentications with built-in remedies for

[43] "IAPP" <https://iapp.org/news/a/the-indian-supreme-courts-aadhaar-judgement-a-privacy-perspective>.
[44] Supreme Court Observer, "D.Y. Chandrachud J's Opinion in Plain English - Supreme Court Observer" (*Supreme Court Observer*, October 20, 2021) <https://www.scobserver.in/reports/common-cause-union-india-euthanasia-living-wills-d-y-chandrachud-plain-english-judgment-summary/>.
[45] "Technology Has Emerged as Powerful Force for Justice: CJI D.Y. Chandrachud" (*The Hindu*, February 3, 2024) <https://www.thehindu.com/news/national/technology-has-emerged-as-powerful-force-for-justice-cji-dy-chandrachud/article67807393.ece>.
[46] Sebastian S and Law L, "Live Law" *Live Law* (July 24, 2023) <https://www.livelaw.in/top-stories/cji-dy-chandrachud-cautions-about-artificial-intelligence-says-it-can-make-biased-decisions-based-on-societal-prejudices-233417>.

 [ISSN 2581-5369]

blocked users while establishing specific guidelines about biometric information usage[47]. The State operates under responsibility to justify its actions throughout the implementation of the Aadhaar program. The government must establish it operated appropriate casualty-prevention protocols while also demonstrating prior evaluation of alternative authentication approaches that present less risk to individuals. Since the State functions as the entity that infringes upon individual rights it must present reasonable proof when defending its actions. Amongst a framework of discriminatory social practices, the dissent of Justice Chandrachud in the Aadhaar case demonstrates compelling logic. Biometric authentication systems yield errors which disadvantage marginalized groups thus raising critical ethical standards required in system deployment[48]. The differences between his dissent and the majority opinion show how protecting person rights stands crucial before technical growth while maintaining justice and equality levels. All future discussions about government technology interventions must benefit from lessons learned through the Aadhaar Supreme Court decision to establish standards for system development accountability and oversight and accessibility[49].

The meaning of identity combined with state authority takes shape through individual rights in the Aadhaar judicial decision. The Aadhaar case dissent provides an advanced assessment between technological factors and individual rights and state interference. The legal decision established a new standard because it required the Supreme Court to study pivotal elements about how constitutional concepts relate to technological developments. He explicitly communicates that "*our choice demands we understand the communication between technological capability and power applications*"[50]. The dissent reaches its conclusion by condensing its core arguments regarding the complicated dimension of identification during the biometric governance period. During the Aadhaar case hearing the court examined evolving human-state relationships instead of focusing on the introduction of identification systems. Intense discussion on how programming algorithms and gathered data allow control systems to ascertain individual privileges and rights was sparked by the introduction of biometric solutions. The technical efficiency obsession in the Majority opinion totally dismisses how this relationship affects human autonomy and privacy[51] because the majority's techno-utopian

[47] Das A and Law L, "Live Law" *Live Law* (April 8, 2023) <https://www.livelaw.in/top-stories/cji-dy-chandrachud-digital-inclusion-technology-itself-not-remedy-all-ills-225837>.

[48] Perez JL, "▷ Biometric Authentication: Advantages and Disadvantages" (*Recordia*, September 5, 2024) <https://recordia.net/en/understanding-biometric-authentication-advantages-and-disadvantages/>.

[49] Vedantu, "Speech on Human Rights: Advocating for Equality and Justice" (*VEDANTU*) <https://www.vedantu.com/english/speech-on-human-rights>.

[50] Srivathsan B, Sorel M and Sachdeva P, "AI Power: Expanding Data Center Capacity to Meet Growing Demand" (*McKinsey & Company*, October 29, 2024) <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand>.

[51] Narayanan R, "The Concerns of Using Aadhaar in Welfare Schemes | Explained" (*The Hindu*, October 2, 2023)

vision overlooks how cutting-edge technology may exacerbate inequality while curtailing individual liberty, the darker side escapes. He reiterates how the Aadhaar system seeks to expedite welfare payments while also posing a risk of exacerbating already-existing disparities[52]. When biometric technologies are used, they cause underprivileged areas to receive less attention, which presents significant ethical questions regarding the inclusion and equity of programs.

X. IDENTIFICATION AND IDENTITY

One of the define characteristics in Justice Chandrachud's dissent stands out through his analysis of "*identity*" and "*identification*" terms. One of his key points explains how an alarming disconnection developed between these concepts from advancing technology[53]. The growing power of identity determination by authorities affects both fundamental aspects of how States interact with citizens. This reform of identity laws has led to two essential aspects that protect people from forced identification while allowing them to choose their representation methods[54]. According to him, this concept stands in direct opposition to how the current system simplifies identity into technical identifiers within databases. People have an ongoing right to determine their public identifiers as per statements from Justice Chandrachud. The right to make voluntary decisions and set identity according to personal will collapses when individuals must use Aadhaar as their exclusive verification method[55] This stance serves both theoretical purposes yet stands as a call for basic human dignity recognition in our rapidly advancing digital world.

From the dissenting viewpoint of Justice Chandrachud, the State must establish its action did not harm citizens' rights. The State must demonstrate its identification protocols protect people's constitutional rights according to his arguments. This view captures the worrying dangers of discrimination and exclusion which accompanies the Aadhaar identification system especially well. Based on available realities the State lacks justification to enforce sole use of identification mechanisms without resident considerations. Hon'ble Mr. Justice Chandrachud raises doubts about the majority approach of treating Aadhaar as an ongoing project needing continuous

<https://www.thehindu.com/news/national/the-concerns-of-using-aadhaar-in-welfare-schemes-explained/article67366706.ece>.

[52] "The Impact of Digital Technologies | United Nations" (*United Nations*) <https://www.un.org/en/un75/impact-digital-technologies>.

[53] (*Economic and Political Weekly*, April 5, 2019) <https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare>.

[54] "Safeguarding Identity: The Case for Legal Recognition of Personality Rights in India – SPRF" <https://sprf.in/safeguarding-identity-the-case-for-legal-recognition-of-personality-rights-in-india/>.

[55] Vovk D, "Developing Our Understanding of Human Dignity for the Digital Age - Talk about: Law and Religion" (*Talk About: Law and Religion*, July 2, 2024) <https://talkabout.iclrs.org/2024/07/02/developing-our-understanding-of-human-dignity-for-the-digital-age/>.

enhancement. Per his argument the pursuit of technological efficiency produces unacceptable risks which justify the exclusion of human test subjects. Aadhaar implementation methods violating the constitutional guarantees of Articles 14 and 21 should never receive social acceptance. According to his. view the ethical duties of implementing systems that affect public life require these rights to remain inviolable. Besides being ethical it is essential to include stakeholders in biometric technology development according to Justice Chandrachud's dissenting opinion. The Aadhaar program's efficiency needs evaluation together with its impact on disadvantaged groups within society according to him. The common problem of technical errors poses a substantial threat to deny fundamental rights as well as cause people to become excluded from society[56]. The factual numbers regarding exclusion produced by the Aadhaar system have been analysed in detail by Justice Chandrachud. Research findings along with reports present evidence showing how massive numbers of people face service refusals because of authentication problems. The statistics he provides demonstrate State obligations to eliminate institutional inequalities across its agencies.

XI. CONCLUSION

Through rigorous constitutional reasoning, Justice Chandrachud exposes the majority's assumptions about the legality of Aadhaar, exposing its shortcomings in protecting privacy, preventing exclusion, and maintaining proportionality. His dissent in the Aadhaar judgement is not just a critique of a single legal decision, but a broader warning against the dangers of unchecked technological governance. His dissent highlights the fundamental principle that constitutional rights cannot be subjected to technological expediency. His dissent, as this study has shown, raises serious questions regarding Aadhaar's potential use as a surveillance tool, its effects on marginalised communities, and data security threats. The dangers of judicial acquiescence to official claims of efficiency are brought to light by his emphasis on a higher evidentiary bar for state justification. His claim that Aadhaar places an excessive burden on people to verify their identities highlights how incompatible it is with the right to autonomy and dignity.

Justice Chandrachud demonstrates that Aadhaar does not adhere to the constitutional requirement for restricting basic rights by using the proportionality test. In his dissent, he urges a review of digital governance frameworks to make sure they don't violate people's rights in the name of administrative effectiveness. His criticism goes beyond Aadhaar and offers a guide for

[56] Haqdarshak Empowerment Solutions Pvt. Ltd., "Unseen and Unrecognised: The Indians Excluded from Aadhaar" (*Haqdarshak*, August 24, 2023) <https://haqdarshak.com/2023/08/24/unseen-and-unrecognised-the-indians-excluded-from-aadhaar/>.

assessing further technology initiatives spearheaded by the government. Reiterating the significance of constitutional safeguards in an era of growing digital governance is essential to the research's effective conclusion. The dissent of Justice Chandrachud provides a fundamental defence against technological overreach by the state. Even if it is a minority position, his dissent might influence future legal discussions about surveillance, privacy, and striking a balance between the rights of individuals and the state. His logic continues to be a vital defence against the erosion of constitutional liberties in the digital era as Bharat and the rest of the globe struggle with biometric governance.

*****

 [ISSN 2581-5369]