Page 1001 - 1036 **DOI:** *https://doij.org/10.10000/IJLMH.11561*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Biometric Data, Identification and Authentication in India - Legal Framework, Challenges and Impact

TRISHNA DEVI[1]

ABSTRACT

In the last decade, technology has developed rapidly to include the use of biometric data in our daily life. Biometric Data is being used to identify people and authenticate their identity in India in almost all spheres, from the use of Aadhar for government and welfare benefits, banks, workplaces, access to data, and to use of biometric in rapidly growing e-commerce industry. Usage of Biometric Data Authentication has become the new norm as it has been to solve a lot of security issues. However, Biometric Data being our most personal and sensitive data is not free from the flaws in the system and is vulnerable to many issues such as data privacy and security and authentication issues. In India, there is still no exhaustive and comprehensive laws on the usage of biometric data that reflects international standard. This paper aims to study the introduction of Biometric Data, Identification and Authentication in India and the legal challenges it puts in the IT sector and how such biometric authentication works with other variables such as e-transactions, e-commerce and others. This paper will delve into prevalent legal framework that governs such practices and understand the undergoing challenges and impact that effects and governs the present scenario.

Keywords: *Biometric Data, Biometric Authentication- Legal Issues, Biometric Identification.*

I. INTRODUCTION

This paper aims to study the introduction of Biometric Data, Identification and Authentication in India and the legal challenges it puts in the IT sector and how such biometric authentication works with other variables such as e-transactions, e-commerce and others. This paper will delve into prevalent legal framework that governs such practices and understand the undergoing challenges and impact that effects and governs the present scenario.

We see that nowadays we need to upload our photos, signature and fingerprint through the

[1] Author is a student at National Law University and Judicial Academy, Assam, India.

 [ISSN 2581-5369]

electronic media and internet. These are biometric data which are unique to a person and is largely used in today's world.[2] Biometrics started major development from the 1800s mainly for law enforcement agencies and military and slowly percolated into the civilian world. After the 2000's automated biometric systems began to come into focus and the world largely began to use biometrics for various purposes such as commercial transactions and others. At the same time biometric protocols and committees began to form to prescribe standards and protocols regarding biometrics. The committee by the ISO to support and form standardisation of biometric technologies was also formed during this period.[3] However, most legislations regarding biometrics has formed after 2015. In 2016, India formed its Aadhar Scheme that uses biometric data for forming of national identity. We also the important legislation of European Union named GDPR during 2018 that forms one of the toughest data privacy laws in present date and also concerns use of biometric data.

Legal issues such failing in registration and acceptance of biometrics, data privacy, data security, privacy right of person, ethical issues run rampant in the minds of people regarding necessary use of biometric data by payment agencies, government , law enforcement, private parties, banks and others .Biometric data is saved by the party with which we interact and again such data is accessible to the parties with a click of the finger. As such a lot of question arises regarding the privacy and security of such data and whether the present legal framework we have has prescribed stellar standards for the handling of such data. We see the effect of such laws and legal issues regarding biometrics in this paper.

(A) Research Aims and Objective

- To comprehend what is Biometric Data
- To understand the regulations of IT in connection to Biometric Data.
- To understand the present legal scenario regarding Biometric Identification and Authentication in connection to electronic and digital data security, data privacy and others
- To find the legal challenges faced by the introduction of Biometric Identification and Authentication In India
- To decipher the gap in the regulations

[2] Alison Grace Johansen, NORTON LIFELOCK, (January 18, 2021 8.29 PM), https://us.norton.com/internetsecurity -iot-biometrics-how-do-they-work-are-they-safe.html

[3] Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE (January 18, 2021 8.29 PM) https://www.biometricupdate.com/201802/history-of-biometrics-2

 [ISSN 2581-5369]

- To critically analyse the legal framework in view of current scenario in India as well compare it to laws of a few other countries. (mainly to find the lacuna in the law)

(B) Scope of the paper

The scope of the paper is to cover both the regulatory and procedural aspects of law regarding Biometric Data, Identification and Authentication and find the gap and challenges in the legal framework prevalent in the present scenario

(C) Limitation of the paper

The paper is limited to the data available as it will require huge amounts of data. The paper's main focus is on the regulatory framework regarding Biometric Identification and Authentication in India. Here the paper will limit the study of Biometric Identification and Authentication to data that has been uploaded electronically or digitally and is available for access through electronic and digital media. At present the paper is limited to primary and secondary data available to the researcher.

If possible for the researcher to arrange primary data then the limit of the paper will be:

1. Primary Data – Data collected from Statutes, Judgments
2. Secondary Data - Data collected from the whole of India
   Data collected from Rules, laws and reports published in by International organisations, companies and Nations.

(D) Literature Review

i. 'Information Technology Act, 2000 ' is the most important act that regulates the distribution, collection, information and others of data. This Act was referred because at the present moment this is the sole act that governs any law relating to usage of data and its circulation.

ii. 'The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules)' has been referred because it in one present enforced rule in the State that talks about the legal framework regarding biometric data.

iii. 'Personal Data Protection Bill, 2019' has been referred to get an idea on how the future rules and legal framework will be in India regarding the usage of Biometric Data.

iv. 'United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism' has been referred because it puts forward suggestions and standard of legal framework regarding use of biometric data by nations

 [ISSN 2581-5369]

v. The book 'Regulating Biometrics- Global Approaches and Urgent Questions' edited by Amba Kak has been referred to know the various regulations regarding biometrics.
vi. Aadhar Act, 2016 and Aadhar (Enrolment and Update) Regulations , 2016'
vii. Various circulars, notices, orders and others issued in regards Biometric Data
viii. Judgments related to biometric data.
ix. Online References such as Researchgate.net, lexisnexis.in, shodhganga.inflibnet.ac.in and others resources are proposed to be used as materials to substantiate the research
x. International reports, judgments, journals and articles regarding biometric data.

(E) Research Hypothesis

The main hypothesis is that Indian legal framework does not have stellar standards on the privacy and security of such biometric data. India does not have exhaustive legal framework to tackle with problem of using Biometric data and India needs both strict and flexible regulatory framework to mitigate the challenges and impact faced in Biometric data.

(F) Research Questions

1. Whether India has stellar standards or protocols to deal with privacy and security of biometric data?
2. Whether the present Indian Legal Framework is capable of handling the legal issues put forward by biometric data?

(G) Research Methodology

- Qualitative Method, Doctrinal Research
- Secondary Data collection

II. CONCEPT OF BIOMETRIC DATA

Biometric data is used to basically mean the data gotten by collecting biological data of any organism, such as data sample collected to recognize fingerprints, features of a face or facial recognition, eye iris recognition, voice recognition, and other biological samples. The biological data are called biometric samples which are then used as identity attributes to identify a biological organism[4]. Basically, biometric data is biological physical or behavioural data attributes that are unique to a biological organism that can be used to identify the organism such as DNA sample, fingerprints, and face, paw prints and so on. The biological data so collected should have the attribute of being unique and have the characteristic of something

[4] DOMINIQUE PARET, PIERRE CRÉGO: ASPECTS TO TAKE INTO CONSIDERATION FOR WEARABLES, SMART TEXTILES AND SMART APPAREL 39-98 (WEARABLES, SMART TEXTILES AND SMART APPAREL2019).

that can be rendered into data by being storable, matched at convenience and that can be accessible. The concept of biometric data or biometrics is not new, it is as old as 500 BC wherein Babylonian empire biometrics was used in clay tablets by recording fingerprints of the person[5]. In olden days, faces and fingerprints were rendered into a paper to use as means of recognition for access into certain high-security areas, fingerprints were used as signatures for contracts and others.[6]The now modern concept of biometric data is mainly used to mean the biometric ID system used regarding human beings such as unlocking our phone with fingerprints, using the photo of our face in driver's licence, passbook, passport and other documents, and many others[7]. To understand the concept of biometric data as it is used now, we need to see the evolution of biometric data.

(A) Evolution of Biometrics:

The etymology of the term biometric arises from the combination of the Greek word 'Bios' meaning life and the word 'metrics' meaning to measure.[8] A simple system of using biometrics to identify human beings have been around for thousands of years. In many civilizations, fingerprints have been used as authentication to form contracts or were imprinted in clay tablets as a means of recognition. Even Chinese merchants as Joao De Barros mentions used fingerprints to settle contracts or agreements.[9] We also find the mention of using fingerprints to identify people in the book called 'Jaamehol-Tawarikh', a Persian treatise which was written by Khajeh Rashiduddin and Fazlollah Hamadani. One of the important early works that discussed the use of fingerprints in differentiating human beings was that of Dr Nehemiah Grew. In his paper, "Philosophical Transactions of the Royal Society of London", published in 1634 he discussed extensively on using fingerprints to identify human beings. His work was carried forward later by numerous persons notably Govard Bidloo, Marcello Malpighi, Dr J.C.A. Mayer.[10]

[5] Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPTADE, (Jan 18, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2

[6] MORDINI, E. and MASSARI, S, *Body, Biometrics And Identity*. 22 Bioethics, 488-498.(2008) https://doi.org/10.1111/j.1467-8519.2008.00700.x

[7] Alison Grace Johansen, NORTON LIFELOCK, (January 18, 2021 8.29 PM), https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

[8] Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, (Jan 18, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2

[9] Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, (Jan 18, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2

[10] Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, (Jan 18, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2

 [ISSN 2581-5369]

The modern concept of using biometric data to identify persons came about in the 1800s.[11] The pioneer of the scientific system of biometric data that we use today was done Czech anatomist Johannes Evan-gelista Purkinje in 1832 who designed a system of classification of fingerprints at the University of Breslau.[12] The system of using biometrics such as handprints was also used in India by the British officer Sir William Herschel to sign contracts with farmers.[13] However, before the fingerprinting system became popular the concept or system of using biometrics to identify criminals was done by one Parisian police clerk and anthropologist named Alphonse Bertillon who in the year 1890 developed the system of Bertillonage, which used precise body measurements and classifications of a person along with marks such as scars, birthmarks and others to identify a person to use it in the criminal identifying system.[14] This system of criminal identification had many faults meaning that two persons may get different results while taking the measurements of two persons and there may be even false matching. This became absolutely apparent in the case of Will West who was convicted of a crime with the identity William West because the former was the twin of the actual offender.[15] Hence, attention was drawn into the fingerprint system. In the meantime, Francis Galton who had read on Dr Henry Faulds research on fingerprints took forward the idea of using of fingerprints to identify criminal in the 19th century, mainly because he researches yielded that fingerprint of each human being was completely unique, with no similarity between twins or triplets or others[16]. He is, in fact, the pioneer of the system of 10 fingers fingerprint classification system and he had found that only 1 out of around 64 billion may have similar fingerprints[17], making identification system of using fingerprints as identity attributes one of the most accurate systems. Then in British India, seeing the work of Galton, Sir Edward Henry, the general inspector in Bengal collaborated with him to create the Henry Classification system, a method devised to easily store and classify fingerprints of people for their efficient and effective use.[18]

[11] A.K. JAIN, et al P. FLYNN & A.A. ROSS eds, HANDBOOK OF BIOMETRICS 1-22 (2nd ed Springer 2007)
[12] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT, 3921, 3922-3923 (2013)
[13] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT, 3921, 3922-3923 (2013)
[14] *Biometrics*, *History of biometrics*, HOMELAND SECURITY, (Jan 18, 2021, 8.00AM) https://www.globalsecurity.org/security/systems/biometrics-history.html
[15] *Biometrics*, *History of biometrics*, HOMELAND SECURITY, (Jan 18, 2021, 8.00AM) https://www.globalsecurity.org/security/systems/biometrics-history.html
[16] *Biometrics*, *History of biometrics*, HOMELAND SECURITY, (Jan 18, 2021, 8.00AM) https://www.globalsecurity.org/security/systems/biometrics-history.html
[17] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
[18] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

 [ISSN 2581-5369]

The 1900s ushered in a new era of revolution in the biometrics. This is the era that introduced facial recognition and iris pattern recognition.[19] The concept of iris pattern recognition was put forward by Frank Burch, an American ophthalmologist and later in 1960, a company in Palo Alto, California used machine for facial recognition for the first time. This was a pioneering movement for automated biometrics. The year of 1965 saw the development of the first system to recognise signatures by the North American Aviation and again in the year 1974, the University of Georgia made a major breakthrough by using a system able to recognise hand geometry.[20] In the meanwhile FBI had begun using fingerprint identification system and moreover work progressed on automated facial recognition, an exceptional contribution was made by researchers L.D. Harmon, A.J. Goldstein and Lesk who analysed around 21 special facial markers for the task.[21] Also, the very basic model of speech recognition system was being made by Dr Joseph Perkell and later in 1976, Texas Instruments was credited with making the first prototype of a speech recognition system, which was again later studied upon by NIST Speech Group.[22] At this stage, we see that most concepts of biometrics that we use in the modern-day such as fingerprint recognition, speech recognition, facial recognition and others have started to come together. Law enforcement and government agencies have also started using biometrics and in the year of 1992, the NSA formed a consortium consisting of academicians, government agencies, private members from commercial and other industries to form the Biometric Consortium.[23] This led to a new digital and automated biometric system and standards that we see now. FERET (Face Recognition Technology Evaluation) 1993- 97, then IAFIS (Integrated Automated Fingerprint Identification System), Human Authentication API- an SOP one of the very firsts of protocols of biometric standards, that set the standard for commercial and generic biometric to be used in the market and the study by International Civil Aviation Organization on the compatibility of biometrics with MRTD process to use biometrics as an identification method for international standard opened the doors for biometrics system and biometric authentication and identification that we have at the present.[24]

---

[19] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (Jan 17, 2021, 8.00AM)

[20] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[21] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[22] *History of Biometrics*, REFACES.COM , https://recfaces.com/articles/history-of-biometrics (Jan 17, 2021, 8.00AM)

[23] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (Jan 17, 2021, 8.00AM)

[24] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (Jan 17, 2021,8.00AM)

 [ISSN 2581-5369]

(B) Present concept of Biometric Data System

1. Biometric Data

The present concept of biometric data is of automated and digital biometric data. [25] Biometric data refer to physical or physiological or behavioural unique identity attributes of a human being collected as data through a biometric system.[26] Biometric data are fingerprints, iris, DNA, hand vein patterns and others. [27]These data are created from creating a profile from the samples of biometric data received from a natural person. An automated system scans the data and preserves or stores it in a digital form that is easily disseminated across various channels. Biometric data is mainly favoured because of its uniqueness, as no other individual will be able to access or duplicate a biometric data.

2. Types of Biometric Data:

The Biometric Institute provides certain biometric data types that are common in todays' world and is useable as biometric data. They are DNA Matching- a sample of DNA is collected from the person and that sample's analysis is stored in digital for further match in the future, retina and iris recognition of the eyes , face recognition, fingerprint recognition, finger geometry recognition, ear recognition, vein recognition, behavioural aspects like gait recognition and keystroke recognition, others such as voice recognition and speaker identification and authentication, hand-geometry recognition, the very commonly used signature recognition. [28]

3. What is biometric system?

Biometric systems are nowadays basically automated systems that are able to authenticate and identify a person using biometric data such as fingerprint, iris recognition, DNA and many others. Systems can range from simple system that can recognise one or two biometric data to complex systems that are capable of recognising multitude of characteristics or biometric data.[29] These data are generally called a biometric modality, that is chosen as one modality but generally a combination of modalities to represent the profile of a person depending on the purpose such data is collected. The modalities must contain certain features. They are:

---

[25] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[26] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[27] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[28] *Types of biometrics*, BIOMETRICS INSTITUTE, (January 18, 2021 8.29 PM) https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

[29] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute.

 [ISSN 2581-5369]

- "Universality- the modalities or data must be generally found in all human beings around the world
- Unique- they must be such that there must be completely negligible chances of two individuals possessing the same characteristic of data. In case of identical twins, although they may share same face or DNA, they will have different fingerprints or even signatures.
- Permanent: they must be stable and they should not be erasable throughout the time, there should be negligible changes even after taking into account human life cycle and even then, there must be stability over a period of time. Example: faces of human being change as they age but they remain stable for a period of not less than three years after the age of five
- Measurable : the data must be able to easily digitized and also it should be one that can be acquired in a cost-effective and convenient manner form people
- Perform Effectively: the data acquired should be so that it is accurate and when authentication is carried out it is a speedy process
- Acceptable: one of the most important features of biometric modality is that they must be such that the society does not find it objectionable in giving such data to the government or put it in public and they must be capable of such that they can be used by a majority of the population."[30]

4. Biometric authentication and identification

Biometric authentication and identification are basically the process of authenticating biometric details of a person to match his identity to the profile already in a system to allow him access to any document or area or use for any other purposes like government id card, etc. Generally, the system works in two ways, one is physical authentication and one is distance authentication. Physical authentication and identification are done through present biometric devices such as fingerprint scanner, facial recognition machine, iris scanner and others wherein the person himself is physical present and scans his biometrics at that point of time. This maybe done so to let him access something at the present time. An example is using fingerprint scanner to unlock a laptop. Distance authentication is generally done to identify the profile and collect

[30] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute.

and match data, example a bank may ask for biometric authentication card or number to verify whether you are the actual holder of your personal details and verify the identity of the person. Biometric data and authentication are being used largely in the present world.

III. USAGE OF BIOMETRICS IN THE PRESENT WORLD

Earlier in Chapter 2 of the paper, we discussed how biometrics evolved and how it was first used for signing contracts and for the purpose of creating a criminal identification system. In the US biometrics was used in the prison system and armed forces, aviation and others. The end of the 20th century and the start of the 21st century saw huge usage of biometrics in all matters from using biometric authentication and identification system in criminal identification system to armed forces, from passport to social welfare systems, from commercial transactions and businesses to academics and office work. It slowly percolated into the daily life of people. As I write this paper, I am writing from a laptop that uses biometric authentication to access the content of the laptop. From this, we can see that the biometric data system has completely percolated into our daily life. At the present day, our world uses biometric systems in multi sectors and through multiple platforms for the smooth and higher functioning of everyday life. It is mainly so because it is unique, trustworthy and very convenient to use. There is no need to remember complicated passwords or worry about password being hacked. Biometric data isn't duplicable and it is unique, so with one scan of fingerprint, iris recognition or voice speech recognition one can get a work done. It can create an identity that cannot be repeated or duplicated.

(A) General usage of biometric data

Currently, there is a general use of fingerprints, facial recognition, speech recognition and signature recognition in everyday life of almost all people on the planet. Google, which is one of the biggest technology platforms uses user speech recognition as one of the methods to allow users to search data, give commands and do other functions. Many other technology platforms and sectors have started using biometric authentication in the 21st century. The first to use biometric data system was government agencies mainly the law enforcement sectors in prison systems, military access controls, criminal identification along with civilian identification especially in the United States of America.[31] Later in 2001 in Super Bowl, a facial recognition system was used which didn't yield much results.

[31] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

The 21st century sees rapid and expanding use of biometrics. The sectors that started using biometrics were government agencies and law enforcement agencies for civilian identification and criminal identification, military for identification and access control, banking sectors for customer and business identification, commercial industries, healthcare sectors, mobile and laptops and many others.

Let's consider the case of USA for instance, the FBI and other agencies have been using various types of biometric data sample of biometric profile for identifying and tracking criminals, especially the building of an IAFIS by Lockheed Martin for the FBI in the year 1994.[32] After the incident September 11 in 2001, security in the States further increased with the founding of NBSP or National Biometric Security Project to develop modern biometric techniques.[33] They even managed to locate one terrorist from the incident using biometric who was a part of planning the 9/11 incident. The EU also requires biometric authentication and registration of civilians for availing government facilities. Biometric registration is completely present in countries like USA, China, Japan, Russia and many other countries.[34] Biometric authentication and identification is also associated with Government IDs and social security system and European countries, along with countries like USA, China, and many other countries use biometric data such as fingerprints, facial recognition, palm print, signature recognition for issuing IDs such as Driver's License, social security card, Bus Card, and others. EU is known for 'ePass' to its citizens under the rules of EU Council Regulation and biometrics play an important role in such ePass. Biometrics is used in border and migration as well as visa and passport. Generally, people used facial recognition and fingerprint recognition in passports. Meanwhile in borders generally facial recognition and digital photo is done along with finger prints especially in USA borders, with the intent to track criminals, counter terrorism and to avail the people security features.[35] Even the UN in the prepared CTED document 'Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism' emphasizes the use of biometric authentication and identification in a safe manner to track terrorists and counter terrorism. For example, International Terrorist Osama bin Liden's bodily remains was identified and authenticated by CIA in 2011 using

[32] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[33] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[34] Mehedi, *25 Uses of Biometric in Today's Society*, BIOMETRICTODAY, (Jan 18, 2021, 8.00AM) https://biometrictoday.com/uses-of-biometric-technology-today-society/

[35] Busch, Christoph. *"Facing the future of biometrics. Demand for safety and security in the public and private sectors is driving research in this rapidly growing field."* Vol 7 Spec No EMBO reports, S 23-5. (2006) doi:10.1038/sj.embor.7400723

biometric data i.e., through his previously recorded DNA sample and facial recognition.[36] It is not only the Government, military or law enforcement that uses biometrics for security, welfare schemes or tracking of criminals.

Biometric authentication and identification system is used largely in banking sectors and in commercial transactions. Banks collect our photo, digital and otherwise, signature and thumbprints for general transactions and such data are recorded in the system of banks. Nowadays banks have facilitated mobile or e-banking apps and encouraged its use by customers. Such apps are generally found to record our biometric data. Also, payment apps or platforms that use payment gateways have been found many a times to use and encourage biometric authentication and identification for allowing access to such platforms and then allow users to confirm transactions. We can take the example of GPay, PayPal, Paytm, BHIM Upi or others where we can scan our fingerprints in the app, they will record the data and then allow future transactions and access to any of our data in the app after verifying our fingerprints and authenticating them. This is so also for many apps that allow commercial transactions such as Amazon, and other apps. Banks also use biometric authentication for secure vaults and lockers for customers. And even banking personnel has to use biometric banking for secure access in certain cases. In many countries bank accounts are linked to government ids that use biometric system, such as the United Kingdom and countries in EU. EU also requires incoming students from other countries to update their biometrics with respective townhalls of their residing town or the town of their colleges.[37] We often see work places and offices using biometric system such as punch machines that use fingerprints to record attendance. It has been the practice of many industries and companies to secure their workspaces, factories, documents and other high-security areas and things by using biometric authentication of iris recognition, facial recognition and thumb print registration to allow access only to authorized personnel and prevent such data from theft and misuse. Nowadays it is common for government offices, schools, colleges, workplaces, factories and others to use punch machines and other biometric system to allow access to facilities and to register attendance. Also, nowadays most hospitals and healthcare facilities link their patients' files with their government ids that use biometric authentication. At this juncture we can't forget to talk about researches, scientific and technological developments, research laboratories and high-security documents and documents

[36] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (Jan 17, 2021, 8.00AM)

[37] EMN SYNTHESIS REPORT – IMMIGRATION OF INTERNATIONAL STUDENTS TO THE EU, European Migration Network Study 2012

 [ISSN 2581-5369]

of national security which are protected by using biometric systems and authentication to allow only registered and authorized personnel to access the data and the information.

While we talk about biometric authentication and identification, we must talk about the present generation of smartphones, laptops, computers, AI operated systems and others. The smartphones now are biometric enabled which uses facial recognition and fingerprint recognition to allow users access to the phone, enhancing security since no one else than the user can unlock the phone and access its contents. Technology companies are also rapidly producing laptops and PCs that use facial recognition and fingerprints for biometric authentication and recognition. We have Apple's MacBook Pro using fingerprint recognition system to unlock the MacBook by using Apple ID and Apple Pay; same ways we have other laptop companies such as Lenovo which use FIDO (Fast Identity Online), HP, Samsung and DELL which use fingerprint authentication and facial recognition. We are also increasingly using home security features such as doors and locks that use either fingerprint sensors, facial recognition or voice recognition to allow entry or unlock the doors. [38] With the launch of technologies such as SIRI, Google voice and speech recognition technologies, ALEXA have used these technologies that store our private data along with our biometric data to operate a lot of our home and offices appliances, our documents, our accounts, to do shopping, operate cars, machines and many others. We can ask Alexa to buy a product from amazon with just one voice command or ask Siri to send an email. Also, nowadays entrance examinations also use biometric data to ensure that the candidates appearing in the exam are the legitimate candidate themselves. As we can see that biometric system has completely percolated into our daily lives everywhere from banks to schools, to academics to workplaces to government and everywhere. Such percolation in our daily lives require certain measures and regulations so that such data are not misused.

IV. BIOMETRIC REGULATIONS AND LAW AROUND THE WORLD

Biometric system has gained universality and extensivity in the late 20th Century and at the present period. It has changed its nature from physically stored data to automated and digital system of data which is generally stored in a digital format as a biometric profile. Since, Biometric Data are extremely personal, i.e., completely unique to one person, it is considered as 'Personal Data' or 'Sensitive Personal Data' under the laws of many countries.

[38] Mehedi, *25 Uses of Biometric in Today's Society*, BIOMETRICTODAY, (Jan 18, 2021, 8.00AM) https://biometrictoday.com/uses-of-biometric-technology-today-society/

(A) Legal Definition of Biometric Data

Biometric data is considered 'special categories of personal data'. The GDPR (General Data Protection Regulation) claimed to be toughest law in the world regarding privacy and security classifies biometric data as a special class of data or sensitive data and under Article 4 of the law defines it as - 'Personal data' that results from using a specific technical process to get the physical, behavioural or physiological data or characteristic of a natural human being resulting in allowing or confirming the unique identity of that human being by using things such as facial recognition or dactyloscopy data.[39] The E-Governance site of the Indian Government defines biometric data as data that represents a biometric characteristic.[40]Basically biometric data is sensitive personal data.

(B) Bodies regulating standards of Biometric Data

One the first bodies that was formed to develop standards for biometric data was the Biometric Consortium by NSA. The main mission of the consortium is the management of relations between the main federal government of the USA and other national and international entities with the main goal on securing an identity management system to protect, increase the defence support of the country. On the other hand, the EAB i.e., the European Association for Biometrics, a non-profit organisation in Europe is working towards the interests of the citizens of Europe and to develop biometric data in a way that provides and looks out for the security, privacy and human rights of the people in EU. Another organisation that lays emphasis on the proper use of biometrics is The Biometrics Institute, which is an independent forum that was developed by think tanks and leaders way back in 2001 to monitor the use of biometric data and preserve the industry's moral standards by using biometric for right purposes and to facilitate its development. They are also credited with the development of Biometric Institute that work on the technological development of Biometrics and share such knowledge to many nations with their offices being in London and Sydney, building a truly international and global network that is representative of more than 800 individuals, 204 organisations and 24 countries.[41] One of the oldest attempt for standardisation was the establishment of the ' ISO/IEC JTC1 Subcommittee 37 (JTC1 /SC37)' by the ISO (The International Organization for Standardization) whose purpose was to standardise the technologies used in biometric

[39] General Data Protection Regulation, 2018, Art 4, Regulation (EU) 2016/679, 2018 (EU)

[40] *E-Governance Standards*, STANDARDS FOR E-GOVERNANCE APPLIANCE, STQC DIRECTORATE, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA, (Jan 18, 2021, 10:53 AM) http://egovstandards.gov.in/biometrics

[41] John Trader, June 17, 2016, *The Top 5 Biometric Associations and Regulatory Bodies Around the World*, M2SYS BLOG , (Jan 18, 2021, 11.00 AM), https://www.m2sys.com/blog/biometric-hardware/top-5-biometric-regulatory-bodies/

 [ISSN 2581-5369]

system and biometric data. In 1998, the International Biometric Industry Association was founded in the USA in Washington D.C mainly to ensure the privacy, suitability, efficiency and security regarding usage of biometric data and technology for identity management. IBIA put emphasis on data security, cybersecurity of biometric data used in US border issues, immigration issues, visa issues, healthcare, and many others like financial services, government benefits.

(C) Laws that regulate the use of Biometric Data

It is the 21st century that has seen the rapid usage of biometrics in many countries to authenticate and identify people. There has been raising concerns on the use of biometric data the main of which are privacy, human rights, ethical reasons, and the most important is that of data privacy and security. Considering, that biometric data is considered as 'Sensitive Personal Data', there is need for laws to ensure that biometric data of a person is not used willy-nilly. The very first difficulty is that we need to form common and standardised terms that are used to define the variables used in biometric systems and the 'ISO/IEC JTC1 Subcommittee 37 (JTC1 /SC37)' established by the ISO is in charge of that. [42] One of the regulations to start protecting biometric information was the 'Illinois Biometric Information Privacy Act' or BIPA. This regulation which was enacted in 2008 was designed mainly to provide and promote safe use of biometrics , by regulating its collection, disclosure of such data and destruction of the collected biometric data.[43] The Act has simple rules which prescribed that private entities or bodies must get informed consent form a natural person before collecting or circulating the collected biometric data and these private entities are prohibited from profit mongering by selling them to other parties or otherwise profiting from them by leasing or trading such data or do any activities that will lead to profiting from the biometric information of a natural human being.[44] The private entities or companies which wished to use biometric data or authentication are also required to follow a set procedure and guidelines that provide how such data must be

[42] Technical Text of Standing Document 2, version 5 – Harmonized Biometric Vocabulary, JOINT TECHNICAL COMMITTEEISO/IEC JTC 1, SUBCOMMITTEE SC 37, 31 January 2006, a working document, , (Jan 18, 2021, 11.30 AM), http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-1480.pdf?nodeid=4954581& vernum=0

[43] AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,52-62 (Al Now Institute, 2020), https://ainowinstitute.org/regulatingbiometrics.html.

[44]Biometric Information Privacy Act., 740 Ill. ICLS. 14/15 ("§15(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it [informs the subject what is being collected and receives a written release]….§15(c) (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless [the subject of the biometric identifier or biometric information consents or disclosure is required pursuant to a valid warrant or subpoena]." (2008)

retained, collected and destructed.[45] The BIPA Act put forward a strong standard and bound the private entities to prescribed rules and care necessary for transmission, storage and protection of biometric data of a person that is in some ways greater than other sensitive information. In Illinois many cases have been brought under the BIPA alleging privacy harms such as breaches of data, unconsented surveillance, or disclosure of sensitive information. One of the key features of BIPA is that it does not follow the line of thought that malicious harm must occur for there to be an infringement of rights, it follows the principle that whether any malicious harm was done or not with the biometric data collected; however, if such data was collected or processed without explicit consent of the person and any prior notice given, then such action was enough to cause breach of the law and affront to the autonomy of the victim.[46]

Such was in the case of Rosenbach v. Six Flags Entm't Corp.[47], where a claim was brought into the court by the mother that the amusement park collected her minor child's fingerprints for their system without her consent. Here the Supreme Court of Illinois held under BIPA the above company violated the person's right to privacy to control who had access to their biometric identification and who are the biometric identifiers that they will share their own biometric identification. We can also see the recent case of Clearwater AL which accessed more than three billion images of people without their express permission and in 2020 ended all its contract with all agencies not involved in law enforcement in Illinois.[48] Important guidelines were set forward by the 'Data Protection Working Party' on August of 2003; which in its opinion WP 80 focused mainly on the verification process of biometric data rather than on the aspect to gain control or access through biometric data implicitly pointing out that biometric system should mainly be used for verification purposes.[49] The Directive 95/46/EC also sets forth principles regarding data quality which states that personal data must be kept modernised when essential and must be true.[50]Two of the most important principles regarding biometric data was given by Article 29 of the Data Protection Working Party which gave two

[45]Biometric Information Privacy Act, 740 Ill. ICLS. 14/15 § 15(a). ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.") (2008)

[46]. AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,52-62 (Al Now Institute, 2020), https://ainowinstitute.org/regulatingbiometrics.html

[47] Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 8, 129 N.E.3d 1197, 1200–01

[48] Ryan Mac, Caroline Haskins, and Logan McDonald*, "Clearview AI Has Promised to Cancel All Relationships with Private Companies,"* BUZZFEED, (May 7, 2020,6:50 PM ET), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies

[49] Els Kindt, *Biometric applications and the data protection legislation, The legal review and the proportionality test*, 31 DuD, Datenschutz and Datensicherheit, Schwerpunkt, 166-170 (2007)

[50] Directive 95/46/EC of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 1995, Article 6.1 (d)

purposes for acquiring personal data; one is that any personal data collected so is processed in a fair manner after it has been lawfully collected and secondly such data should be only gathered for purposes that are legitimate,….specified …., explicit and they should be adequate but not excessive of such purposes. [51] The DPAs work on whether a biometric identification system is lawful depending on Article 6 of the Directive 95/46/EC such as a whether iris recognition is necessary for air passengers will be decided on the proportionality principle. This principle also comes forward for the balancing of interest in Article 7(f) of the Directive 95/46/EC[52] that puts forward limitation on government power for processing personal data and that such data should not violate fundamental freedoms and should only be done for interests that are of legitimate concerns such as to counter terrorism, healthcare, government IDs and others and also the extent of biometric that will be taken. For example, iris recognition cannot be taken for simply making a metro card while iris recognition maybe necessary for military documents. We also see prescribed guidelines by the United Nations in its report 'United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism'. The compendium deals with the issues of biometric data violating data privacy and human rights and states that under the ICCPR article 17- a person cannot be subjected to any unlawful intervention of his/her privacy and he/should have protection of law against attacks on his/her privacy[53] and the UNHRC also recognised that if right to privacy is violated or abused it affects the human rights and fundamental freedoms of persons.[54] Since, right to privacy by States must be done accordingly on the foundation of law and under very reasonable situations,[55] the compendium suggested that States should try and review their data protection and privacy laws regarding personal data so as to prevent misuse of biometric data and to meet the current standards of biometric data technologies. It also suggested for the building of procedural safeguards and the establishment of human rights approach based independent committees or bodies that will supervise the States in their use of Biometric data and ensure their and the private sector's compliance of data protection and privacy laws, along with providing remedies to the victims of such violations.[56] The compendium sets forward standards that will help in establishing a biometric system compliant

[51] Directive 95/46/EC of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 1995, Article 6
[52] Els Kindt, *Biometric applications and the data protection legislation, The legal review and the proportionality test,* 31 DuD, Datenschutz and Datensicherheit, Schwerpunkt, 166-170 (2007)
[53]The International Covenant on Civil and Political Rights (ICCPR), United Nations General Assembly Resolution 2200A (XXI), Article 17, 1966
[54] Human Rights Council Resolution A/HRC/RES/34/7 (2017).
[55] Human Rights Committee General Comment No. 16: Article 17 (Right to privacy), para 3-4.
[56] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute

with laws that protect data and protect data privacy and security. The compendium set forward that the 'Enrolment Quality Assurance'[57] is a factor in setting up the system and nations should use excellent and superior quality enrolment standards to ensure accuracy even in remotest, busiest, fastest of areas and should be able to consider mitigating factors such as age of children and old person whose biometrics may show difference as they age. It also put forwards the requirement that biometric data must only be collected through informed consent through the method mentioned and only used for the stated purposes with the people having the right to correct any inaccuracy or misleading records or changing records.[58] The compendium also states that when any nation make any law or use personal data, the standards of such data should be in conventionality with standards set by international organisations such as the International Civil Aviation Organisation (ICAO), World Customs Organisation and mainly the International Organisation for Standards (ISO) and for the purposes of protection of privacy of data the 'Privacy Guidelines and Privacy Impact Assessment Checklist' by Biometric Institute must be followed.[59] Also data should only be shared with trusted recipients and there should be prevention of misuse of personal data. As we can see from the above, biometric data should only be used for lawful purposes and must be collected legally with informed consent for a stated purpose and must not be shared without consent and that it must not be used for profit. The main principles are the following of principle of proportionality, accountability , consent of the person whose data is processed, limitation of powers of government and other data processors, transparency, ability to withdraw consent, principle of 'right to be forgotten', and others.

Recently, there have been many data protection laws that govern the use of biometric data. The General Data Protection Regulation (GDPR) of the European Union which came in force from May 25, 2018 is one such regulation that protects the use, collection, dissemination and sharing of personal data, especially sensitive personal data like biometric data. The regulation sets out seven principles of accountability and protection of personal data in the Article 5.1-2 of the Regulation. These principles states that processing of data must be done in a lawful and fair manner that is transparent and such data should only be used or collected for legitimate purposes that have explicitly explained to the person from whom the data have been collected. The data so collected must be minimized by necessity and only such must be collected that is completely necessary for the purpose and not in excess. The data must be accurate and only

[57] *Id.* at 55,
[58] *Id.* at 55
[59] *Id.* at 55

 [ISSN 2581-5369]

collected for a period that is necessary for the purpose. Here, the principle of 'right to be forgotten' comes into play meaning that a lifetime record of any data should not be kept as long as it is not necessary. The most important of all of them is that confidentiality and integrity of the data must be maintained. Also, the person who controls the data is responsible for compliance with all of the regulations of GDPR. Article 6 of the GDPR put emphasis on when a party is allowed to process data; it put emphasis on unambiguous and clear consent by a party to allow the other party to process their data, or when there is necessity to process personal data such as signing a contract with the person whose data the other party want to process, or when a party processes other's personal data in compliance with any legal obligation or in pursuance of a task of public interest or legitimate interest.[60] The Regulation also provides for the appointment of Data Protection officers for ensuring compliance with GDPR and redressal of grievances. So basically, the privacy rights of a party whose data has been collected has the right to be informed that his data has been collected and he should have access to that data so that the person can rectify, erase, object or restrict processing of such data. [61] The person also has rights against automated profiling and choice making. We can see that the Data Protection laws are pretty comprehensive under GDPR and since Biometric Data falls under Article 4 of the regulation we can see comprehensive protection of biometric data. Another important legislation is the Washington House Bill 1493 (2017) signed on May 16, that is valid for both government entities and non-government entities and individuals. The Bill mainly controls the way biometric data is collected, kept, shared and the way those parties use biometric identifiers.

In a similar way of BIPA it restricts use of biometric data for commercial purpose without consent. Since 2018 there have been many changes on the forum of biometric data laws. At first, there was the enactment of Data Protection Law Enforcement Directive by European Union to tackle with personal data security. In 2019, along with introduction of 'Identity Service Matching Bill by Australia in July, The International Red Cross Committee adopted a biometric policy in August and Kenya also passed the Huduma Namba Bill legally authorizing the NMIMS Project. However, 2019 also saw Jamaican Supreme Court saying that the biometric ID system is unconstitutional, with three places in USA, San Francisco, Oakland and Somerville banning use of technology that uses facial recognition; however the UK High Court in the case of police collecting and using facial recognition live on people found that there was

[60] General Data Protection Regulation, 2018, Art 6, Regulation (EU) 2016/679, 2018 (EU)

[61] *What is GDPR, the EU's new data protection law?* GDPR.EU, https://gdpr.eu/what-is-gdpr/#:~:text=The%20regulation%20was%20put%20into,tens%20of%20millions%20of%20euros.

 [ISSN 2581-5369]

such provisions in the common law.[62] The United States of America proposed a new act in the year 2020 to regulate data privacy of biometrics through the 'National Biometric Privacy Act' while many states in the USA introduced moratorium bills on biometric data. Even in Kenya its High Court suspended the NMIMS project. Gradually we see that people became aware of the issues and risks regarding biometrics and are cautious of use of biometrics and seek to limit the power of its usage. The issues and risks of using biometrics in India will be discussed later after we discuss the present scenario of Biometric Data system in India.

V. BIOMETRICS DATA SYSTEMS IN INDIA

Biometric system was introduced in India as early at the late 1800 by Sir William Herschel who used fingerprints for contracts.[63]In India, the largest biometric system in the world, i.e., Aadhar Scheme was doled out in 2009. It used iris recognition, facial recognition and fingerprint recognition to authenticate and identify a person or citizen and to create a national identity. It is mainly used to deliver welfare schemes to the vulnerable and the marginalised community[64] and it joins with other platforms of private sectors like banks, finance, healthcare and others to provide benefits to the Aadhar card holder. Private sectors build biometric payment related products and systems where people would be able to pay from their smartphones with the help of authenticating their fingerprints in mobile phones or laptops. [65]

It is not just Aadhar in India that use biometric system, but also schools, colleges, workplaces, smartphones, laptops and many other devices. The Government of India has implemented punching machines that use fingerprint recognition to record attendance. The Biometric Attendance System (BAS) Manual 2018 published by the government of India provides for recording of biometric attendance through the BAS employee registration and through the implementation attendance terminals or devices like fingerprint punch machines, desktop fingerprint or iris recognition.[66]Nowadays, the government is also proposing to use biometric data for e-governance functions and use them to issue documents, perform surveys and others.[67]

---

[62]. AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,42 (Al Now Institute, 2020), https://ainowinstitute.org/regulatingbiometrics.html

[63] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[64] Krishnadas Rajagopal, "*Centre's Aadhaar Affidavit in Supreme Court: 'Welfare of Masses Trumps Privacy of Elite',"* THE HINDU, (June 9, 2017, 11.39 PM IST) https://www.thehindu.com/news/national/centres-aadhaar-affidavit-in-supreme-court-welfare-of-masses-trumps-privacy-of-elite/article18951798.ece; and see the Preamble of The Aadhaar Act.

[65] *Banks Can Use Aadhaar for KYC with Customer's Consent: RBI*," (May 29, 2019,11:51PM IST) https://economictimes.indiatimes.com/industry/banking/finance/banking/banks-can-use-aadhaar-for-kyc-with-customers-consent-rbi/articleshow/69568435.cms

[66] Biometric Attendance System Manual 2018

[67] *E-Governance Standards*, STANDARDS FOR E-GOVERNANCE APPLIANCE, STQC DIRECTORATE, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA, (Jan 18,

Biometrics are also used in payment gateways or apps such as BHIM Upi by the government of India where we can use our fingerprint to unlock the app and transact with money. In India, other common uses of biometric data are also done such as usage for authentication and identification and as access control tool for home security appliances, mobile phones, computers, secure documents and others. We don't particularly see law enforcement agencies having a biometric database or doing profiling in India; however, work spaces, companies , military and research organisations are nowadays prone to use biometric data authentication systems in conjecture with other traditional systems to secure access to confidential data, risky areas or restricted areas.

(A) Legal Framework in India

The present regulation which governs biometric data usage in India is the IT Act of 2000[68] and the 'Privacy Rules'[69]. The Rules defines 'biometrics' as the technologies which measure the human body physical characteristics such as 'voice patterns', 'fingerprints', 'facial patterns', 'eye retinas and irises', hand measurements and DNA for the purpose of authenticating the identity of a natural person.[70] It also characterises such data under sensitive personal data or information.[71] The Privacy Rules provides for the collection, retention transfer and disclosure of sensitive information. It provides in Section 4 of the Rules that anybody corporate must provide for a very clear privacy policy regarding the handling of sensitive data that details the information on type of data that has been collected and the purpose for which it has been collected and that policy must be published on the body corporate's website and give the view of a clear statement of the practices and policies of the company or entity.[72] The rules provide that consent must be taken from the person whose biometric data is to be used in writing and that such information can only be used for necessary, lawful purposes and the onus is on the body corporate to make the person aware that his data is being used and collected for the stated person and who are the identifiers and retainers of his data and their particulars.[73] The institution or organisation is also only allowed to retain data for an amount of time as is

2021, 10:53 AM) http://egovstandards.gov.in/biometrics

[68] THE INFORMATION TECHNOLOGY ACT, 2000, Act no 21 of 2000

[69] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, India

[70] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, §2 clause b, 2011 (India)

[71] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, § 3 sub-clauses vi, 2011 (India)

[72] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, § 4, 2011 (India)

[73] Sec 5 (Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, § 5, 2011 (India)

 [ISSN 2581-5369]

necessary for the purpose which such data is required and it must require permission of the owner before sharing or transferring biometric data with others except for government agencies who will seek such data by clearly stating the purpose of seeking the biometric data of a person.[74] The Rules also provide for reasonable security practices and procedures in Section 8 of the Rules of 2011.

The Personal Data Protection Bill 2019 is a piece of legislation that has been inspired by the GDPR of the European Union and it also imports elements of the landmark judgment of 'Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors'.[75] It also deals with biometric data under sensitive data same as the Privacy Rules of 2011. The Bill seeks to regulate the processing of personal and sensitive data. Chapter II provides for the obligations of a data fiduciary or a person who will collect and process data. It provides that personal data must only be processed for lawful purpose and such personal data will lone be composed to the necessary extent with notice being given to the data principal – i.e., person whose data is to be collected which will encompass certain information- purpose for collection and process, what kind of data is being collected, right of principal to withdraw the consent given to process such data and the process for withdrawal, details of data fiduciaries and other entities with whom the data may be shared, his rights under the Bill and other information provided under Section 7 of the Bill.[76] The bill also provides that there will be time limit to the retention of data and data can only be retained for a necessary period to satisfy the purpose for which the data was obtained.[77] The Bill also provides for the Rights of person whose data is obtained in Chapter V and the rights are of access to the personal data and confirmation of it, also correction of such data in case there is mistake and erasure of such data, ability access such data given to the fiduciary in course of use of services and others. The Bill offers for consent of the person before obtaining any biometric data, especially that of the children. The Personal Data Protection Bill, 2019 also provides for measures regarding transpaerancy of privacy policies and lay down guidelines on processing of data, maintaining of records, assessment of data protection impact, maintain transparency in their processing of biometric data, allow for withdrawal of consent, protect data and prevent misuse and others. The Bill also provides for periodic analysis of the safeguards issued by a data fiduciary. One of the biggest and important contribution of this Bill

[74] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, § 6 clause 1, 2011 (India)
[75] Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors ,2019 1 SCC 1
[76] Personal Data Protection Bill, 2019, § 7, Bill no 373 of 2019, (India)
[77] Personal Data Protection Bill, 2019, § 9 Bill no 373 of 2019, (India)

 [ISSN 2581-5369]

is the establishment 'Data Protection Authority of India' under Chapter IX of the Bill, providing for redressal for breach of privacy and security of data.

In case of biometric data the most important element in the above piece of rule is that of consent which is that to collect, process, share, transfer or do anything with the biometric or personal data of a person, he must be able to give clear and free consent that is not unambiguous with him being informed of the purpose and all other necessities and particulars regrading how his data will be used, processed , shared or anyway managed.[78]The personal data so collected must not be used in excessive i.e., it must follow the principle of proportionality. The Bill also provided that consent for personal data can be withdrawn. The exceptions to consent on biometric data are any Government action, court action, action done to comply with legal order, emergency action or to an extent certain employee related action.[79]

VI. LEGAL CHALLENGES, ISSUES AND IMPLICATION REGARDING BIOMETRICS IN INDIA

In India, we have seen a resurging use of biometrics after 2011 and it has been used in workforce, military and schools and others. The Indian Government's largest scheme of UIDAI or Aadhar Project that aimed to link the biometric data of individuals in a centralized scheme to provide people with government benefits was launched in 2009. It is a twelve-digit unique number issued by the UIDAI (Unique Identification Authority of India) to the citizens of India, free of charge that requires biometric information along with other demographic data to form a national identity system with the help of which the government provides benefits and other facilities to the people. One of the main aims of the Government in introducing the Aadhar Scheme was to stop corruption in distribution of government funds through food cards, housing subsidies , healthcare. To now, avail any facilities under government schemes it was mandatory to use Aadhar and therein lies the problem.

(A) Biometric Data Acceptance in authentication and identification

The first issue is that of Biometric Data Acceptance in authentication and identification uses human data and hence is flawed. It is known that fingerprints authentication system has problems, i.e., cuts and bruises and moisture content may change the ridge structure of fingerprint and also it is inconvenient for children to use fingerprint authentication as the

[78] Suneeth Katarki , Namita Viswanath and Ivana Chatterjee, *The Personal Data Protection Bill, 2018 - Key Features And Implications*, INDUSLAW, (15 August 2018), https://www.mondaq.com/india/data-protection/727550/the-personal-data-protection-bill-2018--key-features-and-implications
[79] Personal Data Protection Bill, 2019, Chapter III Bill no 373 of 2019(India)

fingers will grow and change over time.[80] Also more importantly persons with disabilities are facing problem. While the 'Unique Identification Authority Of India, Regulations, 2016' in Rule or Section 6 provides exception for persons with disabilities or injury who cannot provide with fingerprint, by providing for iris scans, it does not address the issue of persons who has disability or injury after getting Aadhar. Many persons with disabilities have been deprived of getting their Aadhar or their Aadhar are being rejected in spite of the provisions because they need fingerprints and many of the operators are not trained that one can use only one component of biometric for persons with disabilities. The law is also silent on the changing nature of fingerprint and iris biometric data, only chalking it up to upgradation of biometric data to be done by the person at his own cost from time to time. Researches have repeatedly said that the same iris may register differently due to various variables such as gaze, effects of contraction and dilation of iris, motion blurriness, angle of the camera and even fingerprints' ridges may register differently.[81]It only provides for minor fixes and is completely silent on what will be the consequence of the biometric data of persons who have been injured or suffered disability in hands or eyes after the making of Aadhar.[82]

There has been a lot of issues regarding fingerprint registration in Aadhar and many cases has been reported in the newspapers. We see the case of Motka Manjhi, from Jharkhand whose fingerprint was not registering in the new system and hence was deprived of food subsidies from the ration shop. He needed to do an online update of his fingerprint, however for that he needed to go to a distance of more than 7 kms from Dumka, his village to a private centre with no guarantee of even getting the work done in one day due to poor network in the centres. Nowadays, low-income groups need Aadhar to get subsidised food grains whereas before they needed only paper documents. The problem of Manjhi is very common, what with common network outrages in centres, poor connectivity and remoteness of centres along with existence of sparing permanent Aadhar Enrolment Centres which has led to starvation and loss of the common people. Most of the times people don't understand what has gone wrong and who to approach to fix the problem and the moreover even if somehow one manged to approach the authorities the system in neither cost -efficient nor speed efficient resulting in huge losses to people surviving on support of welfare scheme. Although a grievance redressal has been set up under Section 32 of 'Aadhar (Enrolment and Update) Regulations , 2016' and it has been said

[80] Gawande, Ujwalla & Golhar, Yogesh & Hajari, Kamal. (2017). Biometric-Based Security System: Issues and Challenges. 10.1007/978-3-319-44790-2_8.
[81] *Id.* at 79
[82] AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,52-62 (Al Now Institute, 2020), https://ainowinstitute.org/regulatingbiometrics.html

that grievances should be addressed by service providers in a timely and appropriate manner[83] in the Code of Conduct for Service Providers, it not done so quickly. In Jharkhand, along with the case of Manjhi who died due to starvation outside his home on May 22, because he could not afford to go to the centre; activists dug up 13 other cases of death related to starvation due to failure of the Aadhar system.[84] We even see the shocking case of death of Santoshi Kumari, because her family's ration card got cancelled due to not linking it with Aadhar. Also, due low fingerprint generation of the elderly people i.e., 20% or low fingerprint generation many elderlies, have repeatedly failed to register for Aadhar cards losing out on pension schemes and only after intervention by the forum of senior citizens who held meeting with the Tehsildar.[85] We see from the above cases that although Aadhar has been framed by the Government its implementation is quite poor. There is need for more comprehensive law for implementation of standard systems and monitoring use of such systems that will authenticate Aadhar, although according to the Regulations service providers must use systems according to the specifications of the authority. There also needs to be a quicker grievance redressal system and setting up of a local contact point instead of a central contact point, with permanent enrolment centre for updating biometric data if possible, at every ward or within a distance of 2km.

Nowadays, we also use fingerprint and facial recognition technology in our mobiles and laptops for many apps or services. Even here there is issue regarding changing fingerprints and non-registering of face which prevents users from accessing their data. The Government of India is still silent on comprehensive laws and policies that will govern such private data entities and the standards of biometric system that they should follow. The Personal Data Protection Bill 2019 is still a bill and has not been made into an Act and even that is silent on procedures that the data fiduciaries or processors should follow in case there is mismatch of data, it only provides that a person has the right to correct their data, but not what procedure should be followed regarding the data correction.[86]

(B) Right to Privacy

[83] Aadhar (Enrolment and Update) Regulations , 2016, Rule 7, Schedule V , Code of conduct of Service Providers, No 2, Acts of Parliament, 2016 (India)

[84] Rebecca Ratcliffe, *How a glitch in India's biometric welfare system can be lethal*, THE GUARDIAN, Wed (10 October, 2019, 10:00 BST), https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation

[85] Nisha Nambhar, *Senior citizens with fading fingerprints get UIDAI relief*, TIMESOFINIA.INDIATIMES.COM., (Dec 1, 2017, 1:49 PM) http://timesofindia.indiatimes.com/articleshow/61877572.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[86] Personal Data Protection Bill, 2019, § 25 Bill no 373 of 2019, (India)

One of the most hyped about issue regarding Aadhar was the issue of data privacy and the right to privacy. People were worried about government monitoring because Aadhar could take their biometric data and compulsory linking was made to Banks and for government schemes. Due to this Justice Puttaswamy case was filed and in the Puttaswamy v Union of India (Puttaswamy I)[87] right to privacy was declared to be an inherent right of a human being and that it comes under the ambit of Article 21 regarding right to life and personal liberty. While the above judgment recognised the right to privacy through judicial interpretation; however, in the case of 'Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors'[88] , Aadhar Act of 2016 was held to be constitutionally valid but restrictions were imposed that it could only be used by the Government to establish the identity of individual to allow him/her to receive government schemes but did not allow private institutions to establish the identity of any individual in pursuance of profit, business or contract. It also ruled against the mandatory linking of Aadhar with other entities. However, still today most banks are requiring linking of Aadhar cards to bank accounts through KYC. In fact, nowadays Banks compulsorily require Aadhar to open new accounts for new customers or to process loans. The area is still fuzzy as to why such biometric data is necessary by the bank when other options to ascertain the identity of the person are present. It has been encouraged saying that linking of Aadhar will help government directly transfer subsidies and prevent tax evasion.[89] Banks like the Indian Central Bank have open merchant outposts where people can go link their bank accounts with their Aadhar Numbers with fingerprint sensors and scanners present at the outpost and after doing so the amount of money owed to merchant can be directly credited to him.[90]

Aadhar can be used to do secure market transactions.[91] However, there has been various reports in newspapers and agencies that Aadhar data has been breached and duplicate identity cards has been used to link to the person's bank account to commit identity theft. Hackers have been able to get to the data base of Aadhar and use the cards to link bank cards and other cards and print out duplicate cards to get access to information and commit identity theft.[92]

---

[87] Puttaswamy v Union of India , Puttaswamy I, Writ Petition (Civil) No. 494 of 2012,
[88] Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors, 2019 1 SCC 1
[89] Konark Sikka, *Making Aadhaar Mandatory: Benefits and Drawbacks*, DAILY O (Mar. 25, 2017), https://www.dailyo.in/politics/aadhar-card-uidai-bjpfinance-bill-2017/story/1/16363.html; PTI, *Aadhaar-PAN Link Will Prevent Tax Evasion, Says FM Arun Jaitley*, BUSINESS TODAY, (July 25, 2017, 4:00 PM IST), https://www.businesstoday.in/current/economy-politics/aadhaar-pan-link-tax-evasion-says-fm-arun-jaitley/story/257077.html
[90]Madison Julia Levine, *Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States*, 73 U. Miami L. Rev. 618 (2019): https://repository.law.miami.edu/umlr/vol73/iss2/10
[91] *Id.* at 89
[92] *Id.* at 89

 [ISSN 2581-5369]

Another concern with Data privacy at the present till the 'Personal Data Protection Bill 2019' is not turned into an act is the procuration of biometric data by various mobile apps, mobile and laptop companies, various institutions and others for exams purpose, workforce attendance and others. The only law at the present moment is the Information Technology Act, 2000 and The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules) which regulates any data breach and only provides for compensation, for a limited area of biometric data and limits it only to electronically accessed or issued information. Although the Privacy rules provide for collection, consent , statement of purpose for data collection, retention of biometric data and dissemination and storage of such data, it still gives more freedom to the bodies corporate to decide on privacy policies with which they will govern such biometric data. There are glaring loopholes which can be used to access biometric data for nefarious purposes. The laws are not designed for data protection and does not deal with the procedures, guidelines, principles, rules, regulations, standards that entities need to follow for the usage and collection of biometric data from people.

(C) Data Security and Ethical issues

There is a huge issue of data security in India. India at the present moment does not any law that protects data from unauthorized uses. The IT rules 2011 and IT Act 2000 are not sufficient as they do not mention any transmission of data to third party. India has moved towards common use of biometric data, however still now we do have rules that are in force regarding protecting such data from unauthorized use. Aadhar came into force without any specified legislation and it is mandatory for people to get Aadhar to get government benefits. Recently Government of India announced that it will require Aadhar to verify the identity of the persons who will registrar to receive Covid-19 vaccination.[93]It is almost of a coercive nature without any heed to whether a person is able to get an Aadhar card or not. Government in planning on using biometric data for e-governance functions and even the recent vaccination will use mobile app CO-Win App to register persons for vaccination with biometric data. However, it does not take in to account that there are still people in India who do not have Aadhar Card, whose biometric data have changed and they may not have access to smartphones or suffer from poor net connectivity, even when the Supreme Court in Puttaswamy Judgment held that Aadhar cannot be a precondition or mandatory for citizens to receive such welfare benefits of

[93]Edited by Kritika Bansal, *Aadhar Authentication To Be Done Via CoWIN App To Avoid Proxies in COVID-19 Vaccine Drive,* INDIA.COM NEWS DESK, INDIA.COM, (January 10, 2021, 9:40 PM IST) https://www.india.com/news/india/aadhaar-authentication-to-be-done-via-cowin-app-to-avoid-proxies-in-covid-19-vaccine-drive-4322003/

 [ISSN 2581-5369]

the government.[94] It is totally against ethics to drive such a huge vaccination drive with biometric data usage with proper laws laying down the proper procedures, security measures regarding usage of such biometric data and rules as how such data will be obtained. In India, unlike GDPR consent does not have a major part in case of usage of biometric data. There are at the present moment no guidelines or procedures that govern the sharing of personal biometric data with other parties. Banks especially linked Aadhar and biometric authentication system with payment systems without any policy governing the usage and storage of such biometric data. Even companies are free to implement procedures which they wish to protect biometric data, even if they use data protection that is negligible in nature, they will only be given penalty and asked to be given compensation.[95] Data Security laws in India at the present moment regarding biometric is hardly present and there are no set standards or protocols that govern the usage of such data.

(D) Data Privacy and Ethical Issues

We see in the above paragraphs that Indian Law is seriously lacking in protecting the privacy and security of data, ensuring right to privacy and efficiency and comprehensiveness of law at the present moment. The legal issues in India regarding biometric data is mainly regarding right to privacy, right against monitoring, ethical right and right to live, data privacy and data security rights. There are also other issues that are of importance mainly, many people fear that biometric data will be used for profiling of a person without his consent and knowledge and try to gather other sensitive data like a persons' habits, sexuality, tribe and a persons' preferences in government or other institutions' database. Such databases will be able to track a person completely and he/she will be monitored by different agencies. At present there are no laws in India that limit the gathering of such data linking, monitor the activities of the parties and prevent them from profiling. Sensitive personal data is tracked across so many platforms and there is no law at the present moment to limit the actions of such data processing units or parties. The Privacy rules only provide that consent is necessary to gain access or to transfer biometric data, but it does not account for Third-party agreements or licences which are already a part of the contract at time of obtaining biometric data. Basically, when obtaining the data from a person an institution may already have a clause in the contract which would allow the

[94] Madison Julia Levine, *Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States*, 73 U. Miami L. Rev. 618 (2019): https://repository.law.miami.edu/umlr/vol73/iss2/10

[95] Madison Julia Levine, *Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States*, 73 U. Miami L. Rev. 618 (2019): https://repository.law.miami.edu/umlr/vol73/iss2/10

 [ISSN 2581-5369]

institution or entity to transfer the data to parties licensed with them or in contracts with them. This has created huge problem in India especially regarding biometric data and left it extremely vulnerable.

Another legal question arises is the access to such personal data by the party whose data has been collected. India at the present unlike GDPR does not have any law that allows individuals to ask any other party about the personal data, its quantity, and its usage that it has of that particular individual. It creates confusion and breach of trust and their fundamental rights not allowing people to know what kind and quantity of personal data has been stored with a company or institution and with whom such data has been shared and that data has been used for what kind of purposes.

Although the Privacy Rules of 2011 provides for consent and information given to the parties before biometric data is used most click-wrap user agreements require the parties to immediately agree to policies that require biometric authentication and even more than providing biometric data has become compulsory in order to use certain functions and there is no option to opt-out of such data. For example, nowadays to open bank account in certain banks it has become compulsory to register Aadhar and if we do not give Aadhar number, an account will not be opened; which means that most people opt to provide Aadhar number to the bank to open the account and along with that agree to all its privacy policies. This cannot be said to be completely informed consent as there are huge number of bank rules and regulations which a layman cannot understand and such consent can only be said to a certain sort of coercive content.

The new Personal Data Protection Bill 2019 has brought in many aspects following the GDPR of the European Union, however there is still gap in the frameworks and moreover the bill has in the parliament for too long without being turned into a law till now.

6.5 Gaps in the framework:

India has still to enforce a data protection law based on human rights approach to prevent misuse of data and to monitor and set limits to data use according to UN standards.[96] The Personal Data Protection Bill 2019 although follows UN standards and GDPR law, there are still some gaps in the framework of the Bill. Though the law follows the principles of transparency, consent, accountability, principle of proportionality and others, one of the main

[96] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute.

 [ISSN 2581-5369]

lacunas is that consent is not necessary for government or court necessitated functions, and it does not expressly put limit on the government for which it can access the personal biometric data, it can access data for any legislative function, issue of certificate or license, any function authorised by law, or if nay any benefit is awarded by the government. [97] While, it may seem like crystal clear, the government can access the biometric data for any reason it may want provided it can show government function or any legal order and people will be left without a choice as to whether they want the government to access their data for a particular purpose and they will also not be informed if their data has been used by the government for treating with any difference or for profiling.

In comparison with other countries, the biometric data can be accessed without consent for reasonable purposes for things like public interest, fraud prevention, mergers and acquisitions, credit lending, network and information security, recovery of debt, and others.[98] Also, while the Bill adopted the principle of 'right to be forgotten'[99], the Personal Data Protection Bill 2019 does not completely adopt the principle and allow a person complete control of erasure of his data or allow them to restrict any user; without the permission of Adjudicating Officer and even then, erasure is only possible when certain conditions laid down in Section 27 of the Bill are fulfilled.[100] As we see the Chapter III of the Bill we mainly come to realize that actually many parties can access our biometric data without our consent and the bill is completely vague on the basic reasons, as it does not cap an actual limit on who can access personal biometric data without consent, and put protocols to prevent the use of excessive force. There is ambiguity in the law especially in Chapter III of the Personal Data Protection Bill, 2019. Indian law at the present moment does not follow the UN standards of having privacy policies designed by the Biometric Institute.[101]

VII. CONCLUSION

In today's world where everywhere, there is digitalization and people want easy and speedy access to things, biometric data usage in inevitable. Biometric data usage is being built into the fabric to everyday appliances and devices and objects used by people and is soon becoming the norm of the 21st century. In the near foreseeable future, it will soon become a norm to do everyday functions with usage of biometric data. People find it convenient to use biometrics

[97]Personal Data Protection Bill, 2019, Chapter III, Bill no 373 of 2019(India)
[98] Personal Data Protection Bill, 2019, § 14, Bill no 373 of 2019(India)
[99] General Data Protection Regulation, 2018, Regulation (EU) 2016/679, 2018 (EU)
[100] Personal Data Protection Bill, 2019, § 27, Bill no 373 of 2019(India)
[101] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute

 [ISSN 2581-5369]

because of its uniqueness and security that no one else will be able to use biometrics except for that person and there is no hassle to remember any data.

However, with the growing popularity of biometrics, there is also the fear regarding biometrics since biometrics are associated with the body. Most people have the concept that bodies are the most private and holy. There always has been fear of misuse of biometric data and also there has been many cases where privacy of others has been breached and government and other organisations has collected biometric data without consent and letting people know that government or other parties has been disseminating private biometric data to commercial and other organisations. Many people feared profiling and cataloguing by the government or other agencies. Hence many regulatory bodies have come forward to standardize the protocols and laws regarding biometric data and their use with other organisations. Forefront among them is BIPA, ISO and others.

We see the development true and comprehensive standards regarding biometric data laws towards the start of 2011 after the incident of 9/11 in USA. Although use of biometric data progressed comprehensive laws derived after the GDPR and the United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism in 2018 which gave stellar standards in regards to practices regarding sensitive personal data and biometrics data. We see that many countries are yet to implement comprehensive privacy and protection laws regarding biometric data.

(A) Findings

1. Whether India has stellar standards or protocols to deal with privacy and security of biometric data?

Ans. India at the present moment does not have stellar standards or protocols to deal with privacy and security of biometric data. Aadhar is still being denied to many persons due to lacuna in operational laws with the laws being silent on what biometrics would be used if the biometrics of fingerprints and iris does not work. The law has prescribed certain standard of systems but such systems often result in low grade biometrics and sometimes fingerprints not registering with certain systems. Indian also does not follow the recommendations of United Nations in establishing standard protocols and allows the body corporate to set the standards and procedures.

2. Whether the present Indian Legal Framework is capable of handling the legal issues put forward by biometric data?

 [ISSN 2581-5369]

Ans. The present Indian Legal Framework is not capable of handling the legal issues put forward by biometric data . The IT Act 2000, and Privacy Rules 2011 are mainly regulation regarding Information Technology, and not biometrics. Although biometrics has been mentioned in the Privacy Rules, 2011 and completely left out of the IT Act, 2000, the rules are mainly regarding privacy and security breach of data and not a data protection law. The Privacy rules simply leave in on body corporate to form procedures and privacy policies with which they will govern sensitive personal data, even biometrics and does not provide for any government limitations

(B) Hypothesis

The main hypothesis is that Indian legal framework does not have stellar standards on the privacy and security of such biometric data is confirmed through see the implications on data privacy and security standards of The IT Act of 2000, Aadhar Act, 2016 and the Privacy Rules of 2011. India does not have exhaustive legal framework to tackle with problem of using Biometric data and India needs both strict and flexible regulatory framework to mitigate the challenges and impact faced in Biometric data. In India as we see the current laws especially Privacy Rules 2011, we observe a lot of lacuna in the laws that basically allow many third parties to access data, and the privacy policy protecting data is completely dependent upon the organisation instead of having and guidelines from the government. And the upcoming law of 'Personal Data Protection Bill, 2019' we can see especially through Chapter III, that there is vagueness on the consent section, which undermines the whole act allowing almost everyone to get access to biometric data of a person without consent, especially the government and allow them to use such data without letting the person know. This also hampers the privacy and security concerns of the people regarding biometric data, especially when in emergency anyone can access the biometric data of a person without his/her consent. Also, the doctrine of right to be forgotten, a pivotal principle of biometric data is not implemented completely and a person will only be allowed to stop distributing his data or erase his data upon the will of the adjudicating officer. This also violates their right to be forgotten from the system This is why there is a need to bring forth exhaustive and clear flexible but strict laws that defines the duties and responsibilities and rights and obligations in a proper manner. Hence the hypothesis is hence proved.

(C) **Recommendations**

The paper would like to put forward certain recommendations

 [ISSN 2581-5369]

In conclusion, we can say that biometric data usage in India has many legal issues and the laws need upgradation and sooner implementation of pending bills with major changes to resolve core issues and have a law that is most comprehensive and safe and that protects the rights of the citizens.

*****

 [ISSN 2581-5369]

VIII. BIBLIOGRAPHY

- Aadhaar-PAN Link Will Prevent Tax Evasion, Says FM Arun Jaitley, BUSINESS TODAY, (July 25, 2017, 4:00 PM IST), https://www.businesstoday.in/current/economy-politics/aadhaar-pan-link-tax-evasion-says-fm-arun-jaitley/story/257077.html
- A.K. JAIN, et al P. FLYNN & A.A. ROSS eds, HANDBOOK OF BIOMETRICS 1-22 (2nd ed Springer 2007)
- Alison Grace Johansen, NORTON LIFELOCK, (January 18, 2021 8.29 PM), https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html
- AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,52-62 (Al Now Institute, 2020), https://ainowinstitute.org/regulatingbiometrics.html
- Banks Can Use Aadhaar for KYC with Customer's Consent: RBI," (May 29, 2019,11:51PM IST) https://economictimes.indiatimes.com/industry/banking/finance/banking/banks-can-use-aadhaar-for-kyc-with-customers-consent-rbi/articleshow/69568435.cms
- Biometric Attendance System Manual 2018
- Biometrics, History of biometrics, HOMELAND SECURITY, (Jan 18, 2021, 8.00AM) https://www.globalsecurity.org/security/systems/biometrics-history.html
- Busch, Christoph. "Facing the future of biometrics. Demand for safety and security in the public and private sectors is driving research in this rapidly growing field." Vol 7 Spec No EMBO reports, S 23-5. (2006) doi:10.1038/sj.embor.7400723
- Directive 95/46/EC of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 1995, Articles 6 & 6.1 (d)
- Edited by Kritika Bansal, Aadhar Authentication To Be Done Via CoWIN App To Avoid Proxies in COVID-19 Vaccine Drive, INDIA.COM NEWS DESK, INDIA.COM, (January 10, 2021, 9:40 PM IST) https://www.india.com/news/india/aadhaar-authentication-to-be-done-via-cowin-app-to-avoid-proxies-in-covid-19-vaccine-drive-4322003/
- E-Governance Standards, STANDARDS FOR E-GOVERNANCE APPLIANCE, STQC DIRECTORATE, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA, (Jan 18, 2021, 10:53 AM) http://egovstandards.gov.in/biometrics

 [ISSN 2581-5369]

- Els Kindt, Biometric applications and the data protection legislation, The legal review and the proportionality test , 31 DuD, Datenschutz and Datensicherheit, Schwerpunkt, 166-170 (2007)
- Gawande, Ujwalla & Golhar, Yogesh & Hajari, Kamal. (2017). Biometric-Based Security System: Issues and Challenges. 10.1007/978-3-319-44790-2_8
- General Data Protection Regulation, 2018, Art 4, Regulation (EU) 2016/679, 2018 (EU)
- History of Biometrics, REFACES.COM , https://recfaces.com/articles/history-of-biometrics (Jan 17, 2021, 8.00AM)
- The International Covenant on Civil and Political Rights (ICCPR), United Nations General Assembly Resolution 2200A (XXI), Article 17, 1966
- Krishnadas Rajagopal, "Centre's Aadhaar Affidavit in Supreme Court: 'Welfare of Masses Trumps Privacy of Elite'," THE HINDU, (June 9, 2017, 11.39 PM IST) https://www.thehindu.com/news/national/centres-aadhaar-affidavit-in-supreme-court-welfare-of-masses-trumps-privacy-of-elite/article18951798.ece; and see the Preamble of The Aadhaar Act
- Konark Sikka, Making Aadhaar Mandatory: Benefits and Drawbacks,DAILY O (Mar. 25, 2017), https://www.dailyo.in/politics/aadhar-card-uidai-bjpfinance-bill-2017/story/1/16363.html
- Madison Julia Levine, Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States,73 U. Miami L. Rev. 618 (2019): https://repository.law.miami.edu/umlr/vol73/iss2/10
- Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
- Rebecca Ratcliffe, How a glitch in India's biometric welfare system can be lethal, THE GUARDIAN, Wed (10 October, 2019, 10:00 BST), https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation
- Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview AI Has Promised to Cancel All Relationships with Private Companies," BUZZFEED, (May 7, 2020,6:50 PM ET), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies

 [ISSN 2581-5369]

- Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, (Jan 18, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2
- Suneeth Katarki , Namita Viswanath and Ivana Chatterjee, The Personal Data Protection Bill, 2018 - Key Features And Implications, INDUSLAW, (15 August 2018), https://www.mondaq.com/india/data-protection/727550/the-personal-data-protection-bill-2018--key-features-and-implication
- Types of biometrics, BIOMETRICS INSTITUTE, (January 18, 2021 8.29 PM) https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics
- United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter - Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute.

*****

 [ISSN 2581-5369]