LEGAL CHALLENGES OF DNA PRIVACY AND GENETIC PROTECTION

Shreya Mahapatra, Maharashtra National Law University (MNLU), Chhatrapati Sambhajinagar (Aurangabad)

ABSTRACT

The unique characteristics of genetic data, the shortcomings of the privacy frameworks in place, and the pressing need for new laws to stop abuse and prejudice are all examined in the legal difficulties of DNA privacy and genetic protection. It draws attention to the conflict between advancing advantageous genetic research and protecting the privacy of individuals and families. Genetic data is unique in that it provides extremely intimate information about a person's health, ancestry, and potential future predispositions. It is impossible to completely anonymize a person's DNA, and the information is useful for many generations. Additionally, the genetic data of a single person can disclose information about their whole biological family, posing "relational" privacy problems that go against conventional consent models. Limitations of informed consent, it can be difficult to obtain fully informed permission for genetic testing and data sharing. Since new findings may uncover health information that was not immediately obvious, the average individual might not completely understand the implications of their agreement, particularly with regard to future or secondary uses of their data. Data breaches and vulnerabilities: Whether in private direct-to-consumer (DTC), government, or medical settings, DNA data is susceptible to security breaches due to its vast database storage. When de-identified genetic data is combined with publicly accessible information, like that found on genealogical websites, it can occasionally be re-identified, jeopardizing privacy. The research article caters the legal challenges in protecting DNA privacy and regulating genetic protection.

Keywords: Genetic data, DNA privacy, Genomic data security, Genetic discrimination, Data breaches.

INTRODUCTION

Recent developments in molecular biology and genetics have transformed medicine by opening up previously unheard-of possibilities for individualized care and a better comprehension of human health. These innovations are accompanied, therefore, by intricate and dynamic legal issues pertaining to DNA and genetic information privacy and protection. Genetic material is distinct, unchangeable, and contains incredibly sensitive and extensive information on a person's health, inclinations, and even family ties, in contrast to other types of personal data. This data is easily retrieved from everyday sources, such as hair or saliva, and is very portable, allowing it to be shared and kept in large databases in the commercial, governmental, medical, and scientific domains. The introduction of direct-to-consumer (DTC) genetic testing and large-scale genetic databases has increased these issues. While delivering significant insights regarding genealogy and health risks, these services expose users and their families to hazards like data breaches, misuse, and discrimination in employment and insurance. Compounding the issue is a patchwork of inconsistent and often insufficient federal, state, and international regulations struggling to keep pace with rapid technological advancements. Due to the complicated legal context brought up by the quick development of genetic technology, society is being forced to reconsider long-held beliefs about individual rights and privacy.

Legislators, judges, and individuals must address these issues as genetic testing becomes more widespread in order to guarantee the responsible use of genetic data while striking a balance between scientific advancement and the moral obligation to uphold human rights and dignity. Thanks to growing public awareness and technological developments, genetic testing has been increasingly popular in India in recent years. These days, tests can be used for a variety of things, such as tracking down ancestors, determining a person's risk of contracting specific illnesses, and creating individualized treatment regimens. Although these tests have many advantages, they also gather a lot of biological and personal data that needs to be handled carefully to avoid abuse.

INTRODUCTION TO THE DNA PRIVACY AND GENETIC PROTECTION

The right to manage one's genetic data and shield it from unauthorized access, use, or disclosure is known as DNA privacy. The legal and policy frameworks put in place to uphold this right and prevent genetic discrimination by organizations such as the government, insurance companies, and employers are referred to as genetic protection. Why special protection is

needed for genetic data For a number of reasons, genetic data is regarded as being more sensitive than other types of personal information.

Uniqueness: Each person has a distinct genetic code, with the exception of identical twins. This data may act as an unchangeable, permanent identifier, making complete anonymization impossible and raising the possibility of re-identification.

Implications for family: Without their express consent, a person's genetic information is shared with their blood relatives and may disclose details about their ancestry, parentage, and general health. The "right not to know" and medical confidentiality present difficult moral conundrums as a result.

Predictive nature: Even if a person is asymptomatic at the moment, genetic testing can identify their susceptibility to future diseases. This information can be used to discriminate based on perceived genetic risk, even though it is helpful for proactive health management.

Historical misuse: The historical misuse of genetic data in eugenics movements raises public concerns and shows how seriously society could be harmed if these data are not properly protected.

Genetic material, such as DNA from saliva or a discarded item, is widely available and simple to obtain, frequently without the subject's knowledge or consent. This brings up concerns about privacy due to covert testing.

Benefits of Genetic Information: Genetic information can provide information about ancestry, health, and disease. This information can be utilized in medical research, raise an individual's awareness of their own health, and facilitate early disease prevention intervention. Genetic data, which includes a person's DNA and chromosomes, has drawbacks. It can provide private information about ancestry and health. Genetic tests sold directly to consumers are not always accurate and may unintentionally reveal personal information. Unauthorized access to genetic data can have detrimental effects on a person's life and privacy, including unwanted reactions from the government, insurance companies, and employers.

Status of Genetic Privacy:

In 2018, The Delhi High Court ruled against United India Insurance Company's discrimination

in health insurance against a person with a heart disease that was thought to be a genetic disorder. Genetic discrimination is a breach of Article 14, which guarantees that everyone is treated fairly under the law. [1]The Supreme Court of India unanimously stated that the Right to Privacy is a Fundamental Right under Article 21 in Justice KS Puttaswamy (Retd.) & Anr. v. Union of India[2]. Genetic discrimination is illegal in almost all countries. In 2008, the United States passed the Genetic Information Non-discrimination Act (GINA), a federal law that protects people from genetic discrimination in health care and jobs.

The Genomic Revolution

The term "genomic revolution" describes the paradigm shift in biology and medicine brought about by quick and affordable developments in genetic testing, DNA sequencing, and the computational field of bioinformatics. This advancement has had a significant impact on society by paving the way for the era of personalized medicine and revolutionizing diagnosis and treatment. However, it also raises difficult moral, legal, and societal issues related to genetic privacy. DNA sequencing is the foundational technology of the relatively new scientific field of genomics. The scope of research has expanded in tandem with technological advancements that have reduced the cost and scale of genome characterization over the course of sequencing's 40-year history. The paradigm of genomics has been revolutionized by massively parallel sequencing, which allows for the genome-wide investigation of biological issues. Clinical diagnostics and other facets of healthcare, such as disease risk, therapeutic identification, and prenatal testing, are now made possible by sequencing. The current status of genomics in the era of massively parallel sequencing is examined in this review.

The Concept of Genetic Privacy

Genetic data includes a great deal of personal and predictive information that affects not only the person being tested but also their biological relatives, it is thought to be particularly sensitive. This unique quality is frequently called "genetic exceptionalism" and is a major topic in discussions about DNA privacy from a legal and ethical standpoint.

Predictive health data

Future health status: Genetic testing can identify a person's inherited susceptibilities to certain

[1] United India Insurance Co. Ltd. v. Jai Parkash Tayal, 2018 SCC OnLine Del 12915 (India).
[2] Justice KS Puttaswamy (Retd.) & Anr. v. Union of India

diseases, including Alzheimer's, heart disease, and some forms of cancer. This data can be used to discriminate based on perceived future health risks, even though it is useful for proactive health management. Not only a diagnosis This data can offer a lifetime of health-related information and is not just useful for diagnosing conditions A genome sequence that was gathered decades ago for a different reason might yield new health insights as genetic research progresses, raising persistent privacy issues.

Details regarding ancestry

Tracing ancestry: A person's ancestry can be determined through genetic testing, which provides details about their origins and the historical migration patterns of their ancestors.

Unexpected revelations: Genetic ancestry testing can reveal surprising and occasionally upsetting family secrets for people who are adopted or whose parentage is unclear. Large databases that can be used to link people with unknown relatives have proliferated as a result of the rise in consumer genetic testing, which has significant social and personal ramifications.

Effects on biological relatives

Information shared: Since close relatives share a large portion of their DNA, genetic data has a "supra-individual" or "familial" character. One person's genetic test may reveal private and sensitive information about their blood relatives who have not given their consent. Healthcare professionals face ethical dilemmas as a result of this, having to weigh their obligation to maintain patient confidentiality against the possibility of having to alert family members of a hereditary disease to the patient's increased risk.

Identification and irreversibility

Data that cannot be changed: The human genome is mostly unchangeable and does not alter over the course of a person's lifetime. Genetic information cannot be retracted once it is made public, and its meaning may change as science develops.

Identifiability over time: Genetic information can never be completely anonymized, in contrast to other personal data that can be "de-identified." Researchers have linked public genetic data to individual identities using other public records, demonstrating that re-identification is always

a risk due to its uniqueness (for all but identical twins).[3]

Historical Context and Early Legal Responses

In the 1990s, the first wave of human genome projects most notably the public U.S. Human Genome Project (HGP) and its private rivals catalysed the field of genetics while simultaneously requiring a direct response to a number of difficult ethical and legal issues. A slow and disjointed response resulted from early legal frameworks' inability to manage the special sensitivity and familial nature of genetic data.

Initial ethical and legal issues

• *Genetic prejudice:* The possibility that genetic data would be used to discriminate against people was one of the most urgent early worries.

• *Employment:* There were concerns that companies might use genetic information to reject applicants for jobs, fire employees, or deny promotions on the basis of a suspected genetic predisposition to specific illnesses. This was especially problematic in industries that deal with hazardous materials, where employers may screen for employees who have a genetic predisposition to occupational diseases.

• *Insurance:* Another significant area of concern was the insurance sector. Actuaries may use the results of genetic tests to support premium increases or exclusions from health, life, or disability insurance for individuals with specific genetic risks.

Implications for family

Conflicts over privacy and consent arose because genetic information was shared.

• *Family privacy:* One person's consent essentially makes genetic information about their relatives who might not have given their consent or might have a "right not to know"—public.

• *Duty to warn vs. duty of confidentiality:* Genetic information can pose a risk to family members (e.g., a hereditary cancer risk). Medical personnel had to balance their obligation to protect patient privacy with their possible moral or legal obligation to alert family members

[3] Mark A. Rothstein, "Is Deidentification Sufficient to Protect Health Privacy in Research?," 10 Am. J. Bioethics 3 (2010)

who might be in danger.

• *Eugenics potential:* The HGP was plagued by the spectre of past eugenics campaigns. There have been worries expressed regarding the possible abuse of genetic knowledge to establish social hierarchies or base reproductive choices on genetic "fitness."

Dependency on current legislation and fragmented state laws

• *Existing laws are inadequate:* Statutes pertaining to general privacy and medical information, like the Health Insurance Portability and Accountability Act (HIPAA), did not particularly address the special characteristics of genetic data. Enacted in 1996, HIPAA provided general protection for health information, but it did not provide full protection for genetic data.

• *Different state laws:* A patchwork of state laws developed in the absence of comprehensive federal action. Early laws varied greatly in their reach and efficacy and frequently targeted particular illnesses, such as sickle-cell anaemia. This led to contradictions and failed to address all of the issues related to genetic discrimination.

Legislative delays and concessions

It took nearly two decades for meaningful federal legislation to emerge.

• *Pushback from the industry:* Initially, federal anti-discrimination laws were opposed by the insurance industry and some business associations, who argued that genetic information was a necessary tool for risk assessment.

• *GINA's restricted scope:* The 2008 passage of the Genetic Information Non-discrimination Act (GINA) was a major step forward, but its application was limited. It provided federal protection against genetic discrimination in health insurance and employment, but it did not cover life, disability, or long-term care insurance.

This historical trajectory demonstrates how scientific discoveries can swiftly surpass established legal and ethical frameworks. Even though the legal system's tardy response left gaps that are still being filled today, the initial concerns raised during the HGP set the stage for future discussions.

THE CHANGING LEGAL DEFINITION OF GENETIC INFORMATION

Genetic Data vs. "Sensitive Personal Data"

Genetic Data is personal information about a person's inherited or acquired genetic traits is known as genetic data. It is obtained by analysing biological samples, like blood or saliva, and can be used to determine a person's identity as well as details about their background, health, and even biological kin.

Sensitive personal data (SPD) is a subset of personal data that is legally protected to a higher degree because it is sensitive and could cause more harm to an individual if compromised. Sensitive personal data is usually more private information that, if handled improperly, may result in financial fraud, stigma, or discrimination, even though personal data generally refers to any information that can be used to identify an individual.

The majority of jurisdictions agree that genetic data needs special protection, but they differ greatly in how they define and govern it. A patchwork of inconsistent laws may result from this. The main question is whether genetic data should fall under a distinct and particular category or be covered by more expansive and general definitions of privacy.

Clearly classified jurisdictions

The General Data Protection Regulation (GDPR) of the European Union (EU)

Article 9 of the GDPR specifically names "genetic data" as a "special category of personal data." This puts it in the same category as other sensitive data, such as biometric, health, and ethnic origin data.

Genetic data is defined by GDPR as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person."

Implications: Unless there is a specific exemption, processing genetic data is normally forbidden due to explicit classification under Article 9. The most frequent exception is the individual's express consent, which must be more detailed and open than it is for other types of personal information.

The Genetic Information Privacy Act (GIPA) in California

California's strategy blends a specialized statute with more general privacy law.

Direct-to-consumer (DTC) genetic testing businesses are specifically governed by GIPA. It requires businesses to obtain explicit consent for disclosure, give consumers clear policies on data collection, and respect their request to have their biological sample and genetic data destroyed.

CPRA/CCPA: Genetic information is classified as sensitive personal information under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA). This imposes extra responsibilities on businesses that handle this data, such as obtaining consent before collecting it.

The Digital Personal Data Protection (DPDP) Act of 2023 [4]in India

The new law in India is controversial because it does not specifically classify genetic data as sensitive, which is a significant distinction from the GDPR.

No Particular Category: Genetic information is neither defined nor classified as sensitive personal information under the DPDP Act. This indicates that it is handled using the same general "notice-and-consent" framework as non-sensitive data.

Inadequate Defences: Critics contend that this method ignores the special dangers associated with genetic information, including its familial nature and the possibility of stigmatization and discrimination.

The difficulty of striking a balance between context and exceptionalism

The divergent methods draw attention to a primary conflict:

Genetic Exceptionalism (EU): The idea that genetic information is particularly sensitive and should be given extra, stringent protection.

Contextual Method (US/India): believing that rather than being handled according to its

[4] The Digital Personal Data Protection (DPDP) Act of 2023

intrinsic qualities, genetic data should be handled according to its identifiability, context of use, and potential for harm.

The difficulty of developing broadly applicable legal principles for genetic data is illustrated by the differences between these frameworks. Some contend that privacy objectives would be better served by a strategy that places more emphasis on the particular applications of genetic data than on its innate "special" status.

GENETIC DATA IN CRIMINAL JUSTICE AND FORENSICS

Forensic DNA Databases

Since its establishment in the 1990s, the U.S. Combined DNA Index System (CODIS), a fundamental forensic tool, has expanded dramatically. CODIS, a cooperative and decentralized system, has increased its data capacity, search capabilities, and collection criteria, sparking continuous discussions about how to regulate it and strike a moral balance between privacy protection and crime solving.

The establishment and composition of CODIS

The FBI implemented the National DNA Index System (NDIS) in 1998, and the federal DNA Identification Act of 1994 authorized the creation of CODIS. The three-tiered hierarchy upon which the system is based permits information exchange between various jurisdictions:

•Local forensic labs initially create DNA profiles through the Local DNA Index System (LDIS).

•All of the LDIS profiles in a state are centrally stored in the State DNA Index System (SDIS), a state-level database.

•The FBI oversees the National DNA Index System (NDIS), which is a nationwide database of DNA profiles submitted by participating state and federal agencies.

Control and supervision

•Federal and state law: While individual states frequently have their own laws for their respective SDIS and LDIS databases, federal law establishes standards for profiles submitted

to the national NDIS. These state laws may have different retention policies or more expansive collection criteria.

•Mechanisms of oversight: Quality assurance standards (QAS) are required by the FBI for all labs taking part in the CODIS program. Policies created and put into effect at the local and state levels, which cover everything from hit confirmation to sample processing, also provide oversight.

Legal and ethical disputes

•Racial and socioeconomic bias: Racial differences in arrest rates and policing tend to be reflected in the makeup of forensic DNA databases. Critics contend that the extension of collection to arrestees disproportionately impacts minority groups and that it exacerbates pre-existing biases within the criminal justice system.

•Rights to privacy: It has been argued that the gathering and permanent storage of DNA profiles from people—particularly those who have never been found guilty—violates their right to privacy and the Fourth Amendment's ban on unjustified searches. The privacy rights of a suspect's relatives who have not been charged with a crime are also called into question by the use of IGG and familial searching.

Legal requirements and safeguards

• *Constitutional challenges:* The Fourth Amendment, which forbids unjustified search and seizure, was invoked in the United States to contest the collection of DNA from arrestees.

• *Informed consent:* The necessity of obtaining informed consent from family members and clients of for-profit genealogy services is a topic of discussion in many jurisdictions, especially in light of recent innovations like IGG.

• *Legal protections:* The complete lifecycle of DNA data, from collection to expungement, must be governed by precise, well-defined legislation. Additionally, oversight organizations must be established to guarantee accountability.

Legal and Constitutional Rights

Strong but not absolute protection against "unreasonable searches and seizures" is offered by

the Fourth Amendment of the US Constitution. Law enforcement's use of DNA has sparked intense constitutional discussion about how these rights should be applied, especially in relation to the privacy of genetic data, the extent of warrantless searches, and the rights of both arrestees and their innocent family members.

Maryland v. King: Warrantless collection from arrestees

In Maryland v. King, decided in 2013[5], the Supreme Court considered whether it was constitutional to take a felony arrestee's DNA as part of a standard booking process.

The case: In accordance with Maryland law, Alonzo King had his cheek swabbed for a DNA sample after being arrested for a serious offense. King was charged with rape because the sample matched an unresolved case from 2003.

In a 5-4 ruling, the Court ruled that the DNA cheek swab was a Fourth Amendment-protected reasonable search, comparing it to taking an arrestee's fingerprints and taking their picture.

The justification The legitimate interests of the government were the main focus of the majority opinion:

• *Correct identification:* One of the most important aspects of the booking procedure is correctly identifying the person who has been arrested.

• *Officer and public safety:* An arrestee's criminal history can be used to assess whether they are a risk.

• Determining an arrestee's potential risk to the public if they are released on bail can be aided by DNA evidence.

• *The opposition:* The dissent contended that since DNA collection looks for proof of prior offenses unrelated to the current arrest, it constitutes a far greater invasion of privacy than fingerprinting.

• *Innocent relatives' right to privacy:* The biggest worry is that law enforcement is successfully searching innocent family members using a person's DNA. These family members are not

[5] Maryland v. King, decided in 2013

under criminal suspicion and have not granted permission for a search.

• The "reasonableness" standard of the Fourth Amendment requires courts to weigh the government's interest in solving major crimes against people's and their families' right to privacy.

• *Absence of judicial oversight:* Family searches are frequently carried out by law enforcement with little to no judicial supervision. Critics contend that a warrant or court order based on a lesser standard of suspicion than probable cause should be required for this procedure, at the very least.

The "third-party doctrine" and genetic genealogy.

Investigative genetic genealogy (IGG) is the process of identifying suspects by looking for distant relatives using consumer DNA websites like GEDmatch. The "third-party doctrine," a legal precedent that maintains that people have no legitimate expectation of privacy in information they voluntarily share with third parties, is challenged by this practice.

•The Carpenter precedent: In Carpenter vs. United States (2018), the Supreme Court decided that even though cell phone location data was stored by a third-party company, police still needed a warrant to access it. The Court reasoned that the Fourth Amendment protected the data because of its vast volume and highly revealing nature.

•Carpenter's application to genetic genealogy: Many legal experts contend that IGG should be subject to the Carpenter precedent. A warrant should be needed to search consumer genetic databases because genetic data is arguably more sensitive and revealing than cell phone data.

Genetic Data in Criminal justice and forensics in India

Although DNA technology has a long history in Indian criminal justice, the country's legal system is convoluted and disjointed. Instead of a single, specific statute for a national DNA database, it depends on a patchwork of procedural laws and court precedents. Since many of the provisions of the proposed DNA Technology (Use and Application) Regulation Bill, 2019 were incorporated into the Criminal Procedure (Identification) Act, 2022, the bill was withdrawn in 2023. Concerns about data privacy, constitutional rights, and ethics continue to

cast doubt on the use of genetic data.[6]

The existing legal system, courts rely on a number of provisions from various statutes because there is no specific law pertaining to DNA profiling.

• *The 2022 Criminal Procedure (Identification) Act (CPI Act):* [7]The Identification of Prisoners Act of 1920 was superseded by this law, which greatly increased law enforcement's authority to gather and preserve "measurements," such as biological samples and their analysis.

• *Required collection:* Under the Act, biological samples must be taken from anyone detained for crimes against women or children or for crimes carrying a sentence of seven years or more in prison.

• *Creation of a database:* It gives the National Crime Records Bureau (NCRB) permission to gather, preserve, handle, and disseminate these records for a period of 75 years.

• *In 2023, Bharatiya Nagarik Suraksha Sanhita (BNSS):* The BNSS allows for the medical examination and collection of biological samples, including DNA, from accused individuals during an investigation, taking the place of the Code of Criminal Procedure (CrPC).

• *The 1872 Indian Evidence Act:* DNA evidence is admissible in court and is regarded as expert opinion under Section 45. It is not regarded as definitive proof on its own, though, and its weight and probative value are open to interpretation.

Legal precedents: Indian courts have rendered decisions outlining the parameters and extent of DNA evidence:

 The Supreme Court stated in Selvi v. State of Karnataka (2010)[8] that the collection and preservation of tangible evidence, such as DNA samples, are not subject to the same constitutional restrictions as the involuntary use of specific forensic techniques.

 The Supreme Court published new guidelines in Kattavellai @ Devakar v. State of Tamil Nadu (2025) [9]to guarantee the integrity and appropriate handling of DNA samples in criminal

[6] Sanger, F., et al. "DNA Sequencing with Chain-Terminating Inhibitors." Proceedings of the National Academy of Sciences, vol. 74, no. 12, 1977, pp. 5463–5467.
[7] The Criminal Procedure (Identification) Act, 2022
[8] Selvi v. State of Karnataka (2010)
[9] Kattavellai @ Devakar v. State of Tamil Nadu (2025)

cases, with a focus on the chain of custody and prompt submission to forensic labs.

Privacy and constitutional issues

The Supreme Court upheld the right to privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017)[10], but the use of DNA technology in India has sparked serious concerns.

Privacy and physical integrity rights: Critics contend that by permitting the non-consensual collection of biological samples, the CPI Act's and other related laws' expanded powers violate people's rights to privacy and bodily integrity. Legal professionals wonder if such widespread violations are justified by the state's interest in maintaining law and order.

The 2023 Digital Personal Data Protection (DPDP) Act: The sensitive nature of genetic data, which affects not only the individual but also their entire family, is not sufficiently addressed by this Act's general "notice-and-consent" data processing model. Genetic information is susceptible to possible misuse because it is not considered sensitive personal data by the law.

Article 20(3), the right against self-incrimination: According to Indian courts, the right against self-incrimination is not violated by the collection of DNA samples since it is not a type of testimonial compulsion.

Equality and discrimination: Concerns have been raised about the potential use of genetic information for discrimination in insurance, work, and other contexts. Although the Delhi High Court has declared that discrimination on the basis of genetic conditions is prohibited, there is currently a lack of strong legislation.

Technological gaps and capabilities

Even though India has established DNA testing procedures and developed sophisticated forensic labs like the Centre for DNA Fingerprinting and Diagnostics (CDFD), there are still many obstacles to overcome.

• *Forensic infrastructure:* The lack of standardized procedures, resource constraints, and backlogs at Forensic Science Laboratories (FSLs) can result in delayed results, contaminated

[10] Justice K.S. Puttaswamy v. Union of India (2017)

samples, and the possibility that evidence will be excluded from trial.

• *Limitations of the database:* Although there have been plans for a national DNA database since 2003, it has not yet been fully operationalized with a strong legal foundation. A national system is currently being developed, although Himachal Pradesh has set up a state-level database for unidentified bodies.

• *Genetic genealogy:* Although genetic genealogy databases such as GEDmatch are used by law enforcement in the United States, their use in India is not specifically regulated and presents difficult privacy and ethical problems.

Although India has made progress in integrating DNA evidence into its criminal justice system, there is still a big ethical and legal gap. Without a specific law, the use of patchwork legislation and judicial interpretation fails to address important concerns about data security, consent, and privacy. To create a national database with stringent ethical oversight, strong data protection, and open procedures for managing genetic data, a comprehensive DNA-specific law is required.

CONCLUSION

A complex environment characterized by substantial technological promise, disjointed legal frameworks, and enduring ethical and constitutional challenges characterizes the development of forensic DNA databases in India. Although DNA evidence has been crucial in settling significant criminal cases and clearing innocent people, its regulation has been haphazard, depending on both general criminal procedure laws and court precedent. India decided to integrate genetic data collection into the current system, mainly through the Criminal Procedure (Identification) Act, 2022 (CPI Act), after the proposed DNA Technology Bill was withdrawn. However, this strategy has not entirely addressed the core problems of data security, consent, and privacy, particularly with regard to the creation of a national DNA database.

Findings

• Dependency on a Disjointed Legal System: The Indian Evidence Act, the CPI Act, and court rulings are among the patchwork of laws that regulate the use of DNA evidence in India. As a result, there is now uncertainty about standardization and admissibility, which may cause irregularities in court cases.

• Extension of Collection Powers: By extending the period of record retention to 75 years, the CPI Act, 2022, greatly increased the state's authority to obtain biological samples from arrestees, prisoners, and people in preventive detention. Critics contend that this overreach may violate the right to privacy by obfuscating the distinction between those who have been found guilty and those who have only been charged or detained.

• Lack of Explicit Genetic Data Protection: India does not have any specific laws that specifically protect genetic data, even though the Supreme Court upheld the right to privacy in the Puttaswamy ruling. Though a positive step for general data, the Digital Personal Data Protection (DPDP) Act, 2023, offers extensive exemptions for state instrumentalities and does not classify genetic information as sensitive personal data.

• Privacy and Surveillance Issues: One major worry is the possibility of abuse, "function creep," and state-approved biological surveillance. Without express consent or supervision, genetic data may be used for purposes other than criminal investigations due to the absence of particular legal protections pertaining to data retention, deletion, and cross-referencing.

• The quality and timeliness of DNA analysis are impacted by problems like sample contamination, inconsistent handling, and a lack of lab capacity, which cause India's forensic science infrastructure to lag behind international standards. This compromises the integrity of DNA results in court and increases the possibility of shaky evidence.

• Vulnerability to Genetic Discrimination Genetic discrimination in insurance, employment, and other areas is still a real threat in the absence of specific legal provisions similar to the Genetic Information Non-discrimination Act (GINA) in the United States.

Suggestions

The following recommendations ought to be taken into account in order to develop a strong and moral framework for the use of genetic data in India's criminal justice system:

• Adopt Specific Genetic Data Law: There is an immediate need for a stand-alone law that addresses the special characteristics of genetic data. This law should establish a data protection authority with specialized knowledge in genomics, clearly define acceptable uses, and develop a strong consent framework.

• Classify Genetic Data and Put Risk-Based Processing into Practice: Genetic data should be specifically recognized as a highly sensitive category by amending the DPDP Act. A risk-based framework should be used in future regulations, with stronger processing standards for high-risk applications and improved protections against abuse.

• Adopt Specific Genetic Data Law: There is an immediate need for a stand-alone law that addresses the special characteristics of genetic data. This law should establish a data protection authority with specialized knowledge in genomics, clearly define acceptable uses, and develop a strong consent framework.

• Classify Genetic Data and Put Risk-Based Processing into Practice: Genetic data should be specifically recognized as a highly sensitive category by amending the DPDP Act. A risk-based framework should be used in future regulations, with stronger processing standards for high-risk applications and improved protections against abuse.

REFERENCES

• BOOKS

1.Mark A. Rothstein (ed.), Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era. Yale University Press, 1997.

2.Bartha Maria Knoppers, Genetics and Life Insurance: Medical Underwriting and Social Policy. Kluwer Law International, 2002.

3.Graeme Laurie, Genetic Privacy: A Challenge to Medico-Legal Norms. Cambridge University Press, 2002.

4.Sheila Jasanoff, Designs on Nature: Science and Democracy in Europe and the United States. Princeton University Press, 2005.

5.Laurie, Graeme, Shawn Harmon, and Edward Dove, Mason and McCall Smith's Law and Medical Ethics. Oxford University Press, 2021 (12th ed.).

• ARTICLES AND LAW JOURNALS

1.Human Genome Project, U.S. Department of Energy Office of Science, National Institutes of Health (2003).

2.Sanger, F., et al. "DNA Sequencing with Chain-Terminating Inhibitors." Proceedings of the National Academy of Sciences, vol. 74, no. 12, 1977, pp. 5463–5467.

3.Rothstein, Mark A. "The Law of Genetic Privacy: Applications, Implications, and Limitations." Journal of Law, Medicine & Ethics, vol. 40, no. 4, 2012, pp. 804–812.

4.Saha, Anirban. "Legal Issues Surrounding Genetic Testing and Data Privacy in India." Indian Journal of Law and Technology, vol. 15, no. 2, 2021.

5.U.S. Department of Health and Human Services. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164.

• CASES

1.Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India, (2017) 10 SCC 1.

2.Mr. X v. Hospital Z, (1998) 8 SCC 296

3.Selvi v. State of Karnataka, (2010) 7 SCC 263.

4.Kattavellai @ Devakar v. State of Tamil Nadu, (2025) SCC OnLine SC (DNA Evidence Guidelines Case).

5.United India Insurance Co. Ltd. v. Jai Parkash Tayal, (2018) SCC OnLine Del 11199.

6.People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

7.Maryland v. King, 569 U.S. 435 (2013).

8.Carpenter v. United States, 138 S. Ct. 2206 (2018).

9.Ferguson v. City of Charleston, 532 U.S. 67 (2001).

10.Skinner v. Railway Labor Executives' Association, 489 U.S. 602 (1989)

11.Schmerber v. California, 384 U.S. 757 (1966).

• WEBLIOGRAPHY

1.World Health Organization. "Genomic Resource Centre." https://www.who.int/genomics

2.Ministry of Electronics and Information Technology (MeitY), Government of India. "Digital Personal Data Protection Act, 2023." https://www.meity.gov.in

3.European Commission. "EU General Data Protection Regulation (GDPR)." https://gdpr.eu

4.National Human Genome Research Institute. "Ethical, Legal, and Social Implications (ELSI) of Genomics." https://www.genome.gov

5.United States Department of Justice. "Combined DNA Index System (CODIS)."https://www.fbi.gov/services/laboratory/biometric-analysis/codis