LEGAL ANALYSIS OF AADHAR 5-JUDGE BENCH CASE ON JUDICIAL TRENDS IN INDIA'S PRIVACY AND DATA PROTECTION LANDSCAPE

Deepika Sharma, LLM, Hidayatullah National Law University

Prableen Kaur Jhajj, LLM, Hidayatullah National Law University

ABSTRACT

According to the Supreme Court, privacy is not an absolute right like many other fundamental rights listed in Part III of the Indian Constitution[1]. It is possible for a person's private interests to be overridden by important "governmental or individual interests", as long as some reasonable conditions are met. This paper highlights Justice D.Y. Chandrachud's strong belief in self-determination as a key part of Article 21 and the clash between the use of biometrics in Aadhaar and the citizens' right to remain anonymous.

The paper discusses the importance and relevance of the minority opinion in the Aadhaar case[2], which was decided by a panel of five judges, concerning the right to privacy and data protection laws in India. The paper also examines the major concerns in the current legal framework in India regarding privacy and data protection. Additionally, the paper explores the legal complexities and possible consequences of adopting the minority opinion on the privacy rights of citizens, as well as the government's transparency and accountability, and public trust in data management practices in India. The paper concludes by suggesting some ways to include the minority judgment in the Aadhaar case, considering India's developing digital environment.

[1] India Const. art. 12-35

[2] Beghar Foundation through its Secretary and Anr. vs. Justice K.S. Puttaswamy (Retd.) and Ors, (2019) 1 SCC 1

1. Introduction

Technology continuously evolves, significantly impacting virtually every aspect of our lives. This influence was central to the debate on the constitutionality of the Aadhar Act[3]. The court[4] endeavoured to balance its commitment to social welfare with the preservation of liberal constitutional democracy's core principles.

The minority opinion emphasized the balance between technology and power. It argued that the technology and biometrics integral to the Aadhar project should not infringe upon individual privacy rights. The Honourable judge noted that the court's decision would account for technology's impact on state functions and its potential to redefine boundaries where privacy is paramount. The court's explanation underscored its dedication to constitutional principles and limited government.

Previously, a nine-judge bench[5] had unanimously affirmed that the "right to privacy is a constitutionally protected right," elaborating that this right is fundamental and inherent to all individuals. It represents the ability to control one's personal identity, which some might argue is the foundation of human liberty.

The court recognized privacy as a natural and fundamental right emanating from Article 21.[6] Transitioning to a knowledge economy, marked by an information revolution, emphasizes the importance of the "volume, reliability, and availability" of information for growth. Given that Aadhar, the world's largest biometric identity scheme, collects the demographic and biometric details of nearly 1.3 billion people, its compliance with human rights standards is crucial.

Justice Chandrachud expressed significant concerns regarding the mandatory nature of Aadhar enrollment. He highlighted issues of "consent" and the "option to opt-out," stating that while Aadhar was initially voluntary, it later became mandatory for accessing various state benefits and services.[7] This expansion of scope effectively coerced individuals into enrollment, thus infringing upon their fundamental right to liberty.

[3] Aadhaar Act, 2016, No. 47, Acts of Parliament, 2016 (India).
[4] Beghar, *supra* note 2
[5] Justice K.S.Puttaswamy (Retd) and anr. vs. Union Of India and ors., AIR 2017 SC 4161
[6] ibid
[7] Beghar, *supra* note 2

The minority judgment also focused on the insufficient security for individual information and the inadequacy of consent mechanisms.[8] The state has entrusted UIDAI with complete control over individual data, raising concerns about potential data leaks and misuse. The judgment criticized the term "enrolling agency" for being broad enough to include private organizations collecting data, which increases the risk of privacy breaches.[9] Moreover, although the act requires entities to inform Aadhaar holders of alternatives for providing identification and to obtain consent, it fails to specify what those alternatives are if individuals refuse consent.[10] This omission is significant, especially since India lacks robust data protection laws, heightening the risk of privacy violations.

The judgment also addressed technology failures and the potential for erroneous biometrics, which could result in beneficiaries losing out.[11] In his dissent, Chandrachud J. noted that the current Aadhaar structure permits mass surveillance and profiling. He argued that the act's allowance for temporary biometric storage, the use of IP addresses for tracking, and database access by third parties—as well as the linking of databases—compromises privacy.[12] He maintained that no biometric system, regardless of its design, could guarantee privacy protection, and this standard should apply to Aadhaar. [13]

2. Relevance Of Privacy And Data Protection In Judicial Decisions

Following the landmark judgment[14], the right to privacy is now recognized as a constitutionally protected right in India. This decision has made privacy a crucial consideration in the creation of new legislation and emphasizes the importance of respecting an individual's privacy and dignity. It underscored the fundamental nature of privacy for an individual's existence. Subsequent rulings have consistently placed the right to privacy and data protection at the forefront in legal adjudications.

2.1 Homosexuality and privacy

[8] ibid
[9] ibid
[10] ibid
[11] ibid
[12] ibid
[13] ibid
[14] Justice, *supra* note 5

The Indian Penal Code[15] ("IPC") explicitly categorized non-consensual homosexual relations and unnatural lust towards animals as criminal offenses under Section 377. This provision aimed to address and penalize such acts, ensuring legal repercussions for violating the personal autonomy and consent of individuals. The Apex Court, while determining the constitutional validity of Section 377 of the IPC, decriminalized it to the extent where the actions of the parties are "consensual".[16] Section 377 categorizes consensual sexual intercourse between individuals of the same gender as an "unnatural offence," which it states goes "against the order of nature." The court found that Section 377 violates the right to privacy guaranteed under Article 21 of the Indian Constitution.

In its decision, the court emphasized the significance of the right to privacy, asserting that if an individual chooses to engage in sexual intercourse with someone of the same gender, that is a matter of personal choice and bodily autonomy. It further stated that as long as such sexual activity is consensual and does not harm the other person involved, any interference in these matters would be a violation of Article 21, as it constitutes an invasion of privacy.[17]

The court also highlighted the importance of bodily privacy, which was extensively addressed in the privacy judgment. It declared that the individual is central to the Constitution and that no law should infringe upon their right to privacy since privacy is crucial to an individual's life and dignity.[18]

However, the newly introduced Bhartiya Nayay Sanhita, 2023[19] ("BNS"), omits similar provisions, raising significant legal and ethical concerns. The absence of these specific offenses in the BNS could lead to a legal vacuum where acts previously deemed criminal under the IPC may not be explicitly covered. This move might weaken the protection against non-consensual acts and bestiality, potentially complicating the prosecution of such offenses. Consequently, the legal system may face challenges in upholding justice in cases involving these acts, unless the BNS is amended or the courts interpret its provisions to align with the established jurisprudence under Section 377. Therefore, this omission could significantly affect how rights

[15]The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India)
[16] Navtej Singh Johar vs. Union of India Ministry of Law and ors., AIR 2018 SC 4321
[17] ibid
[18] ibid
[19] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

and protections are enforced within the Indian legal framework, impacting both legal precedent and the safeguarding of individual rights.

In response to the omission in the BNS, the courts will likely play a crucial role in interpreting the new law to maintain consistency with prior legal precedents. The judiciary may need to extend interpretations or guide the application of BNS to ensure that protections against non-consensual sexual acts and bestiality remain robust. This judicial intervention will be vital to fill any legislative gaps and safeguard the rights and dignities of individuals under the new legal framework.

2.2 Right to marry and privacy

The right to privacy encompasses multiple facets, including privacy of the body, proprietary interests, intellectual activities, decision-making, behaviour, and personal information. The highest court has endeavoured to balance an individual's choice to marry and have children with the societal norms that frame these decisions.

The Supreme Court in Shafin Jahan[20] stated that the right to life includes the freedom to practice any religion and to marry anyone of one's choice. These constitutionally protected freedoms, as covered under Article 21, also extend to the expression of opinions on matters that define one's identity and personality. Based on the nine judge bench decision[21], the court recognized that an individual's choice of partner is protected under the right to privacy. This decision highlights the significance of the minority opinion in the Aadhaar case. The court reiterated that autonomy entails the ability to make decisions about important aspects of one's life.

In the case of Supriyo[22], the Supreme Court addressed the issue of same-sex marriage and the marriage rights of transgender individuals. The court recognized the marriage rights of transgender individuals in heterosexual relationships but stopped short of extending this recognition to same-sex couples. The judgment cited "institutional limitations" that hinder the reinterpretation or amendment of the Special Marriage Act[23] and the Foreign Marriage Act[24]

[20] Shafin Jahan vs. Ashokan K.M., AIR 2018 SC 1933
[21] Justice, *supra* note 5
[22] Supriyo Chakraborty v Union of India, W.P.(C) No. 1011/2022
[23] The Special Marriage Act, 1954, No. 43, Acts of Parliament, 1954 (India).
[24] The Foreign Marriage Act, 1969, No. 33, Acts of Parliament, 1969 (India).

to include provisions for queer marriages.[25] This decision, while upholding the right to privacy and the right to choose one's partner, differentiated between these rights and the fundamental right to marry, specifically in the context of queer couples.[26]

The impact of this judgment sets a complex precedent that could influence future legal actions regarding the rights of LGBTQ+ individuals. For future progress, both the legislature and the judiciary need to take proactive steps. The legislature should consider amending existing marriage laws or introducing new legislation that explicitly recognizes and protects the marriage rights of all individuals, regardless of their sexual orientation or gender identity. This legislative change would align domestic law with international human rights standards. Meanwhile, the judiciary should continue to interpret existing laws in ways that expand rights and freedoms for marginalized groups, potentially setting the stage for such legislative changes through progressive judicial interpretations. These steps are crucial in ensuring justice and equality for all citizens, in light of previous and existing judgments.

2.3 WhatsApp Privacy Policy case

The 2016 WhatsApp privacy policy faced a challenge in a Special Leave Petition (SLP) before the Apex Court.[27] The petition highlighted the urgent need to protect the information of Indians using online messaging platforms such as WhatsApp. It argued that WhatsApp compromised its users' privacy by sharing personal data with Facebook and its associated companies.

In January 2021, WhatsApp introduced a new privacy policy and gave users until February 28 to agree and update their settings.[28] Several aspects of this new policy ignited debate due to their contentious nature. The minority opinion in the Aadhar 5-judge bench[29] highlighted the importance of an "option to opt-out," which is notably absent in WhatsApp's updated privacy policy. This policy change[30] mandates that users must agree to share their data with Facebook, its parent company, to continue using the app. This has sparked significant concerns regarding privacy as it effectively forces users into consenting to their data being shared, underlining an

[25] Supriyo, *supra* note 22
[26] ibid
[27] Karmanya Singh Sareen v Union of India, S.L.P. (C) No. 804 of 2017
[28] Techdesk, *WhatsApp updates terms of service and privacy policy: Why you need to accept it*, Indian Express, (January 16, 2021, 12:40 pm), https://indianexpress.com/article/technology/social/whatsapp-new-2021-terms-of-service-and-privacy-policy-new-changes-accept-or-delete-7134815/
[29] Beghar, *supra* note 2
[30] Techdesk, *supra* note 28

issue of forced consent similar to the Aadhar case, where enrollment was mandatory to access services.

This policy could significantly impact users' privacy by potentially exposing personal information without providing users the autonomy to decide otherwise. The ongoing Supreme Court case[31] will play a critical role in shaping India's data protection regime. Depending on the outcome, it could lead to stricter regulations around user consent and data sharing practices by tech companies, enhancing the protection of personal data against misuse.

The Digital Personal Data Protection Act, 2023 ("DPDP Act")[32], outlines significant stipulations that relate to the issues at hand. Notably, the DPDP Act emphasizes that consent must be "free, specific, informed, and unambiguous,"[33] with a clear affirmative action from the data principal[34]. This is particularly relevant in contesting the forced consent criticized in WhatsApp's policy, where users cannot opt-out. The DPDP Act allows for data processing for specified purposes where the data principal has not explicitly withdrawn consent, reinforcing the need for transparency and voluntary participation in data sharing.[35]

Moreover, the DPDP Act delineate the roles and responsibilities of 'Significant Data Fiduciaries[36],' likely including companies like WhatsApp.[37] These sections require such entities to appoint a Data Protection Officer[38], conduct periodic audits, and ensure the rights of the data principal are respected, aiming to bolster accountability in data handling practices.

In addressing the privacy concerns raised by the WhatsApp policy, the courts play a pivotal role. The Supreme Court's decisions in this case will set precedents for how privacy and user consent are treated under Indian law, particularly in the context of digital data transactions. In the Karmanya Singh case[39], the courts stressed the importance of safeguarding individual privacy rights against arbitrary and non-consensual data sharing practices.

[31] Karmanya, *supra* note 27
[32] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[33] Id., § 6
[34] Id., § 2(j)
[35] Id., § 7
[36] Id., § 2(i)
[37] Id., § 10, 11
[38] Id., §2(l)
[39] Karmanya, *supra* note 27

By emphasizing the need for clear and informed consent and the ability to opt-out, the judiciary upholds the fundamental right to privacy as enshrined in the Indian Constitution and reflected in the new DPDP Act. These judicial decisions not only influence the legal landscape but also serve as a regulatory check on how companies formulate and implement their data policies, ensuring they align with constitutional and statutory provisions dedicated to protecting citizen's privacy.

2.4 State Surveillance and Privacy

The Pegasus controversy, marked by allegations of unauthorized surveillance using the Israeli-made Pegasus spyware, has raised significant legal and ethical questions within India. One of the pivotal legal examinations of this issue occurred in the Manohar Lal case[40]. In this landmark case, the Supreme Court was petitioned to investigate the alleged use of Pegasus by government agencies against journalists, activists, and politicians, which raised profound concerns about the violation of privacy.

The case underscored the tension between state surveillance for security purposes and the protection of individual privacy rights. The petitioners argued that such surveillance, if proven, was a direct infringement on the right to privacy, which is protected under the Indian Constitution[41]. The court's inquiry aimed to determine the legality of the surveillance activities, scrutinizing whether they were sanctioned through lawful channels and whether they adhered to the principles of proportionality and necessity.

This controversy draws parallels with the minority opinion in the Aadhaar case[42] where Justice Chandrachud argued that the act's provisions allowed for a potentially invasive data collection process that could infringe on privacy rights. This minority opinion emphasized the need for a robust legal framework to safeguard against unauthorized data collection and surveillance, underscoring the potential for misuse of power in the absence of stringent checks.

The impact of mass surveillance on individuals extends beyond the mere invasion of privacy. It creates a chilling effect on free speech and expression, as individuals may refrain from expressing dissent or engaging in open dialogue due to fear of surveillance. Moreover, the lack

[40] Manohar Lal Sharma vs. Union Of India, AIR 2021 SC 5396
[41] India, *supra* note 1, art. 21
[42] Beghar, *supra* note 2

of transparency in surveillance operations can lead to mistrust in governmental institutions, undermining democratic governance.

In the Manohar Lal case[43], the court's decision to investigate the allegations reflected a judicial acknowledgment of the critical need to balance state security with individual rights. The influence of the Aadhaar verdict, particularly the minority opinion, was evident as it provided a jurisprudential basis for scrutinizing state actions against the fundamental right to privacy. This case highlighted the judiciary's role in upholding constitutional guarantees and ensuring that any form of surveillance is conducted within the bounds of law, justified, and proportionate.

The ongoing discussions and legal battles around issues like Pegasus and Aadhaar signify a broader debate on the scope and limits of surveillance in a digital age. They call for a re-evaluation of existing laws and policies to better protect individual rights without compromising national security. As technology evolves, so too must the legal frameworks that govern its use, ensuring that they robustly protect the fundamental rights of individuals against the overreach of surveillance.

The Telecommunications Act 2023[44] ("Telecom Act"), intended to modernize and consolidate the legal framework governing India's telecommunications sector, has sparked concerns regarding potential misuse for mass surveillance. The Telecom Act grants the government sweeping powers to intercept, monitor, and decrypt information transmitted through telecommunications networks under the guise of national security. Critics argue that such broad powers, without stringent oversight mechanisms, could lead to violations of individual's privacy.

The potential for misuse of these provisions to conduct mass surveillance on citizens without adequate checks raises alarm. This scenario could not only infringe on individuals' privacy rights but also stifle freedom of speech and expression. The opaque nature of surveillance processes under the Bill could lead to a lack of accountability, where misuse of powers may go unchecked.

[43] Manohar, *supra* note 40
[44] The Telecommunications Act, 2023, No. 44, Acts of Parliament, 2023 (India).

The way forward requires a balanced approach, ensuring that the government's legitimate security concerns do not trample individual freedoms. It is imperative for the legislature to introduce stringent oversight mechanisms within the Telecom Act. This could include judicial oversight, where any decision to intercept or monitor communications must be accompanied by a judicial order. Additionally, transparency measures, such as periodic reporting on the use of surveillance powers, should be mandated to foster trust and accountability.

The courts also play a critical role in safeguarding constitutional rights. They must rigorously scrutinize any reported misuse of surveillance powers under the new Bill, ensuring that any infringement of privacy is both necessary and proportionate. The judiciary should enforce strict adherence to the principles of legality, necessity, and proportionality when it comes to surveillance activities. By establishing robust checks and balances, both legislators and the judiciary can prevent the misuse of surveillance powers and protect the fundamental rights of citizens in the digital age.

3. Conclusion And Suggestion

The Aadhaar 5-Judge Bench decision, along with subsequent judicial interpretations, marks a significant development in India's privacy and data protection regime. This legal scrutiny underscores an evolving jurisprudence that integrates technology with human rights, maintaining a delicate balance between innovation and individual liberties. The judiciary's role in interpreting and applying the constitutional guarantees of privacy has been pivotal, establishing precedents that influence not only the legislative framework but also societal norms concerning privacy and personal autonomy.

The decision rendered by the minority opinion in the Aadhaar case highlighted the intricate relationship between state-mandated schemes and individual rights. Justice Chandrachud's dissenting opinion was particularly influential, drawing attention to the necessity of protecting personal data against unauthorized access and potential misuse. His assertions about the lack of consent mechanisms and the risks associated with biometric data collection have resonated through subsequent legal challenges and debates on privacy.

Furthermore, the Supreme Court's rulings on various issues, including the decriminalization of homosexuality and the right to privacy in the context of marriage, reflect a broader acknowledgment of privacy as a fundamental human right. These decisions reiterate the

principle that privacy is not merely a statutory right but an aspect of human dignity, essential for the development of personal identity and the exercise of individual freedom.

The introduction of the DPDP Act[45], is a step forward in consolidating data protection laws. However, the legal framework still requires significant enhancements to address the complexities of digital data management and to safeguard against the risks of a digital economy. The current legislative and judicial measures, while promising, need continuous refinement to keep pace with technological advancements and emerging threats to privacy.

To further strengthen the privacy and data protection regime in India, several measures are recommended:

Enhanced Legislative Framework: There is a need for comprehensive data protection legislation that includes specific provisions for data minimization, storage limitation, and the right to be forgotten. Such laws should be clear on the purposes for which data can be collected and processed, ensuring that these purposes align with the principles of necessity and proportionality.

Independent Regulatory Authority: Establishing an independent data protection authority is crucial. This body should have the power to enforce data protection laws, conduct audits, and ensure compliance. It should also be empowered to handle complaints, impose penalties for violations, and provide guidance on best practices in data protection.

Judicial Training and Awareness: Given the technical nature of data protection and privacy issues, it is essential to enhance the capabilities of the judiciary by providing specialized training in cyber laws and data protection. This would equip the courts to handle complex cases involving technology and privacy more effectively.

Public Awareness Campaigns: Increasing public awareness about data rights is fundamental. People should be educated on their rights to consent, data access, data correction, and how to seek redressal against data breaches. Awareness campaigns can empower citizens to better manage their personal data and navigate the digital space securely.

[45] Digital, *supra* note 32

Strengthening Cybersecurity Measures: Strengthening cybersecurity protocols to prevent data breaches and unauthorized access is paramount. This includes the adoption of international best practices and standards in cybersecurity, regular security audits, and ensuring that data handlers adhere to stringent security measures.

Encouraging Privacy by Design: Encourage organizations to adopt privacy by design as a core approach in the development of new technologies and systems. This method ensures that privacy and data protection are considered at all stages of development, minimizing privacy risks from the outset.

Regular Review and Updates of Laws: Technology evolves rapidly, and so do the methods for exploiting vulnerabilities. Regular reviews and updates of existing laws and policies are necessary to ensure they remain relevant and robust against new challenges.

By implementing these recommendations, India can build a stronger, more effective privacy and data protection framework. This will not only protect individual rights but also enhance trust in digital systems, fostering a secure and resilient digital economy.