Page 193 - 200 **DOI:** *https://doij.org/10.10000/IJLSI.111890*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 3

2024

Regulation of Personal Biometric Data: Understanding Usage and Processing Law in India

KOPAL ARORA[1]

ABSTRACT

Biometric data usage has become very prevalent in the past few years, but the benefits its brings also comes with a fair share of challenges. This paper argues that the law for collection, storage and usage of biometric data in India is not adequate to balance the rights of the individuals vis a vis businesses or the State. It is first argued that there are technical limitations in the safety of personal biometric data through the exploration of the Aadhar project, then the paper further explores the impact of processing of biometric data through analyzing usage by private entities. The paper further contextualizes the Indian and EU law to identify the pitfalls in regulation of biometric data. The paper concludes by stating that the laws currently are not enough and constructive suggestions to fill the identified gap are made.

Keywords*: Biometric, Data Privacy, DPDPA, GDPR, Aadhar.*

I. INTRODUCTION

The technological development in the last few years has left no doubt that data is the new oil of the economy.[2] With the advent of the digital age, data is commodified and now holds an exchange value, even if the exchange patterns of data are dissimilar to traditional commodities.[3] However, with ushering in this new age, where data is used to develop products based on consumer needs and tailor services to each and every individual, it is necessary to regulate the use of this data and balance the rights of the people it belongs to. One such category of data is biometric data, some examples of which are iris scan, finger prints, face scans etc[4]. This paper argues that the law for collection, storage and usage of biometric data is not adequate to balance the rights of the individuals vis a vis businesses or the State. The first sub-issue argues about

[1] Author is a student at Jindal Global Law School, India.

[2] 'The World's Most Valuable Resource Is No Longer Oil, but Data' (The Economist, 6th May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 27th April 2024.

[3] Jim E. Thatcher and Craig M. Dalton, 'What Are Our Data, and What Are They Worth?', *Data Power: Radical Geographies of Control and Resistance* (Pluto Press 2022).

[4] Lynnette. X. Ng , Abigail c. M., Adrian x. W. Lim , Araz Taeihagh , 'Digital Ethics for Biometric Applications in a Smart City' (2023) Volume No 4 No 4. Digital Government: Research and Practice.

 [ISSN 2581-9453]

the technical limitations in the safety of personal biometric data through the exploration of the Aadhar project, the second sub-issue explores the impact of processing of biometric data through analyzing usage by private entities. The paper further contextualizes the Indian and EU law to identify the pitfalls in regulation of biometric data.

II. BIOMETRIC DATA USAGE BY THE STATE

The largest project for the collection of biometric data by the State was carried out through the 'Aadhar Card' project in India. The unique identification mechanism, which has been in the works for over a decade, was finally launched in 2016 through 'The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016'. However, the release came with its fair share of challenges. The Act which introduced the Aadhar Project was constitutionally challenged in the Supreme Court in the case of Justice KS Puttaswamy v Union of India.[5] This further gave rise to the question of whether the right to privacy was a fundamental right under the Constitution, which was answered in the affirmative by a seven-judge bench of the Apex Court[6]. The Court also propounded a test to check under what circumstances can the right to privacy be reasonably restricted. Through the application of the said test (existence of law, necessity and proportionality), the Aadhar Act of 2016 was said to be constitutionally sound for the most part. The Act established a Unique Identification Authority of India (UIDAI), which issues a unique 12 digit number to individuals and collects plethora of data.[7] The data collected includes Name, Phone Number, Address, Date of Birth as basic information, and biometric data collection is inclusive of Finger Print Scans, Iris Scans and most recently Facial Scan as well.[8] The objective of having a system like the Aadhar is simple – identification and authentication.[9] In a developing country like India, with the world's largest population, it has been a task to bring each and every individual on a single roaster, despite the census every decade. The second objective, was authentication, for the provision of subsidies and benefits to people. This objective of authentication of individual is also in some extents shared with private parties, where the investigating party could verify the identity of an individual with the UIDAI. Therefore, the overarching objective of the Aadhar project was to make the Indian population more 'legible' to the government and businesses, and for the former to be able to carry out their so-called 'service' function in a more efficient and streamlined

[5] *Justice KS Puttaswamy v Union of India* SCC 2019 SC 1.
[6] *Justice KS Puttaswamy v Union of India* SCC 2017 SC 1.
[7] The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016.
[8] Ursula Rao & Vijayanka Nair, 'Aadhaar: Governing with Biometrics'(2019) Volume No 42 No 3 South Asia: Journal Of South Asian Studies 469.
[9] Lynnette. X. Ng , Abigail c. M., Adrian x. W. Lim , Araz Taeihagh , 'Digital Ethics for Biometric Applications in a Smart City' (2023) Volume No 4 No 4. Digital Government: Research and Practice.

manner.[10]

While the benefits of Aadhar are plenty in nature, it is necessary to ensure that the vast amount of data available with the state is safe. The data of all individuals in the Aadhar program is stored on the Central Identities Data Repository (CIDR). The Aadhaar verification procedure uses either biometrics or a One Time Password (OTP) in conjunction with one of the six demographic variables (name, date of birth, sex, address, mobile, or email) to decide whether to approve an individual's identity with a 'yes' or 'no'. Neither the purpose of the transaction nor any other context is known to the Aadhaar system in order to ensure safety of any transaction. Similarly, according to the UIDAI publication, "Every enrolment record is 'always' kept on disc in encrypted PKI (Public Key Infrastructure) format and is never decrypted or altered by any unauthorised/insider/ outer attacker while a transition is being made." Because of this feature, no unknown individual is able to access the Aadhaar database.[11] But this does not protect the system from internal vulnerabilities and attacks.

However, despite the seemingly sophisticated system, there have been instances of breach in the past, wherein the personal data of many individuals was available for sale on the dark web. The most recent report of the same comes from October of 2023, where it was reported that the data of around 81 crore Indians was being sold online, for a sum of approximately $80,000. This leak came in light of the breach of the servers of India Council for Medical Research, who had access to Aadhar information for record keeping of COVID vaccination information.[12] This leak also highlights another pitfall in the data security aspect of Aadhar which is the interoperability of data within the system.[13] The Aadhar information of individuals is linked to multiple institutes and services, which means that vulnerability in one place can jeopardise a large part of the database. Scientific and technical research has suggested that the CIDR protection and security can be considered secure to an extent, however the biggest threat lies in insider attacks and vulnerabilities.[14] The systems require a technological and hardware

[10] Ibid.
[11] Amit Kumar Tyagi, G. Rekha and N. Sreenath, 'Is your Privacy Safe with Aadhaar?: An Open Discussion' (5th IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, India, 20-22nd December 2018).
[12] 'Aadhaar data leak: Massive data breach exposes about 81 crore Indians' personal information on dark web. Details here' (LiveMint, 31st Oct 2023). <https://www.livemint.com/news/india/aadhaar-data-leak-massive-data-breach-exposes-815-million-indians-personal-information-on-dark-web-details-here-11698712793223.html > accessed 27th April 2024.
[13] Ursula Rao & Vijayanka Nair, 'Aadhaar: Governing with Biometrics'(2019) Volume No 42 No 3 South Asia: Journal Of South Asian Studies 469.
[14] Amit Kumar Tyagi, G. Rekha and N. Sreenath, 'Is your Privacy Safe with Aadhaar?: An Open Discussion' (5th IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, India, 20-22nd December 2018).

update to be able to offer the kind of security for the sensitivity of information held by these servers.[15]

III. BIOMETRIC DATA USAGE BY PRIVATE ENTITIES

Biometric data authentication has almost become a norm for identification in many private sector related activities as well. Smart phones store biometric information for authenticating on device, there are biometric home-security systems which use iris scan or voice patterns to grant access, fingerprint and face-scan technology systems are used in payroll management software. These examples barely scratch the surface with respect to the usage of biometric data in daily life. Another huge aggregator of biometric data however is use of wearable technology, which is becoming increasingly prevalent with the passage of time. Some of the top players in the global market with respect to collection of biometric data are Amazon, Google and Apple, with the Halo, Fitbit and the Apple Watch series respectively.[16] The usage of wearable technology has been a game-changer for the consumers. They now have access to much more information about their personal health and fitness goals, which earlier was not easily accessible to them. While these benefits make wearables an attractive investment for the consumer, they are an attractive product to sell as well, as they give big conglomerates access to an entire new category of data. The major categories of biometric data which private entities hold are Facial scan, Iris scans, Fingerprint scan, Voice Modulation, Heart Rate levels and Stress levels.[17] The dangers of private entities holding this amount of biometric data gets magnified when it is understood in the context of the personal data such organisations already hold. The technology for the analysis of personal data is already advanced enough, that with just basic demographic information alongside surfing and purchasing patterns, pretty accurate predictions about consumer behaviour can be made. Such technology is now widely used in creating targeted marketing campaigns and presenting specific content to specific people, based on what they would enjoy. Targeted advertisement on social media websites, tailored ads on browsers and precise curation of media pages is a testament to the same. Coupling this data with the biometric information available with such entities can lead to further making predictions of consumer behaviour accurate, thus endowing private parties with unprecedented power for influence.[18] A simple example of this can be Amazon studying the heart rate of an

[15] Ibid.
[16] Ian Ducey, 'Biometric Data Collection and Big Tech: Imposing Ethical Constraints on Entities that Harvest Biometric Data' (2022) Volume No 12 No 2 (2) Seattle Journal of Technology, Environmental & Innovation Law.
[17] Ian Ducey, 'Biometric Data Collection and Big Tech: Imposing Ethical Constraints on Entities that Harvest Biometric Data' (2022) Volume No 12 No 2 (2) Seattle Journal of Technology, Environmental & Innovation Law.
[18] Ibid.

individual while online shopping, showing them products they might enjoy. The company through combining this data along with browsing pattern can make deductions about the specific reaction (like excitement, discontentment etc.) of the individual to specific items, which in turn can help them make better suggestions to the user, which indirectly will lead to a rise in sales for the company. This example is one of the many uses of such biometric data that can be made, which further also includes targeting with relation to insurance and electoral choices amongst simple product marketing. The extent to which processing of such data can impact an individual and can easily bleed into the realm of being unethical, and hence it must be regulated more strictly. However, such regulation lacks to the extent it must exist, which is an issue explored in more detail through the remainder of this paper.

IV. LAWS REGULATING BIOMETRIC DATA USE

The conversation around data privacy has been rife with developments and inputs, however, not all of it finds purchase in law. The law in India with regards to data privacy stands at an interesting point, as the new comprehensive law for data protection has been enacted but is not enforceable yet. The system as it stands today, is structured under the Information Technology Act, 2002 (IT Act) and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules). The rules, which have been created under Section 89 of the IT Act, are the first piece of law in India which adequately define 'biometric' data. Rule 2(b) defines Biometrics as 'technologies that measure and analyse human body characteristics'[19]. Rule 3 of these Rules classifies biometric data as a part of 'Sensitive Personal Data or Information'. The Rules further lay down the structure for the collection of such information. It provides for a disclosure of intent by the 'body corporate' through a policy, it also requires them to obtain consent from the owner of the data for the collection and usage of this data, with the option to opt out.[20] The Rules state that such data must only be collected for a lawful purpose and be used for the same by agencies which have been disclosed to the owner of such data. The Rules provide that the data must not be retained for longer than is 'required', (except if required by law) however, such retention periods have not been defined.[21] The Rules provide for the requirements for the disclosure and transfer of data, however what is of relevance are the measures given for carrying out

[19] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, rule 2(b).
[20] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, rule 4.
[21] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, rule 5.

 [ISSN 2581-9453]

'reasonable security practices'. These measures require organisations dealing with sensitive personal information to have certifications under leading international certifications- which include but are not limited to – ISO/IEC etc, the rule further lays down the requirement for disclosure in case of breach or security lapse.[22]

In the international landscape, the General Data Protection Regulation (GDPR) of 2016 by the European Union, has a been a landmark law for data privacy legislations around the world. On a closer look, the privacy structure in India under the IT Act and Rules resembles the GDPR structure, even though it was enacted a few years before the negotiation and enactment of the GDPR. GDPR requires 'explicit consent' to be obtained under Recital 51 when particularly sensitive data like genetical data[23], biometric data[24] or health data[25] is concerned. Explicit consent adds another layer of security to ensure that the data subject understands that their data is being collected and will be processed by the data controller.

However, the Digital Personal Data Protection Act, 2023 (DPDPA) in this regard, is a departure from the GDPR and existing Indian law. This classification of data as sensitive or not is missing from the DPDPA. The Act, which was enacted as recently as August of 2023 does not classify personal data into any major categories. Instead, the DPDPA has a provision for classification of data fiduciaries (entities controlling and defining purpose of processing) as 'Significant Data Fiduciaries'. According to Section 10, one of the criteria for classification as a Significant Data Fiduciary will be the 'sensitivity of data' dealt with.[26] While there is a higher standard of safeguard required to be carried out by a Significant Data Fiduciary, the requirement for a more specific or detailed consent from the data principal, like under GDPR, is not one of those.

This departure clearly shifts the ball from the data subject to the data fiduciary's court. This might raise some challenges in the protection of biometric data of the individuals. While the DPDPA rules are still awaited and are expected to provide more clarity with respect to the specifications of what it entails to be a Significant Data Fiduciary, the entire system as it stands seems opaquer than the one already in place. The notification of data fiduciary as Significant Data Fiduciary will be done by the Central Government, making it an executive action. The government might fail in some instances to adequately classify certain fiduciaries as significant. Further, given that it is now a governmental action, the chances of the process being

[22] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, rule 8.
[23] Council Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 127, 23.5.2018, art 4(13)
[24] Council Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 127, 23.5.2018, art 4(14).
[25] Council Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 127, 23.5.2018, art 4(15).
[26] Digital Personal Data Protection Act 2023, s 10(1)(a)

shadowed by political agendas also increases as governmental discretion may sway in varying ideological directions. As an example, large international corporations which drive investment into the country might be let off the hook for complying with the increased requirements of being a Significant Data Fiduciary.

The compliance requirements for private entities dealing with biometric data as of now are given in the IT Rules and are expected to be detailed in the DPDPA rules. However, it is argued that the requirements are not enough to satisfy the security standard such data should enjoy. An approach which can be followed globally and domestically is the one adopted by the state of Illinois in the United States, where they have a specific law for biometric data protection - Biometric Information Privacy Act (BIPA). This law was enacted in 2008 and is a comprehensive legislation on the usage and protection of biometric data of citizens of Illinois. The law lays down basic requirements for the entities to obtain fully informed consent from the people, as can be seen in GDPR and IT Rules as well. however what sets this legislation apart is the limitation it puts on processing. The law prohibits selling, leasing, trading, or otherwise profiting from a person's biometric information.[27] Adopting such a high standard in a specialised domestic law might suffice to be an adequate safeguard in situations wherein private entities might employ processing of biometric data alongside personal data to further their profit maximising motives. To further strengthen biometric data privacy laws, the nature of liability in case of negligence with handling of data can be set to a higher standard. The DPDPA has laid down a structure for fines for violation of duties and obligations by the data fiduciaries, and many of the sums are hefty, however all the penalties are civil in nature. Some scholars have argued that the liability and compliance requirements for entities holding biometric data should be similar to those of bio-banks.[28] For the uninitiated, bio-banks are banks where samples of various biological samples to make them easily accessible for research purposes. Give that the samples held by them belong to real people, the need for having a solid legal framework for them is essential. The sensitivity of the data involved in biometric data collection might warrant similar safeguards as well, however this is a line which must be treaded carefully.

Another major challenge of biometric data protection is the exclusion or the inadequate inclusion of the State into the ambit of fiduciaries. The GDPR excludes activities carried out by the State from the purview of the legislation as long as they are being carried out in

[27] Woodrow Hartzog, 'BIPA: The Most Important Biometric Privacy Law in the US?' (2021) Regulating Biometrics: Global Approaches and Urgent Questions, Northeastern University School of Law 96.
[28] Ian Ducey, 'Biometric Data Collection and Big Tech: Imposing Ethical Constraints on Entities that Harvest Biometric Data' (2022) Volume No 12 No 2 (2) Seattle Journal of Technology, Environmental & Innovation Law.

furtherance of security or national interest.[29] However, the Indian law, neither under the IT Act nor the DPDPA has classified 'state' or 'government' as a data fiduciary under any circumstance. This leaves the mass processing of biometric data carried out by the State (either under the Aadhar project and other surveillance programs) largely unregulated, even when carried out for purposes other than national security. This problem gains more significance in light of the technical vulnerabilities identified in the CIDR systems, as have been discussed above. Due to a lack of regulation, the technical standards of adequate data protection can be overlooked by the State. To this effect, even the court in the case of Justice KS Puttaswamy v Union of India,[30] has held that while Aadhar is not violative and realizes a genuine state aim, it is pertinent to have a stronger data protection law to ensure higher standards.

V. CONCLUSION

Therefore, it can be safely concluded that the in light of the excessive processing possibilities of biometric data, the law as it stands today in India falls short of fully realizing the right to privacy and data protection of its individuals. As has been discussed in this paper, there exist varying possibilities and benefits for the processing of biometric data. However, there is a gulf in the processing that can be carried out and the involvement of the data principals in the matter, with respect to their choice and knowledge. This gulf can be narrowed through regulation which ensures that the data principals understand the consequences their consent might have, by fully understanding all the ways in which their biometric data can be used and the dangers there might be of sharing such data. Further, such regulations should also limit the data fiduciaries in their processing activities to some extent, as has been done by the state of Illinois. As has been adequately analyzed through having a close look at the various rules, it is clear that the law in India currently fails to achieve this standard. However, it can only be hoped that the DPDPA rules lay down a stronger structure for the protection of biometric data by setting a higher standard for the Significant Data Fiduciaries.

*****

[29] Council Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 127, 23.5.2018, art 23.
[30] *Justice KS Puttaswamy v Union of India* SCC 2019 SC 1.