INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

BIOMETRIC DATA COLLECTION IN INDIA: PRIVACY CHALLENGES

AUTHORED BY - ANKIT DAKSH
Research Scholar
Faculty of Law University of Delhi

CO-AUTHOR - PROF. RAMAN MITTAL
Faculty of Law University of Delhi

Biometric Data and Right to Privacy in India – Issues And Challenges

ABSTRACT

Technology has grown quickly over the past ten years, and we now use biometric data on a regular basis. In India, biometrics are employed in practically every area, from government and social services to banking, employment, and data access. The booming e-commerce market also makes use of biometrics. It is used to authenticate people's identities and identify them. The usage of biometrics is the new standard and is said to be the solution to many security issues. Biometric data is the most private and sensitive type of data, yet it also has the most system flaws and is vulnerable to several privacy, security, and authentication problems. India still lacks a thorough and inclusive biometric usage system that complies with international norms. This article's goal is to address the legal concerns surrounding the introduction of biometrics, identity, and authentication in India as well as how these factors interact with other factors including electronic transactions, e-commerce, and other activities. is to think about how they relate to one another. In order to comprehend the present issues and implications that have an impact on and shape the current situation, this document will discuss the general legal framework controlling such actions.

INTRODUCTION

This paper's goal is to investigate the legal issues surrounding the introduction of biometric identity and authentication in India as well as how these biometrics interact with other factors like e- commerce. I'm done now. In order to comprehend the present issues and implications that have an impact on and shape the current situation, this document will discuss the general

ISSN: 2582-6433

legal framework controlling such actions.

Today we find that photos, signatures and fingerprints must be uploaded via electronic media or the Internet. This is biometric data that is unique to an individual and is widely used in today's world. Beginning in the 18th century, large-scale development of biometrics began, especially for law enforcement and the military, and it gradually made its way into the civilian world. Since the 2000s, automated biometric authentication systems have attracted attention, and biometric data has begun to be widely used around the world for various purposes such as commercial transactions. At the same time, biometric protocols and committees began to be established to mandate biometric standards and protocols. During this time, an ISO committee was also established to help and shape the standardisation of biometric technology. However, most biometric legislation has been enacted since his 2015. In 2016, India launched the Aadhar program, which uses biometrics to form a national identity. 2018 also enacted an important European Union law called GDPR. This is one of the strictest data protection laws to date and also affects the use of biometric data.

Regarding the necessary use of biometrics by payment institutions, governments, law enforcement agencies, individuals, banks, etc., legal issues such as failure to register and accept biometrics, data protection, data security, privacy rights, and ethical issues raise people's concerns. pervasive in the mind of other. Biometric data is stored by the person you interact with, allowing them to access this data with the click of a finger. As a result, many questions have arisen about the privacy and security of that data and whether the current legal framework we have in place imposes good standards on how we process such data. increase. This article discusses the impact of such laws and legal issues related to biometrics.

CONCEPT OF BIOMETRIC DATA

The concept of biometrics or biometrics is not new and dates back to 500 BC. When the Babylonian Empire used biometrics on clay tablets by recording a person's fingerprints. In the past, faces and fingerprints were transferred to paper and used as a means of identification to access certain high security areas, or fingerprints were used to sign contracts, etc.[1] The concept of biometrics or biometrics isn't unused and dates back to 500 BC. When the Babylonian

[1] 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=

ISSN: 2582-6433

Domain utilised biometrics on clay tablets by recording a person's fingerprints. Within the past, faces and fingerprints were exchanged to paper and utilised as a implies of recognisable proof to get to certain tall security regions, or fingerprints were utilised to sign contracts, etc.

1965, the first signature recognition system was developed by a North American airline, and in 1974 the University of Georgia took a further step forward with a hand shape recognition system. Meanwhile, the FBI began using fingerprint authentication systems, and research into automatic facial recognition was underway. Additionally, Dr. Joseph Perkell created a fundamental prototype for a voice recognition system. In 1976, Texas Instruments used this prototype to create the first speech recognition system, which was then retested by the NIST speech group. The majority of the biometric technologies currently in use, including voice recognition, facial recognition, and fingerprint recognition, have been integrated at this point. Law enforcement and government agencies are also beginning to use biometrics, and in 1992 the NSA established the Biometrics Consortium, a consortium of academics, government agencies, businesses and other private sector members.

PRESENT CONCEPT OF BIOMETRIC DATA SYSTEM

1. Biometric Data

The current concept of biometrics consists of automatic biometrics and digital biometrics. Biometric data refers to an individual's unique physical, physiological, or behavioural identity characteristics captured as data through a biometric system. Biometric data includes fingerprints, iris, DNA, palm vein patterns, and more. This data is created by profiling biometric data samples obtained from individuals. An automated system scans the data and saves or saves it in a digital format that can be easily distributed through various channels. The preference for biometrics is primarily due to its uniqueness, as biometrics cannot be accessed or duplicated by others.

2. Types of Biometric Data:

In today's world there are certain and specific biometric data types relating to DNA that are common and can be used as biometric data. In First Generation There Are Fingerprints recognition, Finger Shape recognition, Iris recognition. Retina recognition, Ear Shape Recognition. Now in advanced or second generation there are behavioural aspects such as gait recognition(manner of walking),keystroke recognition, voice and speech recognition. In more

ISSN: 2582-6433

advance level there are certain practice which are analysing emotions of human beings by observing there activities.[2]

The Biometrics must contain certain features. They are:

- Universality- A modality or date must be found universally among all peoples of the world.
- Unique – Must be so unique that the chances of two people sharing the same data characteristic are completely negligible. Identical twins have different fingerprints and even signatures, even if they have the same face and DNA.
- continue: These should be stable and not erased over time. Even considering the human life cycle, the change should be negligible and still be stable over a period of time.
- Human faces change with age, but remain stable for at least three years after the age of five.

3. Application and uses of Biometrics

Biometrics and identification basically authenticates a person's biometrics to match a person's identity to profiles already in the system to grant access to documents or areas, government ID card authorisation, etc. is the process of making it available for other purposes. The system he uses generally functions in two ways. The first type of authentication is physical, while the second is distant. Utilizing modern biometric tools like fingerprint scanners, facial recognition systems, and iris scanners, physical authentication and identification are performed. This will scan your biometridata when you are physically present. This was probably done to give him access to something at this point. An example would be using a fingerprint scanner to unlock a laptop. Remote authentication is typically performed to identify and retrieve profiles.

The 21st century has witnessed a rapid increase in the use of biometric data. Sectors that have started using biometrics include government agencies and law enforcement for private and criminal identity verification, the military for identity verification and access control, the banking sector for customer and corporate identity verification, commercial industry, healthcare sector, mobile devices and laptops.

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

ISSN: 2582-6433

Biometrics and identification systems are primarily used in the banking sector and commerce. Banks collect digital and other photographs, signatures and fingerprints for common transactions, and this data is recorded in the bank's system. Banks now enable mobile and e-banking apps and encourage their customers to use them. Typically, these apps gather our biometric information. Today, punching machines and other biometric authentication systems are extensively used for facility access and attendance registration in government offices, schools, universities, businesses, and industries, among other places. Also, most hospitals and medical facilities now link patient records to government ID cards that use biometrics. At this point, research, scientific and technological developments, laboratories, and research, scientific and technological developments, protected by the use of “biometric systems and authentication, ensuring that only registered and authorised persons have access to authorised data. We must not forget to talk about development, laboratories, and advanced security and national security documents. and the information.

While discussing biometrics and identity, we must also discuss the present era of smartphones, laptops, PCs, AI-driven systems, and other devices. Smartphones are now biometric-enabled, allowing users to access their phones using facial and fingerprint recognition. Since only the user can open the phone and access its data, this increases safety and privacy. Tech firms are also manufacturing laptops and PCs quickly that employ fingerprint and facial recognition for biometric identification. The MacBook is unlocked using Apple ID and Apple Pay using a fingerprint recognition device on an Apple MacBook Pro. While HP, Samsung, and DELL employ fingerprint and facial recognition, Lenovo uses his FIDO (Fast Identity Online) system. Additionally, there is a rise in the adoption of home security systems like fingerprint sensors, facial recognition, and voice recognition locks and doors. With the advent of technologies such as SIRI, Google Voice, and voice recognition technology, ALEXA has operated many home and office devices, documents, accounts, etc., leveraging these technologies that store personal information along with biometrics. I was. shopping, operating cars, machinery, etc. With just one voice command, you can ask Alexa to buy an item on Amazon or send an email to Siri. These days, even entrance exams use biometric data to verify that candidates are themselves legitimate candidates. As you can see, biometric systems are widely used in all aspects of our everyday life, from banks to companies, government agencies, schools, and other institutions. To stop this kind of data misuse, certain steps and rules are needed to penetrate into our daily life.

ISSN: 2582-6433

IV. BIOMETRIC REGULATIONS IN DIFFERENT COUNTRIES OF THE WORLD

A. UNITED KINGDOM- Introduction

The UK has released comprehensive rules and regulations aimed at legalising data protection and protecting individual privacy rights. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 are the current data protection regulations in the UK. The GDPR forbids the collection and use of biometric data in order to automatically recognise a natural person. Privacy and data protection in the UK are protected by Article 8 ECHR (European Convention on Human Rights). Data protection rights in the UK are therefore not only a privacy safeguard, but also protect the fundamental rights enshrined in the ECHR.

B. EU GDPR AND UK GDPR

In the UK, GDPR is the main data protection law, that promotes comprehensive harmonisation of information security regulations across all national laws of EU member states. EU General Data Protection Regulation (GDPR) obligations were introduced into UK law in May 2018 by the Data Protection Act 2018. The UK will then leave the European Union (EU) via Brexit on her 31st December 2021 and will no longer be governed by her EU's GDPR domestically after Brexit. Instead, the UK now has its own version of the GDPR, known to the public as UK-GDPR. However, for EU nationals, UK courts will continue to apply the EU GDPR. The UK GDPR came into force on January 31, 2020.

C. UNITED STATES OF AMERICA - Introduction

The US Biometrics Protection Act reflects a typical set of standards, also known as "Fair Information Practices Standards" or FIPPs (Fair Information Practices Standards). In the United States, various protective regulations have been developed through FIPP.

Biometric data Privacy Act 2008 (BIPA)

As I mentioned earlier, the United States does not have a comprehensive biometric data protection law regarding the right to privacy. For this reason, since 2008, US states have relied on biometric data privacy laws, with Illinois being the first of the 50 US states to pass. Many states, e.g.: B. US Department of Internal Revenue, Washington, etc., have integrated protections for biometric data related to privacy rights in light of BIPA. This is because BIPA avail for protecting biometric data in relation to privacy rights. BIPA is unique in that it allows

ISSN: 2582-6433

victims the right to private litigation. BIPA is an Illinois resolution that governs the collection, use, maintenance, and disposal of biometric data. The Illinois legislature authorised BIPA to combat the growing use of biometrics by organisations to facilitate financial transactions and security screenings. The rationale for BIPA is to provide unique security for such data, on the one hand to reduce the risk of mass fraud, and on the other to encourage the general public to participate in biometric exchanges.[3] BIPA applies broadly to all private entities operating or conducting business in Illinois, regardless of whether that entity resides in Illinois.

D. BIOMETRICS DATA SYSTEMS IN INDIA

The biometric system is used not only in Aadhar, India but also in schools, universities, workplaces, smartphones, laptops and many other devices. The Government of India has introduced a punching machine that registers attendance by fingerprint. The Handbook of Biometric Attendance System 'BAS' released by the Government of India in 2018 states that biometric attendance will be recorded through registration of BAS employees and deployment of devices and equipment. terminals such as keypress, desktop fingerprint recognition, and iris recognition.[4]

Legal Framework in India

According to section 4 of the privacy rules 2011[5], a corporation should have a privacy policy, which is freely accessible to all visitors on their website, declaring clearly about purpose, use, storage of data collected from individuals. It must also provide for the purpose for which this data has been taken from the user or consume. The declaration regarding privacy policy most contains the policy and practices of the company regarding private data collected. it also stipulates that the corporation is bound to seek and get consent of individual providing such data, in written form. The data thus collected in above mentioned ways can be used only of a lawful purpose.

Protection of data is one of the main concern, the onus and responsibility to such protection is on the corporation collecting and storing them. Any institution or company collecting and storing data for any purpose must make it sure that such collection and storage not for eternity but for a limited period of time. If for any purpose a retainer has need to share or transfer the

[3] Michael Hintze, In Defense of the Long Privacy Statement, 76 MD. L. REV. 1044 (2017)
[4] Biometric Attendance System Manual 2018
[5] Rules under The Information Technology Act, 2000

ISSN: 2582-6433

data with any other entity then previous consent of the individual whose data has to be transferred must be managed to acquired. There are some exception to this consent rule in case of some government agencies for security and intelligence purpose. A corporate body or institution other than there agencies are liable under section 8 of the rule of 2011, if they are caught to violating the the dictate provided in section 4 of the rule. The government of India had introduced a data protection bill in 2022 which was in accordance with GDPR of European Union and also in consonance with Puttaswamy Judgement of Indian Supreme Court.[6]

Additionally, it analyses biometric information in compliance with 2011's Privacy Rule for Sensitive Data. The measure aims to control how private and confidential information are handled. The responsibilities of the data administrator, or the individual who will gather and handle the data, are covered in Chapter II. It states that private data will only be used for legitimate reasons and that it may only be consolidated to the degree required with the consent of the data controller, or the owner of the personal details. Particular information will be gathered and used in the data.

The trustee's freedom to revoke permission for this data analysing and removal process, the sort of data gathered the gathering and utilisation of the data, contact details for the data trustee and other organisations with whom the data may be shared, the trustee's rights under the Bill, and additional details stipulated under section 7 of the Bill are all covered.[8] The bill also stipulates that there will be a data retention period, and that data can only be retained for as long as is necessary to fulfil the purpose of data collection. The measure also establishes the rights of individuals whose information is obtained under Chapter V, including the ability to access, amend, and delete their personal information. The ability to access such data is provided to the Trustees in connection with the use of the Services and the like. The bill proposes one person's consent before any biometric data is taken, especially of children. The Personal Data Protection Bill 2022 also provides measures related to privacy policy transparency and establishes guidelines for data handling, record keeping, impact assessment data. privacy, maintaining transparency in the processing of biometric data, the ability to withdraw consent, protect data and prevent abuse and others. The bill also provides for regular analysis of guarantees by data controllers. One of the largest and most important contributions of the Bill is the establishment of the 'Indian Personal Information Authority' under Chapter

[6] Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors ,2019 1 SCC 1

ISSN: 2582-6433

IX of the Bill to provide remedies for privacy and data security breaches.

CHALLENGES, ISSUES AND IMPLICATION REGARDING BIOMETRICS IN INDIA

(A) Biometric Data Acceptance in authentication and identification

The first problem is that accepting biometric data is flawed because human data is used for authentication and identification. Fingerprint authentication systems are known to have the following problems: Cuts and bruises and moisture levels can change the structure of your fingerprint. Fingerprint authentication is also inconvenient for children because their Fingers grow and change.

More importantly, people with disabilities face problems. India Unique Identification Authority Regulations, 2016 provides exceptions for disabled or injured persons who apply for an iris scan and are unable to obtain fingerprints under the Regulations or section 6, however disabled or injured persons I am receiving Aadhar. Subsequent injury issues were not mentioned. Studies have shown that the same iris can register differently based on a variety of variables, including gaze, effects of iris contraction and expansion, motion blur, camera angle, and even fingerprint ridges.[7] It offers only minor modifications and is completely silent on the impact of biometric data on people who have suffered injuries or disabilities in their hands or eyes after Aadhar's creation.

There are many problems with fingerprint registration in Aadhar and many incidents have been reported in the newspapers. In the case of Motka Manji, from Jharkhand state, she was stripped of food subsidies from her grocery store because her fingerprints were not registered in the new system. He had to update his fingerprints online, which required him to drive more than seven kilometers from his village, Dumka, to the civilian center. Due to the poor network within the center, there was no guarantee that the work would even be completed in one day. Although a grievance redressal has been set up under Section 32 of 'Aadhar (Enrolment and Update) Regulations, 2016' and it has been said that grievances should be addressed by service providers in a timely and appropriate manner in the Code of Conduct for Service Providers, it not done so quickly.

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

ISSN: 2582-6433

(B)Right to Privacy

One of the most publicized issues with Aadhar was that of data protection and privacy rights. People were concerned about government surveillance, as Aadhar could have biometrics and mandated links with banking and government systems. Therefore, a case was filed against it by Justice Puttaswami (retired) and in Puttaswami v. Union of India (Puttaswami I), the right to privacy is an inherent right of human beings and falls within Article 21 on the Right to Liberty of Life and Person was declared. Although the above ruling recognized the right to privacy through judicial interpretation, in the case of Judge Puttaswamy (retired) and The Aadhar Law 2016 by the Indian government was found to be constitutionally valid, but the Government that establishes an individual's identity for commercial, business, or contractual reasons that imposes a restriction that it can only be used by the government to prove an individual's identity in order to receive services, but this is not permitted. It also ruled against asking Aadhar to have relationships with other companies. However, even now most banks require him to link his Aadhar card to a bank account via KYC. Indeed, banks these days require Aadhar to open new accounts and process loans for new customers. It is still unclear why banks would want such biometric data, despite other ways to verify an individual's identity. Linking with Aadhar was encouraged as it would help the government transfer subsidies directly and prevent tax evasion. Banks like the Central Bank of India have open outposts for merchants, and people link their bank accounts to their Aadhar numbers by installing fingerprint sensors or scanners in their outposts. You can. Amounts due to the dealer are credited directly to the dealer.[8]

Aadhar allows you to make secure market transactions. However, there have been various reports in newspapers and agencies that Aadhar data has been compromised and that a duplicate of his ID card has been used to link his bank account and identity theft. increase. Hackers can access Aadhar database, use the card to link bank cards with other cards, and print duplicate cards to access information and carry out identity theft.

Currently, the only laws are the Information Technology Act 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Regulations 2011 Privacy Regulations), which govern any data breach. and provide only a limited range of remedies, such as biometrics. Acquire data and limit it only to

[8] 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,*

ISSN: 2582-6433

information obtained or output electronically. Although data protection regulations provide for data collection, consent, description of purposes for data collection, retention of biometric data, and distribution and storage of this data, the privacy policies governing these biometrics nevertheless apply. giving companies more freedom to decide data. There are obvious loopholes that can be exploited to access biometric data for nefarious purposes. The law is not designed to protect privacy and does not address procedures, policies, policies, rules, regulations or standards that organisations must follow when using and collecting biometric information from individuals.

(c) Data Privacy and Ethical Issues

In the paragraphs above, we have seen that Indian law currently has serious deficiencies in protecting privacy and data security, ensuring privacy rights, and the efficiency and integrity of the law. Legal issues related to biometrics in India mainly concern rights to privacy, rights to surveillance, ethical rights and rights to life, and rights to data protection and data security. There are other important issues as well. Many people wonder if biometrics can be used to create personal profiles without their consent or knowledge, and attempt to collect other sensitive information such as their habits, sexuality, tribal affiliation, or hometown. I am afraid that Prioritisation of government databases or other agencies. Such a database would allow individuals to be fully traced and would be monitored by various authorities. There are currently no laws in India restricting the collection of such data linkages, monitoring the activities of parties and preventing profiling. Sensitive personal data is tracked on so many platforms and currently there are no laws restricting the conduct of such data processing organisations or parties.

It turns out that biometric data is considered sensitive data under the principles of data protection law. India's current legal system reflects the protection of biometric data as sensitive data under data protection regulations, and the Aadhar Act establishes certain use cases for biometric data. As a result, groups of individuals, companies, and government agencies are interested in such sensitive information about the human body. Furthermore, the expected purpose and abuse of biometrics is incomprehensible.

The new Digital Personal Data Protection Act of 2022 has adopted many aspects of the European Union's GDPR, but there are still gaps in the framework, and the bill has been before parliament for a long time without being translated into law. It was done.

ISSN: 2582-6433

CONCLUSION

In today's world, where digitisation is everywhere and people want easy and fast access to things, the use of biometric data is inevitable. The use of biometrics is embedded in everyday devices, devices and objects that people use and will soon become the norm of the 21st century. In the near future, using biometrics to perform everyday tasks will quickly become the norm. Using biometrics is convenient for people because it is unique and secure because no one but you can use it and you don't have to worry about remembering the data.

But as biometrics become more popular, so does the fear of biometrics because they are tied to the body. Most people have the idea that the body is the most intimate and sacred thing. Concerns about the misuse of biometrics have always existed, including violations of other people's privacy, governments or other organisations collecting biometrics without their consent, governments or other entities using private companies or other companies to There have also been numerous instances of informing people that they are collecting biometrics of individuals that have been distributed. organisation. Many feared profiling and cataloging by governments and other authorities. As a result, many regulators have decided to harmonise their protocols and laws regarding biometric data and how they are used with other organisations.

In summary, the use of biometrics in India entails a number of legal issues, and in order to resolve the core issues and enact the most inclusive and secure legislation possible, modernisation and major changes to the law will be required. It can be said that expeditious enforcement of the pending legislation with rights protect the people.

BIBLIOGRAPHY:

PRIMARY SOURCES:

1) - INDIAN STATUTES:

- The Constitution of India, 1950
- The Information Technology Act, 2000
- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
- Criminal Procedure Code, 1973
- Identification of Prisoner‟s Act, 1920

ISSN: 2582-6433

- The Criminal Procedure (Identification) Act, 2022
- Indian Panel Code, 1860
- The Digital Personal Data Protection Bill, 2022

2) - INTERNATIONAL INSTRUMESTS AND STATUTES OF OTHER COUNTRIES:

- Universal Declaration of Human Rights (UDHR),1950
- Data Protection Act, 2018(UK GDPR)
- European Convention on Human rightsights,1950
- Fair information practice principles (FIPPs)
- Universal Declaration of Human Rights (UDHR),1950
- Biometric data Privacy Act(BIPA,2008)
- General Data Protection regulation 2016/679(EU-GDPR)

SECONDRY SOURCES:

BOOKS:

1. Marcus Smith And Seumas Miller, Biometric Identification, Law And Ethics, (Springerbriefs In Ethics) , 2021
2. Marcus Smith, Monique Mann and Gregor Urbas, Biometric s, Crime and Security, Routledge, 2018
3. Emilio Mordini (Editor), Dimitros Tzovaras (Editor), Second Generation Biometric s: The Ethical, Legal and Social Context, Springer, (2014)
4. Dr. Talat Fatima, Cyber Crimes, Eastern Book Company, 2021
5. Els J.KIndth, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis (Law, Governance and Technology Series, 12), Springer,2013
6. Patrizio Campisi, Security and Privacy in Biometric s, Springer 2013
7. Lisa Bock, Identity Management with Biometric s, Packt Publishing, 2020 11. B.R. Sharma, Forensic Science In Criminal Investigation And Trials Lexis Nexis; 6Th Edition 2020
8. Sara Smyth, Biometric s, Surveillance and the Law (Societies of Restricted Access, Discipline and Control), Routledge, 2021

ISSN: 2582-6433

ARTICLES:

1. Pawan Singh (2019): Aadhaar and data privacy: Biometric identification and anxieties of recognition in India, Information, Communication & Society, DOI:10.1080/1369118X.2019.1668459
2. Dixon, P. A Failure to "Do No Harm" -- India's Aadhaar Biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.. Health Technol. 7, 539–567 (2017). https://doi.org/10.1007/s12553-017-0202-6
3. Masiero, Silvia (2018): Explaining trust in large Biometric infrastructures: A critical realist case study of India's Aadhaar project. Loughborough University. Journal contribution. https://hdl.handle.net/2134/35413
4. Rao, U. (2018). Biometric Bodies, Or How to Make Electronic Fingerprinting Work in India. Body & Society, 24(3), 68–94. https://doi.org/10.1177/1357034X18780983
5. Christine Rosen, "*Liberty, Privacy and Databases*" The New Atlantis, No. 1 (Spring 2003), pp37-52
6. Vijaita Singh, Rules for identifying criminals, What do the recently notified rules of the Criminal Procedure (Identification) Act, 2022 state? Is there scope for misuse?(https:// www.thehindu.com/news/national/explained-rules-for-identifying-criminals/ article65919414.ece)
7. Anil Sasi, Soumyarendra Barik, What India's draft digital privacy law says — and how it compares with data protection laws elsewhere(https://indianexpress.com/article/ explained/explained-economics/india-draft-digital-privacy-law-data-protection- laws-8279199/)
8. Trishee Goyal, A first look at the new data protection Bill
9. Aadhaar-PAN Link Will Prevent Tax Evasion, Says FM Arun Jaitley, BUSINESS TODAY, (July 25, 2017, 4:00 PM IST),
10. A.K. JAIN, et al P. FLYNN & A.A. ROSS eds, HANDBOOK OF BIOMETRICS 1-22
11. (2nd ed Springer 2007)
12. 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
13. AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,52-62 (Al Now Institute, 2020),
14. Banks Can Use Aadhaar for KYC with Customer's Consent: RBI," (May 29,

ISSN: 2582-6433

2019,11:51PM IST) Biometric Attendance System Manual 2018

REPORTS:

Justice B. N. Srikrishna committ