INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 3 [May, 2026]| Page 146 – 149

WHAT IF OUR PRIVACY IS BREACHED THROUGH AADHAAR LINKED SYSTEMS?

- Sanskriti Srivastava [1]

Aadhar card consists of 12-digit identity identification number. It is issued by unique identification authority of India. It remains as a permanent identity of a person and is universal in nature. Includes lifetime proofs and address. It serves as an identity card for a person like the way we have it in our schools, if a person A is there, he is male, he lives in Kamla Nagar sec 34. This is his identity. Similar way Aadhar card forms as a universal system of identity proofs but at a higher level. It includes name, date of birth, address, residency of that person. It has biometric such as fingerprints and iris scans. The Aadhaar system can be useful in many ways since it can help to open the account of the person, a person can apply for loans to generate income tax provision. Taking example of travelling through airplane where while entering into the airport the person has to show his identity and prove that he/she is the citizen of the country through his identity card verification. If a person A is there, he can update his demographic details through UIDAI Portal.

But Aadhar card can fall into wrong hands where it is being misused? Ghost bank accounts can be opened through linking fake phone numbers so that rapidly loans can be secured. Sometimes even through cloning through fingerprints draining of bank accounts without OTPs can be done.

What if hyper targeted fishing happens and by the use of our names, address, and mobile number highly convincing scams can impersonate. There lies a proving of victims that they did not take the fraudulent loans and the companies are meant to register their leaked numbers.

It was being established through the landmark judgement of justice K.S PUTTASWAMY V. UNION OF INDIA, that the informational control belongs to the citizen and if there is systematic leak it would violate the basic constitutional right. Thereby, the Aadhar can be protected by fingerprints via the UIDIA portal. By masked Aadhar for routine identity proofs which helps in hiding 8 digits of your number. The regular identity review activity history should be there for verification.

Michel Foucault explained it through the panopticon and biopolitics system where there is a constant supervision through constant surveillance. Like the prisoners are there in a central jail and it has been

[1] 1st year, Symbiosis Law School, Nagpur

assumed that they are constantly viewed thereby they maintain decency in jail and have a well-behaved behavior. So here also the state regulates the bodies and populations through data collection. Thereby Aadhar is the biopolitical tool where the human beings are reduced through fingerprints and iris scans. Through sociological point of view Aadhar helps in restricting of the social contract between the citizen and the state. He introduced us with the techniques of governmentality where the society is being rendered governmental and it functions as a internalized forceful control. This makes the citizen visible to the state apparatus at all times. The anatomical breach would undergo a chaotic malfunction. It would include that data is exposed to identity thieves and hackers.

Apart from that sociological thinker Zygmunt Bauman introduced about the liquid surveillance and the algorithmic outcast. The liquid surveillance shows that the modern monitoring systems are not limited to specific institutions like offices and factories but this system flows through the boundaries of public and private sectors. Taking example, the liquid surveillance id flowed through the fintech, healthcare and telecom system. Like in Aadhaar system it was marketed as public distribution system but the growth became gradual and expanded through insurance, Wallers and banking. It lies from communication networks through health registries. So, the liquid nature would ensure that corruption would poison the entire stream. The term used are adiaphorization to show the moral consideration and when breach occurs in the algorithmic system the clone gets leaked automatically.

David Lyon told about social sorting and the amplification of inequality where the surveillance noticed the systems fundamentally. If there is a breach in Aadhaar system social economic stratification will happen where the stratification would be divided into two groups that is the marginalized groups and the affluent groups. The marginalized groups would include loss of basic structure, algorithmic exclusion then the affluent groups it would include financial capital cushion and legal/ institutional remedy. The Lyon's theory shows that if you add a rigid; Ayer of digital documentation over an unequal society it will enhance the inequalities rather than diminishing it.

When our digital advances are translated into our behavioral data aggregation. All the data then translates into the prediction product where everything we do is anticipated. In order to preserve the velocity of digital transactions, the power shifts aways from sovereignty towards algorithmic market sector control.

CONCLUSION

The whole research paper dealt with the breach in Aadhaar system where the error is not just technical error or a normal phishing or a software bug but it is completely visible and controllable including the liquid surveillance. They remain fixed to that centralized identity matrix creating a point of failure to the citizens itself.

The Aadhar system makes them familiar to the market forces and reinforces the social inequalities which has occurred through the earlier times. This shows the fragility is highly visible to power and is deeply vulnerable in nature. These existential risks show a paradigm would show the shift where private identities are being restricted from hoarding and mandating in foundational identity data. It also has true decentralized masked Aadhar to secure the privacy and localize the offline e-KYC tokens. Biometrics have the ability to create trusted identities, and where that exists in digital, transactional ecosystems, a high degree of risk to fundamental civil liberties and privacy also exists. It is simply not possible to have a digital ID with biometrics that does not create fundamental risks of surveillance, risks of social and or political control using the system, and the risk of pervasive privacy violations. No matter what the level of economic or legislative development exists for a region, do no harm must be the bedrock guiding principle of all digital biometric identity systems. (Maulik, R. (2024). A REVIEW ON MITIGATING SECURITY THREATS IN AADHAAR. *Indian Journal of Computer Science and Engineering*.)

REFERNCES

- **[1] Foucault, M.** (1978). *The History of Sexuality: Volume 1: An Introduction*. New York: Pantheon Books.
- **[2] Agamben, G.** (1998). *Homo Sacre: Sovereign Power and Bare Life*. Stanford: Stanford University Press.
- **[3] Mathiesen, T.** (1997). "The Viewer Society: Michel Foucault's 'Panopticon' Revisited." *Theoretical Criminology*, 1(2), 215–234.
- **[4] Bauman, Z.** (2000). *Liquid Modernity*. Cambridge: Polity Press.
- **[5] Bauman, Z., & Lyon, D.** (2013). *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

- **[6] Zuboff, S.** (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.
- **[7] Lyon, D.** (2003). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.