IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Your Dna, Your Data: Legal Protection And The Right To Be Forgotten In The Era Of Genetic Healthcare

Seethalakshmi.S, Samyuktha. V
III[rd] year B.com LLB (hons), III[rd] year B.com LLB (hons)
School of Law
Sastra Deemed University, Thanjavur, Tamil Nadu, India

Abstract: Genetic data holds immense and transformative significance in today's healthcare services. it enables the doctor to give personalized treatment to their patients. it allows easy diagnosis of diseases, customization of medicines, and advancing preventive care. genomics and next-generation sequencing help doctors to find the exact genetic cause of a disease much faster, such as personalized cancer treatment. Tailored medicine helps doctors choose the right medicine at the right dosage for the patient, while electronic health records (EHRs) make diagnosis and treatment faster and more accurate by storing all the personal data in one place. While innovation has paved the way for personalized health care, on the other hand, it calls for robust privacy safeguards, transparent governance, and informed consent to prevent misuse and breaches of the highly sensitive genetic information. the General Data Protection Regulation (GDPR) of the European Union treats genetic data as "special category data" that needs extra protection and requires informed consent of the patient before collecting genetic data. In contrast, India's Digital Personal Data Protection Act, 2023 (DPDPA), a progressive step towards genetic healthcare, doesn't clearly define or classify genetic data as sensitive and provides only a limited Right to Be Forgotten (RTBF). This paper adopts a doctrinal and comparative approach, analyzing statutory provisions, judicial decisions, and ethical frameworks. The study finds that while India's DPDPA provides a general framework, it fails to effectively address the sensitivity and perpetual nature of genetic data, making the Right to be Forgotten concept theoretical in the medical context. Protection of genetic privacy is indispensable to uphold human dignity, informed consent, and trust in the healthcare system.

I. INTRODUCTION

As healthcare becomes increasingly data-driven, genetic data holds high significance in today's healthcare services. Back then, they were confined to labs, but now they form a part of the global digital database. Genetic data enables doctor to give personalized treatment to their patients and allows easy diagnosis of diseases, customization of medicines, and advancing preventive care. Based on individual genetic profiles, it tailors medical intervention, promoting more effective and safer therapies.

Genomics studies a person's genes and creates a profile of the patient to have a better understanding of the diseases. The innovative tools, like next-generation sequencing, help medical examiners to find the exact genetic reason behind a disease much faster. Personalized medicine looks into a patient's genes, lifestyle, and the environment they live in to tailor the best treatment suitable for their disease.

Pharmacogenomics is a branch of personalized medicine that uses genetic data to decide which drugs are best and safest. For faster and accurate treatment, all the personal medical data of their patient are stored in one place, which is called Electronic Health Records (EHRs). While innovation has created a way for customized health care, it demands strict privacy protection, open governance, and informed consent to avoid misuse and compromise of the very sensitive genetic data.

As the genetic data are permanent and unique, they give rise to several legal complexities. It identifies the person forever, and it becomes unchanged. Once the data is disclosed or leaked, it cannot be truly "forgotten" as the digital footprints remain. This makes it difficult to implement the right to be forgotten, as genes are personal and unchangeable; deleting them in one system will not ensure that they will be removed in all the records and backups. There arise grave privacy and ethical issues, as misuse of genetic data can affect individuals as well as their families.

Genetic data encloses information from DNA tests, genomic sequencing, biomarkers, and similar sources from which the person's personal data is collected, revealing a unique biological code of everyone. It is intolerably sensitive because it is immutable, identifiable, and reveals not only the individual's medical history but also their family's ancestry details.

Genetic data are especially permanent and help identify current health risks as well as predict future health risks for patients. Once the information is disclosed, it is practically impossible to erase or forget, or retract. This lasting and predictive nature of Genomics calls for privacy protections, and the enforcement of the Right to be forgotten in the medical context to a larger extent, becomes challenging. For example, a single genome can expose inherited disease risks for the individual and family members, heightening the consequences of misuse or unauthorized disclosure. the core legal issue with genetic data is finding a balance between emerging healthcare services with protecting the privacy and autonomy of the patient's data.

Current laws on data protection have not adequately addressed the unique sensitivity and permanence of genetic data, making the Right to Be Forgotten largely theoretical in medical contexts. while the EU's GDPR treats genetic data as a "special category", giving extra protections to genetic information[1]. on the other hand, India's 2023 Digital Personal Data Protection Act (DPDPA)[2] does not clearly define or specially regulate genetic data, leaving the rules unclear. this lack of adequate laws makes the implementation of Right to Be Forgotten (RTBF), especially for immutable genetic or medical data, where complete erasure is practically impossible, posing unresolved legal and ethical challenges for protecting genetic privacy.

The main purposes of this research are: to explore the legal nature and distinctive sensitivity of genetic data; to study the application and breakdown of the Right to Be Forgotten (RTBF) in healthcare and genetic repositories; to compare India's Digital Personal Data Protection Act, 2023 (DPDPA) to comparable frameworks (e.g. EU GDPR, HIPAA, and GINA); to propose legal and policy reforms that would enhance rights of patients, protections of privacy, and the ethical governance of genetic data. This research adopts a doctrinal and comparative methodology, analyzing statutory frameworks, judicial precedents, and ethical guidelines across jurisdictions to evaluate how genetic data privacy and the Right to Be Forgotten are legally addressed."

This paper is confined to focus only on privacy issues related to genetic and health data regarding the right to be forgotten (RTBF). it does not cover the general concept related to data protection. the study is limited to legal, ethical, and regulatory aspects of genetic data privacy and does not discuss medical or technical details of genomics or healthcare technologies. By keeping this aspect in focus, the paper closely examines the challenges and gaps in protecting genetic data and the application of RTBF under the current legal framework.

CONCEPTUAL FRAMEWORK: LEGAL AND ETHICAL DIMENSIONS OF GENETIC DATA AND THE RIGHT TO BE FORGOTTEN

Genetic data refers to information derived from an individual's DNA, RNA, genetic markers, and biomarkers obtained through techniques such as sequencing, genotyping, or molecular testing. This includes raw sequence files, analyzed genetic profiles, and results from targeted or whole-genome analyses.[3]

Genetic data is collected and stored by different organizations, such as genetic testing companies, hospitals, and clinical laboratories for diagnosis and personalized treatment, research institutions for in-depth analysis on genetics and its associated diseases, digital health databases, and biobanks, as they store the data for long-term use.

the important nature of genetic data is that it is permanent and unchangeable. a person's genes stay with them throughout their life. so, if such sensitive data is shared or leaked, it is not easy to erase or replace, especially if "forgotten". next is they are highly identifiable, even if the names are hidden or removed. With the study of genetic data, we can easily trace back to the owner of the genetic data and their family. another critical nature is that they are predictive. Genetic data can reveal not only their current health status but also possible future

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.*

[2] *Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Aug. 11, 2023 (India).*

[3] *Centers for Disease Control & Prevention, What Is Genomic Sequencing?, Advanced Molecular Detection Program (Mar. 4, 2024), https://www.cdc.gov/advanced-molecular-detection/about/what-is-genomic-sequencing.html.*

diseases a patient can be subjected to. This helps in preventing diseases, as well as being highly risky when it comes to the misuse of the data. genetic data are familial because genes are something that are shared within families of a person, so one person's data can reveal information not just about them but also about their families.

Since genetic data is permanent, identifiable, and predictive, it is seen as extremely sensitive. Many laws treat them as a special category of data that requires strong protection; for instance, the EU's GDPR treats genetic data as a "special category". the main reason behind strong protection is that if they are misused, it can result in discrimination, stigma, or invasion of privacy, not just for the patient but their entire family. The main example that can be derived from society is society's stigma against HIV patients; this is the main reason that the names of the patients are not revealed to the public.

data privacy in healthcare is surrounded by a patient's autonomy and their right to confine and control their personal information from sharing or leaking, ensuring confidentiality and protection from misuse. Patients must be entitled to give or refuse to give their consent as it is part of their right on how the data is collected, stored, shared, and used by the medical professional or by the digital databases.

genetic data is very distinct from typical medical records, which naturally include diagnoses, treatment, and lab results. Unlike an ordinary health record, which is temporary, genetic information is permanent, identifiable, predictive, and familial, extending privacy concerns beyond the patient to their families.

the ethical foundation in collecting genetic data is the autonomy of the individual; the fundamental principle is that individuals have the ultimate power over the access and use of their personal genetic information. the healthcare system's basic principle is to maximize benefit for its patients and prevent any injury or harm, like misuse of genetic data resulting in discrimination and stigma. a foundational to the doctor-patient relationship is the sustaining trust between them; it is imperative to safeguard such genetic data against unauthorized disclosure. in 2023, from 23andMe, a genetic testing company, millions of users' genetic and ancestral data were exposed, revealing sensitive familial relationships and disease risks[4].

Electronic Health Records (EHRs), cloud storage platforms, and AI-driven diagnostic tools are reconstructing healthcare by consolidating patient information for faster and more accurate care. however, an increase in digital connectivity increases exposure to data breaches, unauthorized access, and large-scale leaks.

Some of the risks encompassing genetic information are unauthorized access, where a fragile cybersecurity system welcomes hackers or malicious actors to obtain sensitive genetic data. next is that they are highly identifiable, even if the names are hidden, with data, it can be easily matched with the public data to identify the individuals. Another critical issue is the discrimination and societal stigma against disclosed genetic data of the patients. it can result in denial of insurance, employment, or service based on hereditary risks. in 2019, the Singapore HIV Registry leak case, where sensitive health records, including HIV status of patients, were publicly disclosed, causing stigma and discrimination[5].

The Right to Forget originated within European Union jurisprudence, primarily the Google Spain v. AEPD case (CJEU, 2014), finding the rights of individuals to seek erasure of past or irrelevant personal data from online search engines. This principle was codified in Article 17 of the General Data Protection Regulation (GDPR), which makes people entitled to access the right to request their personal data to be deleted or removed, which has become stale or is no longer needed, or is unauthorized, illegally held data. The reasoning behind this is to ensure personal autonomy, dignity, and privacy in the modern era of technology.

Enforcement of the right to be forgotten faces significant obstacles. The right to be forgotten often conflicts with freedom of expression; deleting data must be balanced carefully with the right to information and freedom of speech. Another issue is that when medical or scientific records are of public good, erasing data becomes problematic for research or public health surveillance. when it is medical legal requirements that may mandate record keeping for patient safety and continuity of care, it might be difficult to erase the data. Genetic information is permanent and, once shared or disseminated, can rarely be fully deleted. Digital footprints persist, especially when data is duplicated across multiple repositories.

genetic data's immutability directly challenges the fundamentals of the RTBF. While laws direct erasure, genes stay with human throughout their lives, and digital permanence often renders the enforcement of the right nearly impossible. Deleting genetic information could compromise diagnosis, treatment, or future care for both the individual and their relatives. Medical and scientific research, especially genomics, often relies on keeping long-term genetic data records. If such data were deleted, it could affect the accuracy and reliability

---

[4] *Helena Kudiabor, "'Anonymous' genetic databases vulnerable to privacy leaks," Nature Vol. 634 (Oct. 14 2024), https://doi.org/10.1038/d41586-024-03236-1. (nature.com)*

[5] *Here is a Bluebook (21st ed.) citation for the webpage:*
Müge Fazlıoğlu, Data Privacy and Genetic Testing: Guidance and Enforcement from Regulators, International Association of Privacy Professionals (Sept. 18, 2024), https://iapp.org/news/a/the-dna-of-privacy-and-the-privacy-of-dna.

of research findings. Genetic records are shared across multiple institutions, databases, and backups, making complete eradication unfeasible.

every country applies RTBF to genetic data differently. In the EU, there are stricter rules and genetic data and categorizing them as a special category to provide protection. whereas in India, DPDPA 2023, RTBF is recognized only in limited terms, and genetic data are not classified under any special category. In the USA, HIPAA[6], GINA[7] are based on protecting health and genetic data; there is no explicit comprehensive provision on RTBF. Balancing an individual's right to privacy and erasure against the broader benefits of genetic data for family, public health, and research embodies a profound ethical conflict in digital healthcare.

II. Safeguarding Dignity, Autonomy, And Accountability In Genetic Healthcare

1. Ethical Foundations in Genetic Data Protection

- Autonomy:

Individuals providing informed consent for obtaining their genetic data must have reasonable control over collection, storage, sharing, and potential deletion of their genetic data, in accordance with globally recognized patent rights.

- Beneficence and non-maleficence

The fundamental principle of healthcare is to provide maximum benefit with minimal risks to its patients. Hence, misuse of genetic information can lead to serious harm. In the UK National DNA Database case, they retained the samples not in the way they originally consented to, which resulted in public outrage and policy changes[8].

- Justice and Equity

When everything is based on justice and equity, it also applies to genetic research. Equity demands that genetic research benefit all populations fairly. Genetic research data have historically excluded certain populations, leading to biased judgments in treatments and results of research. The Havasupai Tribe case in the US highlights this: blood samples given for diabetes research were later used for studies on schizophrenia and migration without tribal consent, sparking lawsuits and broader debates on fairness[9].

- Confidentiality and Trust

The informed consent of the patient is surrounded by their trust in their medical examiner and their duty to maintain confidentiality. Breach of such genetic confidentiality can undermine the purpose of informed consent. This may lead to breach of trust, and patients, along with their families, can suffer serious harm, like discrimination and societal stigma. In 2009, the University of California, Berkeley, lab incident, where staff exposed students' genetic details on public websites, undermined faith in the healthcare system and deterred participation in research[10].

2. Privacy V. Public Good Dilemma

- Individual Privacy:

Patients must have strict control and erasure under RTBF. Because they give their consent with the view that the data will not be used against them, or in a way they did not give consent to. In Denmark's National Genome Project, some participants experienced distress when they found their genetic data had been used for unrelated research, leading to requests for withdrawal that conflicted with scientific objectives[11].

---

[6] *Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.)*

[7] *Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified at 42 U.S.C. §§ 2000ff–2000ff-11).*

[8] *S & Marper v. United Kingdom, App. Nos. 30562/04 & 30566/04, 48 Eur. H.R. Rep. 50 (2008) (Grand Chamber) (holding that the indefinite retention of DNA samples and profiles of persons not convicted of an offence violated art. 8 of the European Convention on Human Rights).*

[9] *Havasupai Tribe of the Havasupai Reservation v. Arizona Board of Regents, No. CV-2004-0024-C in Maricopa County Superior Court (Ariz. Apr. 26, 2010) (settled).*

[10] *Anita Kolsi et al., "Title of the Article," JMIR Bioinformatics and Biotechnology, vol. (online first) e54332 (2024), https://bioinform.jmir.org/2024/1/e54332.*

[11] *Róisín Á. Costello, Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?, 22 Hum. Rts. L. Rev. 1 (2022), https://academic.oup.com/hrlr/article/22/1/ngab031/6497576.*

- Public Interest

Retention of large genetic data helps in research, advances research surveillance, public health, and many other areas. But it also comes with ongoing risks that if data is mismanaged or a policy overhaul results in public outrage and miscarriage of justice. The Iceland deCODE Genetics controversy showed how mass data collection without proper consent can cause public outrage and mistrust[12].

3. Informed Consent and Genetic Literacy

- Informed Consent

Informed consent is tied to the dynamic nature of the research or project. The patients must be informed and their consent must be obtained then and there whenever there is evolution or changes. There must be transparency while obtaining consent. Genomics England are adopting continuous, iterative consent models to inform participants as data use evolves[13].

- Genetic Literacy

Knowledge about Genetics and its related concepts is not well-versed among the general public. This low public understanding leads to uninformed consent. In the Henrietta Lacks case, cells taken for research were commercialized without any proper explanation to their parents or without any benefit-sharing[14].

4. Discrimination and Genetic Stigma

- Risk of Genetic Discrimination

When genetic information is shared or leaked, it can lead to discrimination against the patient and their family. Even if the names are hidden, with the details in the genetic data, it can be easily traced back to the owner. In South Africa, a case involved health insurers requiring genetic risk data for policy decisions, resulting in the exclusion of individuals with certain cancer-linked genes

- Societal Stigma

When society learns about the genetic disease a person carries, they see them differently, often discriminating and judging them. That is why the genetic information mustn't be misused or disclosed without authorization. Patients carrying genes for Huntington's disease have faced ostracism, particularly in regions where education or insurance policies use genetic data without safeguards[15].

- Legal Gaps

India currently lacks explicit anti-discrimination statutes for genetic data, highlighted by advocacy groups after cases where hereditary conditions resulted in the denial of jobs or insurance.

5. Accountability, Governance, and Policy Gaps

- Institutional Accountability

When there is a breach of trust and confidentiality or misuse of genetic data, the institution has to take accountability. Because when consents are given by patients, it's because of the trust in the institution. When the trust is breached, institutions have to be held accountable. In Australia's My Health Record breach (2018), dozens of healthcare professionals accessed patient genetic records unnecessarily, leading to government audits and stronger oversight[16].

- Cross-border Data Transfers

With the rise in technology and evolution in the medical field. Cross-border data transfers require serious supervision and control to prevent any sort of misuse. Here, it does not only involve one country, but the data are transferred across the country with potential risk of misusing the genetic information. The Singapore DNA

---

[12] *Institute of Medicine (U.S.). Committee on Assessing Genetic Risks, Social, Legal, and Ethical Implications of Genetic Testing: Assessing Genetic Risks, ch. 8 (Nat'l Acad. Press 1994) (discussing the deCODE Genetics project in Iceland), https://www.ncbi.nlm.nih.gov/books/NBK236044.*

[13] *IOM, Assessing Genetic Risks, ch. 8 (discussing Genomics England).*

[14] *IOM, Assessing Genetic Risks, ch. 8 (discussing Henrietta Lacks case).*

[15] *Nancy Wexler, "The Tiresias Complex: Huntington's Disease as a Paradigm of Testing for Late-Onset Disorders," FASEB Journal 6:2820-2825 (1990).*

[16] *Anita Kolsi et al., Title of the Article, JMIR Bioinformatics and Biotechnology, vol. (online first) e54332 (2024), https://bioinform.jmir.org/2024/1/e54332.*

Sequencing Research Program's partnership with American firms led to ethical questions when participant data was stored and analyzed overseas, without robust Indian or regional governance[17].

- Need for Governance Framework:

The medical field has been evolving every day. The legislature must cope with the emerging trends. It is an urgent call for a robust policy framework for governance on genetic data and its aligned risks. Recent scandals involving private genetic testing companies in China, like BGI's re-use of samples for projects without full consent, highlight global risks and the urgent need for consistent policies[18].

6. Right to Be Forgotten and Medical Ethics

- Conflict of Ethical Interest

A request for deletion of their data can conflict with the clinical needs. Deleting genetic information could compromise diagnosis, treatment, or future care for both the individual and their relatives. Medical and scientific research, especially genomics, often relies on keeping long-term genetic data records. If such data were deleted, it could affect the accuracy and reliability of research findings. In Sweden, where genomic records must be retained for cancer therapy oversight, leading to legal exceptions to RTBF in the interest of ongoing care[19].

- Global Model

Each country enforces RTBF on genetic data differently. For instance, Canadian law mandates restricted access and anonymization rather than deletion, balancing care continuity and privacy, especially in genomics research consortia. Whereas in the US, HIPAA, GINA are not explicit about RTBF on genetic data. The EU considers genetic data as a Special Category requiring stronger protection. Based on the country model, the RTBF on genetic data is applied differently, aligning with the country's objectives and policies.

- Indian Context:

Lack of medical exceptions within DPDPA complicates hospitals' responsibilities. India's DPDPA 2023, the right to be forgotten is recognized only in limited terms, and genetic data are not classified under any special category.

III. Regulatory landscape of Genetic Data Governance: Global and Indian Perspectives

Europe:

Europe was the first country to recognize this right to be forgotten. In 2018, the General Data Protection Regulation was put into effect[20]. This is a well-made strict regulation that puts all the information users under an obligation to prioritize the consent of the owner of the information to use it. All the data and information that are available should not be used if the owner of the data is not willing to give consent for the usage, or if the data is not relevant, or outdated, data shall not be used. Only legitimate use of data is allowed. It applies not only to EU citizens or residents but for that organization which is not in the EU but access their citizens' data. The penalty and fine for the breach of this regulation are very high and severe. The penalty may extend to £20 million or 4% of global revenue (whichever is higher), and the data subjects shall also get compensation for the breach of their information. This right is also known as "right to erasure." Not all data is the same. Some data need additional protection, such as data related to a person's identity, health, or social security. Article 9 of GDPR was enforced to protect sensitive information[21]. This regulation introduced a category called special data, which includes ethnicity, political inclination, religious belief, biometric, genetic data, health-related data, and data related to sexual orientation. This special data requires stringent requirements, and the organization that is using this information should comply with all the requirements given under this

[17] *Tamra Lysaght et al., "Who is watching the watchdog?": Ethical perspectives of sharing health-related data for precision medicine in Singapore, 21 BMC Med. Ethics 118 (2020), https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-020-00561-8.*

[18] *David Lorenzo et al., The Reuse of Genetic Information in Research and Informed Consent, 31 Eur. J. Hum. Genet. 1393 (2023), https://pmc.ncbi.nlm.nih.gov/articles/PMC10689789/.*

[19] *F. Molnár-Gábor, "Harmonization after the GDPR? Divergences in the rules on genomic data—The case of biobanks in Sweden," Computer Law & Security Review, 2022, https://www.sciencedirect.com/science/article/pii/S1044579X21002947*

[20] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons concerning the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1 (effective May 25, 2018).*

[21] *Regulation (EU) 2016/679, art. 9, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons concerning the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.*

article. But this is not an exhaustive limitation. It has exceptions. When it is needed for matters related to employment and social security, when the data is publicly available, or access for any health or medical-related issue, or to defend any legal claims, legitimate use of data for public health. Nonprofit organizations can use these data for legitimate purposes. This article ensures that for legitimate access to this information, explicit consent to use the data should be given.

This regulation directs the user organization should maintain a detailed documentation of the data they've collected and used. Staff who will use this data should be well-trained. Also, when a third party contracts with the organization for data processing, they should have a data processing agreement that contains all the rules regarding the usage of data. Therefore, in case of any breach of data, the person who has committed the breach shall be found and punished easily.

Convention on human rights and biomedicine:

Due to the rapid development of new technologies in DNA, which could make human genetics, the European government made this convention. Articles 11to 14 focus on the genetics, particularly predictive genetics tests and intervention on the human genome[22]. This convention focuses on consent. Any medical intervention carried out without consent is prohibited, also on the human genome, regulating human organ transplantation, and also gives emphasis on private life and the right to information.

India:

In India, this concept was recognized by the Indian judiciary through various judgments. In Justice K. Puttaswamy vs Union of India, the court recognized the right to privacy, which also implicitly includes the right to be forgotten[23]. But this is not an absolute right. It is subject to public policy and public health, and morality. Even before this case Indian judiciary had pronounced various judgments impliedly related to the right to be forgotten, but this was the first judgment that explicitly recognized this right. And now this right to be forgotten comes under the ambit of Article 21 of the Indian Constitution 1950[24]. Right to live with dignity also includes the right to be forgotten. Even though India has recognized the right to be forgotten as a fundamental right under Article 21, India does not have a specific codified law for this right to privacy. The Digital Personal Data Act 2023 and the Information Technology Act 2000 have some provisions related to the right to be forgotten.

The Digital Personal Data Act 2023[25]:

Section 2(t)- Defines Personal data

Personal data means data that identifies a person or that a person may relate to themselves. This personal data includes name, address, biometric data, location history, digital photos, phone number etc.,

Section 4- Data can only be used for a legitimate purpose. This section emphasizes two important ingredients: one is the consent of the "Data principle" and "legitimate use" of obtained data.

Section 9- Parental or Guardian's consent is required in case of any data related to a child who is under the age of 18. It should be for a legitimate purpose. And the processing should not be detrimental to the child's interests. Any such interest shall be prohibited.

Section 12- Gives the right to correction and the right to erasure of their personal data. This means that the data principle has the right to alter the inaccurate data, misleading data, or correct the incorrect data, or add further information to the existing data. Also have the right to erase their personal data permanently. The data fiduciary must, upon receiving the request, take necessary steps to make the alteration or permanent deletion of data.

Section 37- The Central government is empowered to block any public access to information if the data fiduciary has been penalized more than once. The Data Protection Board should recommend the central government for such a block.

Information Technology (Reasonable security practices and procedures and sensitive data or information) rules 2021[26]:

This rule introduced a special category of data called "sensitive personal data or information" which includes data related to physical health, psychological, mental condition, and medical records. Hospitals will have access to these data for further medical treatment. So, the Hospital is the data fiduciary, and the patient or

---

[22] *Regulation (EU) 2016/679, arts. 4(13), 9, of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons concerning the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.*

[23] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).*

[24] *India Const. art. 21, available at https://legislative.gov.in/constitution-of-india.*

[25] *Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India (Extra), Pt. II, §§ 1 et seq. (Aug. 11, 2023) (India).*

[26] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (Apr. 11, 2011) (India), https://cis-india.org/internet-governance/files/it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.pdf.*

person who is disclosing this information is called the Data principal. The data principal has the right to erasure and the right to correction of the data given to them for their health. These data are highly sensitive, and any further process of this information require proper consent from the data principal and should only be used for legitimate and necessary purposes. If a hospital transfers these data to another institution, it must be done carefully and confidentially. For this, also consent of the data principal is required.

US:

Health insurance portability and accountability Act of 1996:

This act was enacted on 21 August 1996 to protect the privacy and security of Health and medical-related information by the U.S. Department of Health and Human Services[27]. This act was enacted exclusively for this purpose. The main aim of this act is to strike a balance between the free flow of health and medical-related information and protecting the privacy and security of the data principle. The data principle has control over its information. They have the right to correct, alter, or erase their health-related information. This act addresses the information that is used for health and medical purposes as "protected health information," and the organizations that use this information must follow the rules of this act, and it is called a" covered entity". The U.S. Department of Health and Human Services emphasizes the Office of Civil Rights to promote and raise awareness of this act and the rights available to its citizens, and impose civil money penalties. This act protects the "individually identifiable health information" which includes past, present, future health and medical related information and records, and past, present, future payment paid for this health service and provision of health care available to the individual. The officer of civil rights will impose a civil money penalty for violations and noncompliance with rules. The penalty amount may vary depending on various factors, like the date of violation, whether the noncompliance is willful or due to negligence. And for knowingly obtaining and disclosing this individually identifiable health information to any third person shall be liable to a criminal penalty of $50000 and one year of imprisonment.

Comparative analysis:

India and Europe:

Europe has enacted s comprehensive, very clear, and exhaustive law called the General Data Protection Regulation for this matter. On the other hand, the Digital Personal Data Protection Act of 2023 was the first specific act that was enacted for digital data protection. The GDPR have categorized data based on the degree of security needed to protect the data to protect the privacy and interests of the data principal. E.g.: data includes political inclination, religious belief, biometric, and genetic data, etc. The term "sensitive data" is not exhaustive, which means any further data that may demand a higher level of security could be included in this purview. But Indian law does not have such of distinction. There is no clarity on special data. India is mainly based on consent and the legitimate use of data. But in Europe, there are multiple legal requirements like consent, contract, legal obligation, and legitimate interest. The main setback of Indian law is that many people do not even know that these kinds of rights are available to them because the government and legislation are very keen on enacting laws, but not in promoting or raising awareness about the existence of such laws and the availability of remedies. European law has explicitly categorized sensitive data and other data. But there is no such distinction in Indian law. Many questions and ambiguities could arise. The Data Protection Board of India has very limited powers and should act according to the rules framed by the central government. The Independent Supervisory Authority of Europe has stronger powers, which have been given to it by the act itself. In India, individual rights include the right to access, erase, modify, redressal, and consent withdrawal. But Europe has more extended individual rights, which include access, rectification, erasure, portability, and objection.

USA and India:

The USA has specific legislation called the Health Insurance Portability and Accountability Act[28]. This act was specifically enacted for protecting the "individually identifiable data," which is the compilation of all health and medical-related information of a person which including expenses made for treatments. India does not have such a specific law. The Digital Personal Data Protection Act covered general digital data, and it does not give any emphasis on "individually identifiable data." In fact, there is no such distinction made under this enactment. Here lies the problem, there will be vagueness while assessing the degree of punishment because the stricter punishment shall be given only if the aggrieved party can prove privacy of the data principle is so grim. Sometimes it may be difficult for the aggrieved party to prove that the data was his "individually identifiable data". The burden of proof will also lie with the affected party. It might weaken the

[27] *Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).*

enforceability of their rights. This absence will be very favorable to the defendant. So, a special sorting in this regard will be very practical and convenient if such classifications are made. In the USA, the main duty of the officer of civil rights is to promote this act and ensure that all organizations that engage in health care comply with the rules of this act. There is a data protection board in India, but it is not involved in promoting activity and has very limited powers.

IV. Prepare Your Paper Before Styling Judicial Perspectives on Genetic Data Privacy and Right To Be Forgotten

S and Marpher vs the United Kingdom- Mr.S was arrested for attempted robbery. His DNA samples and fingerprint were collected. But subsequently, He was acquitted by the court. And Michael Marpher, another person, was arrested for harassment of his partner. His DNA samples and fingerprints were also collected. Later, the court discontinued this case. But the authority did not delete the samples. They filed a complaint against the authority and contended that this is violating their right to privacy given under articles 8 and 14 of the European Convention on Human Rights. The court decided that it was a violation of their right to privacy[29].
Sunitha Motwani vs Union of India- the petitioner Sunitha Motwani was involved in many criminal cases, and many cases were filed against her. But of them were ended in acquittal. Despite her exoneration, she was publicly labelled as an offender. So she filed a case contending that the offender's name should not be revealed until the judgment. This is an ongoing case and yet to be declared[30].
Mr.X vs Registrar General, High Court of Karnataka- the petitioner filed this case to conceal his name from the digital data of the court. He contended that whenever the plaintiff's name in his earlier case was searched, it revealed that he had been accused of a crime despite his acquittal. The Court declared that the right to live under Article 21 includes the right to live with dignity, which also includes the right to be forgotten. "The right to oblivion is a democratic right given to the citizens."[31]
Jorawar Singh Mundy vs Union of India- the petition was earlier charged under the NDPS Act later he was acquitted. But he was content to remove his name from the legal websites like Indian Kanoon. The court upheld the right to be forgotten and made a distinction between the individual right to privacy and the public right to information and mandated a balancing test[32].

V. The Paradox of Permanence: Challenges in Enforcing the Right to be Forgotten for Genetic Data

Legal challenges:
1. The Digital Personal Data Protection Act provides the right to erasure. So, the data principal has control over their information. But some rules of the hospital may mandate the patient to keep them for some years. So, the applicability of this act may be in question.
2. There is no special specification as to the identification of data. So, there will be ambiguity while deciding a case in this regard.
3. Lack of a specific act for health-related data. Digital Information security in healthcare act 2018. This bill was passed by parliament. But this is still in the bill stage. It was not taken into the next stage.
4. This act gives an exception and gives power to retain the data for research purposes, public interest. This may sometimes curtail the right to erasure.
Operational and technical hurdles:
1. Even though the data principal has the right to erase their information, complete erasure of information is impossible. Because the same information will be stored in many clouds, multiple backup platforms, it could be very difficult for the health providers to find and erase the same data stored in multiple platforms.
2. The Digital Personal Data Protection Act 2023 only focuses on digitalized data. But much historical non-digitized data is available in written form. This act does not give any clarification about the erasure of this data.
Ethical challenges:
1. Medical information of HIV, AIDS patients may lead to stigmatizing them. But this information might be disclosed when some other person's interest is involved. In the Mr.X vs Hospital Z case, information about

[29] *S. & Marper v. United Kingdom, App. Nos. 30562/04 & 30566/04, 48 Eur. H.R. Rep. 50 (Dec. 4, 2008) (Grand Chamber), https://hudoc.echr.coe.int/fre?i=001-90051.*
[30] *Smt. Sunita Motwani v. Union of India & Ors. (W.P. No. 15781/2024)*
[31] *Mr. X v. Registrar General, High Court of Karnataka, W.P. No. 5163/2021 (Karn. H.C.), https://www.advocatekhoj.com/library/judgments/announcement.php?WID=14686.*
[32] *Jorawer Singh Mundy v. Union of India & Ors., W.P.(C) 3918/2021 (Del. H.C. Apr. 12, 2021), https://www.mcolegals.in/kb/Cyber_Law_Issue_4_Right_to_be_forgotten_in_India_Jorawer_Singh_Case.pdf.*

an AIDS, positive patient was disclosed, and consequence this his marriage has been called off. The court upheld the disclosure because AIDS is a contagious disease, and whoever has any sexual relationship with the patient will also be affected.

2. Lack of awareness. Many people are not even aware of this act. So, they do not know this right. So, this cannot be enforced when people are not even aware of it.

3. Lack of clarification and Lack of exclusive act may lead to misuse. People will try to surpass the legitimate use rule and will use this information according to their whims and fancies.

VI. LEGAL AND POLICY REFORMS FOR STRENGTHENING GENETIC DATA PRIVACY AND THE RIGHT TO BE FORGOTTEN

1. A comprehensive and separate law to address genetic information and its related problems. This should include every genetically related and also health and medical-related information and records. All the complexity in enforcing should be clarified. An exception to this right should be precise and should not affect the interests of the data principal.

2. Transform from mere consent to stricter consent. The data principal should understand what he is giving consent to. That consent should precisely define how he wants his data to be used, by whom, and when. So, unauthorized use of data could be curtailed.

3. Categorisation of risk. Liability and punishment should be based on the level and degree of risk and breach of privacy involved. High level risk, medium level risk, low level risk. This will emphasize the seriousness of unauthorised disclosure and the consequences should be according to the severity.

4. Increase the penalty and maintain stricter accountability. The offender should compensate the aggrieved party and should pay the penalty imposed in the act for the non-compliance and violation of rules, and should be prosecuted for gross negligence.

5. A separate board should be constituted exclusively to address these matters. This board should constantly monitor the activity of the data fiduciary and must insist that all data fiduciaries comply with the rules.

6. In court, if the aggrieved party is not willing to speak in open court, then an in-camera proceeding should be allowed. Because if the disclosed information is so sensitive and might affect the party's personal life, then they should not be forced to speak in open court.

7. Right to be forgotten and right to erasure are not the same. Though it is viewed in that same sense, there is a thin line of difference in it. The right to be forgotten is the complete erasure of data as if it had never existed. But in the right to erasure, it cannot be done. But the data principal will only erase his data from where he knows that it was stored. But many third-party contractors could use storage platforms, and multiple backup storage platforms will also have this data. All of this might not be deleted. This aspect should also be included. The act should insist more upon the right to be forgotten.

VII. CONCLUSION

Today's genetic data has drastically changed the way we understand and analyze the health and disease of a person. It allows the doctors to predict risks, personalize treatment, and even prevent illness before it occurs. Yet, the same information that makes personalized care come true also gets into conflict with privacy protection. Unlike normal data, your data can not be changed; it follows you throughout your life. That is why laws and ethics must cope with the evolution of science. The GDPR in Europe recognizes that genetic data is highly sensitive and gives people the "Right to Be Forgotten." India's new Digital Personal Data Protection Act, 2023, is a big step forward, but it still leaves important gaps, especially when it comes to letting individuals truly control or erase their data. Protecting genetic privacy is not just about compliance; it's also about respect. It is about giving patients confidence that their most personal information will not be misused. As genetic technologies become a bigger part of everyday healthcare, the challenge is clear: how do we use data to heal without crossing the line of trust? If laws, hospitals, and technology developers work together, the future of genetic healthcare can be both innovative and humane, where progress and privacy stand side by side.

"Our genetic code may shape our identity, but it must never limit our right to privacy, dignity, and the freedom to be forgotten."