International Journal of Technology and Applied Science (IJTAS)
E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

The Right To Erase: Protecting Biometric Data Through The Right To Be Forgotten

Shilpa Khandelwal

Assistant Professor
Modi Law College
Kota, Rajasthan.

Abstract:
This article explores the intricacies of biometric data and right to be forgotten with respect to biometric data. Considering the peculiar and sensitive nature of the biometric data, it requires special data protection framework as any unauthorised access of such data to miscreant would be devastating for the data subject, it is further discussed in this article.
Currently most of the data protection laws around the world regulate the personal data but have not emphasised regulation of biometric data explicitly despite its crucial and vulnerable attributes. India's latest data protection act DPDP has no mention of biometric data in the entire act.
This article dwells upon the current position of legislations of different jurisdictions with special focus on provisions ensuring right to be forgotten for this sophisticated form of data and challenges in ensuring such rights due to its special features.

INTRODUCTION

In a digital and information age, where to perform a simple task requires data, the need of data protection is non-negotiable. According to Clive Humby, a British mathematician and data science entrepreneur 'data is the new oil' which substantiate the undeniable importance of data in contemporary times.[1] World is going after the data whether it's the government or the corporation, everybody needs data to have leverage upon the data subject. This trend of data mining has transcended the usability of personal data to biometric data. Companies are installing biometric authentication devices to mark the attendance of the employees. Banks are also enabling biometric authentication to strengthen its security even more. Government is using biometric authentication to identify the person while rolling out government schemes like ration distribution, subsidy realisation and other welfare benefits.

Amid the growing demand of data in various sectors all around the world sought the lawmakers' attention towards the framing of data protection legislation but one crucial form of data neglected is biometric data. Considering the crucial nature of this form of data, it requires much more attention in terms of its protection and its deletion by the data depositories. This article delves into the nuances of biometric data, need to protect biometric data, status of legislation of different countries with regards to biometric data and right to erasure of biometric data and finally analysing the challenges in implementing such right.

UNDERSTANDING BIOMETRIC DATA

Biometric data is personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images, fingerprints etc.[2] The human body is a unique

[1] Nisha Talagala, *Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires*, FORBES, https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for- avoiding-data-fires/ (last visited Mar 27, 2025).
[2] General Data Protection Regulation, https://gdpr-info.eu/art-17-gdpr/ (last visited Mar 29, 2025).

art of the almighty, everybody has unique identification whether in terms of face, eyes, and voice etc. Biometric data encompasses data such as facial images, retinal scans, iris scans, fingerprints, hand geometry, voices, DNA, vein patterns, behavioural attributes like a person's gait, signature, or keystroke pattern etc.[3] The use of biometric data is increasing day by day in each sector. One of the major reasons is its reliability in authentication. Phones are coming with inbuilt fingerprints scanners or face-ids for authentication, selves are coming with biometric lock system, the government are issuing ids based on the biometric authentication for example Aadhar.

People are shifting from conventional forms of technology towards AI powered technologies, and to leverage the profit through this shift stakeholders have already started investing in such fields. AI companies are training their AI models by feeding facial geometrics data to let AI learn human demeanour, or to identify humans in crowds. Voices of humans are being used to train machines to speak more human-like. Robotics company making robots to learn the behavioural patterns of humans through machine learning. So, the use of biometric data is extensive in the modern digital age and the use case is going to surge only.

WHY TO PROTECT BIOMETRIC DATA?

With the benefits of biometric data there are various limitations with it being used extensively. These data are immutable, which means the face geometrics, fingerprints, iris image, or voice cannot be changed unlike the conventional source of authentication that is passwords or pins. This implies that once someone gets access to these sensitive personal data, it can be used against the data subject, and they will not have any recourse to it. Since biometric data is so crucial that is why it is important to protect such sensitive personal data so that it cannot lead to the following consequences.

DATA THEFT:

Data theft is the major concern associated with the breach of the biometric data. Biometric data breach is a gateway to enter and steal other data of the data subject from the data repository. Biometric Data is extensively used as a means of authentication to protect other data. Once the hackers get their hands on such biometric data, they can bypass the authentication to steal the data of the data subject which was protected with such biometric keys. In response the data subject will be incapable to do anything as unlike the password or pin these biometric keys couldn't be changed to prohibit such data theft from the data base.

IDENTITY THEFT:

The biometric data is very crucial information which can be used to replicate a person, it contains the facial imagery, voice, fingerprints, behavioural patterns, DNA samples. So, the person who has access to such information can impersonate as the data subject and commit various kinds of crimes like duping the acquaintances of the data subject by borrowing money from them, withdrawing money from the bank account or proceeds to take digital loan on the name of the data subject etc.

MORPHING AND DEEPFAKES:

The facial images of the data subject are assets to make morphed video or deepfakes. Considering the evolution of advance AIs these can be used to malign the reputation or character of the data subject. The data subject could be replicated in the audio or video form through the help of AI and can be used to propagate moral turpitude, like making an obscene video depicting the data subject involved in lascivious activity. Further perpetrator could also demand ransom in lieu of deletion of such obscene video uploaded on the Internet. These data can also be used to digitally arrest a person by impersonating as an influential

[3] Biometrics and Privacy – Issues and Challenges, OFFICE OF THE VICTORIAN INFORMATION COMMISSIONER, https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/ (last visited Mar 27, 2025).

person in law enforcement by replicating their face and voice.

THE RIGHT TO BE FORGOTTEN:

The right to be forgotten or right to erasure or right to deletion are used interchangeably having the same meaning. French jurisprudence on the "right to oblivion" is the gerund source of the right to be forgotten. Right to oblivion was introduced with the intention to integrate the offender back to society. After the completion of sentences of the offender the publication of information about their crime was deleted, which provides social acceptance to them.[4] The right to be forgotten enables a mechanism to the individuals through which it can ask their personal data to be deleted from their data bases. In the modern digital world, the judgement of the famous case law Google Spain SL, Google Inc. Vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González[5] of 2014, led to the advent of this right in 2014, in this case, it was ruled that the European Citizens can ask organisations to remove the personal data once the purpose for which data was provided is accomplished. It was later incorporated in the GDPR. In India, the judgement of Sri Vasunathan Vs Registrar-General[6] of 2017 recognized the right to be forgotten. Justice Byapareddy of Karnataka High court had observed that *"This is in line with the trend in western countries of the "Right to be forgotten" in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned."*[7] This was the first instance where the Indian judiciary cited the right to be forgotten, comparing it with trends in western countries. DPDPA, India's digital data privacy Act also incorporated the recommendations of the judgement of this case. Initially this right was restricted with regards to deletion of personal information from the internet only but later it extended to deletion of such data from all depositories.

Various legislations are complying with this right, Article 17 of GDPR has extensively dealt with it. The right to be forgotten or right to erasure enables individuals to ask for removal of their personal data available to the data controller. According to the article 17 of GDPR, the Controller is required to delete the data of the data subject as soon as the purpose for which the data was collected is served or the data subject has withdrawn its consent for the processing. However, the Controller can retain such data if it is required to do for compliance with any law of the Union or Member State or to fulfil any legal obligations.[8]

According to section 1798.105(a) of CCPA (California Consumer Privacy Act) consumers have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. Another newly enacted legislation is into effect called California Delete Act which has been framed specially to delete the data from the data brokers at one request. This Act further strengthens the power of residents of California over their data. This Act has made the deletion of their data smooth, as they don't need to approach all organisations individually rather at one request deletion can be performed from all organisations. California also has Online Eraser law effective from 2015 which empowers minors (13 to 17 years) to request removal of the information provided or contents posted online. In India, currently no legislation authorises this right to its people specifically, current data governing laws under SPDI rules 2011 just mention that body corporate or any person in behalf shall not retain the sensitive personal information for longer than is required for the purposes or required under any law in force, but this does not grant such right of data deletion to data subject. However, Information Technology (Intermediary Guidelines and Digital Media ethics code) Rule 2021 has mechanism through

[4] Prashant Mali, *PRIVACY LAW: RIGHT TO BE FORGOTTEN IN INDIA*, 7 NLIU LAW REVIEW 2 (2018).
[5] MANU/UKCJ/0001/2014
[6] MANU/KA/0214/2017
[7] Zubair Ahmad, *Right to Be Forgotten*, MANUPATRA ARTICLES (2022), https://articles.manupatra.com/article-details?id=undefined&ifile=undefined (last visited Mar 28, 2025).
[8] Swati Pandita and Lovely Sharma, *Right to be Forgotten: A Study with Special Reference to India,* SSRN (July 20, 2023), https://ssrn.com/abstract=4850700 (last visited April 5, 2025)

which an aggrieved person whose personal information has disseminated online can contact the grievance officer for removal of such data. But newly passed legislation DPDPA (Digital Personal Data Protection Act) 2023 which will supersede current SPDI rules 2011 contains the provisions related to right to erasure. According to section 12 of this Act, a Data fiduciary shall, unless retention of such data for compliance with any law is necessary, erase personal data, upon withdrawal of consent of the data subject or the specified purpose has been fulfilled.

RIGHT TO BE FORGOTTEN FOR BIOMETRIC DATA STATUS IN DIFFERENT COUNTRIES:

As per the DPDPA of India, the biometric data has neither been defined nor mentioned in the whole act. However, according to the definition of the personal data, it pertains to the category of personal data which is subject to the protection and right to eraser under the DPDPA, so indirectly right to eraser for biometric data has been extended through this Act. But more clarity on the subject matter is required and government is expected to issue special regulation or guidelines governing the processing of biometric data.

In USA there is no federal law which deals with the Biometric data specifically, however some states have such legislation like California, Illinois and Texas, Washington. The Visionary Legislature of Illinois passed the Biometric Information Privacy Act (BIPA) in 2008 for the regulation of use of biometric systems in businesses and other kinds of industry engaged in providing security services. The Texas Capture or Use of Biometric Identifiers Act (CUBI) was passed in 2009 to regulate the collection, storage, and use of biometric identifiers in the state of Texas. Washington state's H.B. 1493 also has provisions to regulate the use of biometric data. It provides a mechanism to serve notice and prevention from commercial realisation of such biometric data by the entities. It is a legislation drafted to regulate biometric data however it does not cover data relating to facial structure and voice.[9] Although these three states have legislation concerning biometric data, none of these provide private rights to individuals like the right to erase such data. Consumer privacy rights are regulated by CCPA-CPRA in the state of California. According to Section 1798.140(v)(1) of California Code; Biometric information is one of the 11 categories which falls under the definition of "Personal information" . It implies that businesses will handle biometric data as if it is personal data. So, the right to delete also applies for biometric data. The California Delete Act also draws the definition of "Personal Information" from CCPA, so the newly enacted legislation will also apply for biometric data.

As per the GDPR of European Union countries, according to article 4 (14) the definition of the biometric data itself categorises it as personal data. Thus, the right to eraser shall apply to the biometric data as per the provision of GDPR. The status of various jurisdictions demonstrates that provisions of the right to be forgotten for biometric data are available to multiple countries and some are making efforts to adopt such, but the State of California is leading in such advancement.

CHALLENGES OF IMPLEMENTING THE RIGHT TO BE FORGOTTEN FOR BIOMETRIC DATA:

The biggest feature of biometric data becomes the biggest limitation for itself in case of data leak. The very nature of biometric data is unique, immutable, unidentifiable, etc makes it challenging to implement the right to erase biometric data.

ANONYMITY:

It is hard to determine the data subject merely looking at the biometric identifiers like fingerprints, voice prints, face images, vein pattern, DNA samples, keystrokes, retinal scan etc. except the facial images. If a

[9] Joshua Roller, *4 Legal Insights into Biometric Privacy Laws and Regulations*, IEEE COMPUTER SOCIETY (2024), https://www.computer.org/publications/tech-news/trends/biometric-privacy-laws-and-regulations-insights/ (last visited Apr 5, 2025).

data controller has access to process biometric data other than facial image, it is almost impossible to verify if such data is of concerned data subject or others.

TRACEABILITY:
The nature of biometric data is that it couldn't be represented in character. Which makes it hard for the organisation to trace it and erase it from the database. Even Law enforcement agencies can't verify such data availability in the database of the organisation. Organisation might also hide the biometric data, and the agency couldn't find out due to limitation of traceability and process the data further. So, it is a pain for execution on the part of Organisation and Law enforcement agencies both.

LEGAL CLARITY:
The major challenge among the normal citizens is lack of legal clarity about their rights. The people are not aware of the right to be forgotten, if so, they are not aware of the right to be forgotten for biometric data. The language of the legislation is mainly focused on personal information, and one needs to delve deep into the intricacies to understand their right to erase biometric data. The bare language is not simple and the right to erase biometric data has not been mentioned explicitly.

DATA HUNGER:
In the modern and digital era, where AI is in vogue, and it is predicted to perform most of the work of humans. Companies, especially in the technology sector, do not want to be left behind in this AI race, every company wants to incorporate the AI in its product or services. That is why the need and greed of data is inevitable, these corporations would try every possible way to acquire such crucial data and biometric data is no exception, considering its utility to train AI models. So, preventing these companies would be a major challenge to implement the right to erase biometric data.

INFRASTRUCTURE:
Ensuring the right to be forgotten of data in the digital landscape is a challenging job itself and to ensure the right to be forgotten for biometric data requires sophisticated infrastructure. Small organisations are not equipped with advanced technology due to capital constraint and even the Government enforcement agencies are not equipped with amenities to investigate such compliance violations and enforce such rights.

MAJOR BIOMETRIC DATA BREACH

Meta vs State of Texas[10]
In this case the state of Texas sued meta for violation of state law i.e., Capture or Use of Biometric Identifier Act. State alleged that Meta had rolled out a feature in 2010 to tag photos shared on Facebook with the names of people. In the background it was unlawfully capturing the facial data of the residents of Texas without consent. Company kept processing the data for almost a decade. In 2021, after being exposed, the company shut down this feature and claimed to delete the data collected during this period. Finally, it was settled for a compensation of $ 1.4 billion between the Meta and Texas government.

MERCADONA CASE[11]
In this case Mercadona was sued for violating EU GDPR law. Supermarket chain Mercadona has been alleged to be illegally using the facial recognition system at the entry gate of their 48 stores in Spain. It was originally intended to identify and restrict entry of individuals having criminal records or restraining orders against them. But it was found that the notorious system was collecting the facial images of all the customers, employees, and even children without permission. Supermarket giant was charged for violation

[10] Texas v. Meta Platform, inc. No. 22-0121 (71st Dist. Ct., Harrison County, Tex.)
[11] Mercadona, PS/00120/2021 (AEPD, Spain)

of Article-9 of the GDPR and was fined €2,520,000 by the Spanish Data Protection Authority (AEPD).

CONCLUSION:

Data in general is a very important tool in the modern day which gives leverage to the data controller. In contrast to biometric data, it becomes more crucial due to its nature and utility. Companies are trying to process biometric data for their profit maximisation irrespective of consumer consent, Meta is the prime example. Various countries have taken steps in the direction of protecting the biometric data, even extending the right to be forgotten to the data subject. India's DPDP Act indirectly entails deletion of biometric data however government should issue separate guidelines with regards clarity on the governing the processing and eraser of biometric data. On the other hand, California is leading the race enabling the right to erasure by enacting latest legislation i.e., California Delete Act which is getting implemented in phases starting 1 January 2026. This act empowers the resident of California to delete their data including biometric data from all such data fiduciaries with one single request. Legislature around the world should take notice of such legislation and incorporate such mechanisms in their jurisdiction. Although there are various challenges present while ensuring the right to be forgotten for biometric data, but it can be addressed by incorporating the advanced technology, better infrastructure, educating the data subjects about their rights and holding the companies accountable for non-compliance of such laws.