Volume 6, July 2019 ISSN 2581-5504

"Case Comments: Aadhaar Card Verdict by Supreme Court"

K.V. Puttuswami V. Union of India – (2017) 10 SCC 1

Sahaj Karan Singh
Delhi Metropolitan Education,
GGSIPU

ABSTRACT

The document contains a case analysis/comment on aadhard card verdict by the honorable Supreme Court. The case comment consist criticism on personal or private information, technology of aadhar card, the source code for the aadhaar database is neither owned by the government or unique identification authority of india (UIDAI), linking of aadhar card with pan card, sim cards, e-kyc is in question and use of aadhaar for commercial purposes.

JUDGEMENT AND INTRODUCTION

On 24th August 2017, a nine-judge bench of the Supreme Court in Justice K.S. Puttaswamy Vs Union of India passed a historic judgment affirming the constitutional right to privacy. It declared privacy to be an integral component of Part III of the Constitution of India. The judgment, spanning 547 pages, contains six opinions and a lot of interesting observations. At the outset, however, it is important to note that only the majority opinion in a judgment is binding on future cases. In this case, Chandrachud J. wrote the plurality opinion, on behalf of four judges (Kehar C.J., Agrawal J., Nazeer J., and himself), while the remaining five judges (Nariman J., Kaul J., Bobde J., Sapre J., and Chelameswar J.) wrote concurring opinions. Thus, while Justice Chandrachud's opinion is the "plurality" opinion, it does not constitute the majority, since it has not been signed by a total of five or more judges. Similarly, the concurring opinions too, are not binding and do not constitute 'precedent' for future cases.

As per the verdict, there are also minority judgement was given and my base of the comment is totally based on Justice Chandrachud words on the same case.

"If the requirement of Aadhaar is made mandatory for every benefit or service, which the government provides, it is impossible to live in contemporary India without Aadhaar. The inclusion of services and benefits in Section 7 is a pre-cursor to the kind of function creep, which is inconsistent with the right to informational self-determination. Section 7 is, therefore, arbitrary and violative of Article 14 in relation to the inclusion of services and benefits as defined."

"Section 7 does not declare the expenditure incurred to be a charge on the Consolidated Fund. It only provides that in the case of such services, benefits or subsidies, Aadhaar can be made mandatory to avail of them. Moreover, provisions other than Section 7 of the Act deal with several aspects relating to the Aadhaar numbers, like enrolment on the basis of demographic and

Volume 6, July 2019 ISSN 2581-5504

biometric information, generation of Aadhaar numbers, obtaining the consent of individuals before collecting their individual information, creation of a statutory authority to implement and supervise the process, protection of information collected during the process, disclosure of information in certain circumstances, creation of offences and penalties for disclosure or loss of information, and the use of the Aadhaar number for 'any purpose'. All these provisions of the Aadhaar Act do not lie within the scope of sub-clauses (a) to (g) of Article 110(1). Hence, in the alternate, even if it is held that Section 7 bears a nexus to the expenditure incurred from the Consolidated Fund of India, the other provisions of the Act fail to fall within the domain of Article 110(1). Thus, the Aadhaar Act is declared unconstitutional for failing to meet the necessary requirements to have been certified as a Money Bill under Article 110(1)."

CRITICISM ON PERSONAL OR PRIVATE INFORMATION

While citizens have privacy interests in personal or private information collected about them, the unique nature of biometric data distinguishes it from other personal data, compounding concerns regarding privacy protections safeguarding biometric information. Once a biometric system is compromised, it is compromised forever.

CRITICISM ON TECHNOLOGY OF AADHAR CARD

Constitutional guarantees cannot be subject to the vicissitudes of technology. Denial of benefits arising out of any social security scheme, which promotes socioeconomic rights of citizens, is violative of human dignity and impermissible under our constitutional scheme. According to Justice Chandrachud, absence of regulatory and monitoring framework leaves the law ineffective in the protection of data. Biometric technology, which is the core of the Aadhaar programme is probabilistic in nature, leading to authentication failures. There was a risk of surveillance of people based on data collected under the Aadhaar scheme and the data could be misused. "From the verification log, it is possible to locate the places of transactions by an individual in the past five years. It is also possible through the Aadhaar database to track the current location of an individual, even without the verification log. The architecture of Aadhaar poses a risk of potential surveillance activities through the Aadhaar database. Any leakage in the verification log poses an additional risk of an individual’s biometric data being vulnerable to unauthorised exploitation by third parties,"

THE SOURCE CODE FOR THE AADHAAR DATABASE IS NEITHER OWNED BY THE GOVERNMENT OR UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI),

The biometric database in the Central ID Repository (CIDR) is accessible to third-party vendors providing biometric search and de-duplication algorithms, since neither the Central Government nor UIDAI have the source code for the de duplication technology which is at the heart of the

Volume 6, July 2019 ISSN 2581-5504

programme. The source code belongs to a foreign corporation. UIDAI is merely a licensee." Justice Chandrachud mentioned the contract signed between L-1 Identity Solutions and UIDAI. "Prior to the enactment of the Aadhaar Act, without the consent of individual citizens, UIDAI contracted with L-1 Identity Solutions (the foreign entity which provided the source code for biometric storage) to provide to it any personal information related to any resident of India. This is contrary to the basic requirement that an individual has the right to protect herself by maintaining control over personal information. The protection of the data of 1.2 billion citizens is a question of national security and cannot be subjected to the mere terms and conditions of a normal contract.

LINKING OF AADHAR CARD WITH PAN CARD, SIM CARDS, E-KYC IS IN QUESTION.

Linking it with permanent account number (PAN) and ITR. The seeding of Aadhaar with PAN cards depends on the constitutional validity of the Aadhaar legislation itself. Section 139AA of the Income Tax Act 1962 is based on the premise that the Aadhaar Act itself is a valid legislation. Since the Aadhaar Act itself is now held to be unconstitutional for having been enacted as a Money Bill and on the touchstone of proportionality, the seeding of Aadhaar to PAN under Article 139AA does not stand independently. Mobile phones have become a ubiquitous feature of the lives of people, linking of Aadhaar numbers with SIM cards and the requirement of e-KYC authentication of mobile subscribers must necessarily be viewed in this light. Mobile phones are a storehouse of personal data and reflect upon individual preferences, lifestyle and choices. The conflation of biometric information with SIM cards poses grave threats to individual privacy, liberty and autonomy. Having due regard to the test of proportionality which has been propounded in Justice Puttaswamy (judgement) and as elaborated in this judgment, the decision to link Aadhaar numbers with mobile SIM cards is neither valid nor constitutional. The mere existence of a legitimate state aim will not justify the disproportionate means, which have been adopted in the present case. The biometric information and Aadhaar details collected by telecom service providers (TSPs) shall be deleted forthwith and no use of the said information or details shall be made by TSPs or any agency or person or their behalf." Justice Chandrachud also raised questions on contractual validity of memorandum of understanding signed by UIDAI with registrars. He opined since there was no privity of contract between UIDAI and the enrolling agencies, the activities of the private parties engaged in the process of enrolment before the enactment of the Aadhaar Act have no statutory or legal backing. Under Section 47(1), a court can take cognizance of an offence punishable under the Act only on a complaint made by UIDAI or any officer or person authorised by it. Terming Section 47 as arbitrary for its failure to provide a mechanism to individuals to seek efficacious remedies for violation of their right to privacy, Further, Section 23(2) (s) of the Act requires UIDAI to establish a grievance redressal mechanism. Making the authority, which is administering a

Volume 6, July 2019 ISSN 2581-5504

project, also responsible for providing a grievance redressal mechanism for grievances arising from the project severely compromises the independence of the grievance redressal body.

"While the Act creates a regime of criminal offences and penalties, the absence of an independent regulatory framework renders the Act largely ineffective in dealing with data violations. The architecture of Aadhaar ought to have, but has failed to embody within the law the establishment of an independent monitoring authority (with a hierarchy of regulators), along with the broad principles for data protection. This compromise in the independence of the grievance redressal body impacts upon the possibility and quality of justice being delivered to citizens. In the absence of an independent regulatory and monitoring framework which provides robust safeguards for data protection, the Aadhaar Act cannot pass muster against a challenge on the ground of reasonableness under Article 14.

STRONGLY OPPOSING USE OF AADHAAR FOR COMMERCIAL PURPOSES

Use of Aadhaar for Commercial Purposes could lead to exploitation of personal data of individuals without consent and individual profiling. Profiling could be used to predict the emergence of future choices and preferences of individuals. These preferences could also be used to influence the decision making of the electorate in choosing candidates for electoral offices. This is contrary to privacy protection norms. Data cannot be used for any purpose other than those that have been approved. While developing an identification system of the magnitude of Aadhaar, security concerns relating to the data of 1.2 billion citizens ought to be addressed. These issues have not been dealt with by the Aadhaar Act. By failing to protect the constitutional rights of citizens, Section 57 violates Articles 14 and 21.