



Genetic Privacy and Data Protection in India: Emerging Legal Challenges in the Age of Genomic Research

Nitesh Mehra^{1,2} ✉

¹ NMA Law Offices, New Delhi, India

² Delhi High Court Bar Association, New Delhi, India

Аннотация

Genetic data is a highly specific type of personal data, being inalterable, inherently family-like, capable of being used to predict future health states, and incapable of being completely anonymized. With the growing strides India is making towards its genomic goals defined under the Genome India project and the general push for precision medicine, the current legal architecture to regulate genomic data has become a pressing constitutional, statutory, and ethical concern. This article engages in a doctrinal analysis and comparative legal analysis of the existing regulatory framework of genomic data in India, namely the Justice K.S. Puttaswamy (Retd.) v Union of India (2017) case, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, and the Indian Council of Medical Research (ICMR) National Ethical Guidelines, 2017.

The analysis places India's framework in a comparative perspective, which is based on the General Data Protection Regulation of the European Union, the Genetic Information Nondiscrimination Act of the United States, as well as institutional governance models of the United Kingdom Biobank and Genomics England. The study points out six key regulatory gaps in the Indian regulatory landscape: the absence of a sui generis special category for genetic data, the absence of an adequate informed consent architecture suitable for longitudinal genomic research, the lack of statutory storage and retention limits, the lack of an anti-genetic discrimination statute, structural vulnerabilities in cross-border data transfer governance, and the total absence of any statutory frameworks for AI-driven predictive genomics. The article concludes with evidence-based recommendations for the enactment of a dedicated Genetic Data Protection Act, a Genetic Non-Discrimination Act, and a National Genomic Data Regulatory Authority.

✉ Email: advniteshmehra@gmail.com

Keywords: genetic data, data protection, privacy, genetic discrimination, informed consent, India

To cite this article: Mehra, N. (2026). Genetic privacy and data protection in India: Emerging legal challenges in the age of genomic research. *Lex Genetica*, 5(2), 91–120. (In Russ.). <https://doi.org/10.17803/lex-gen-2026-5-2-91-120>

Received: 10.034.2026

Review completed: 03.04.2026

Accepted: 01.05.2026

Генетическая конфиденциальность и защита данных в Индии: новые правовые вызовы в эпоху геномных исследований

Нитеш Мехра^{1,2} ✉

¹ Юридическая фирма NMA, Нью-Дели, Индия

² Ассоциации адвокатов Высокого суда Дели, Нью-Дели, Индия

Аннотация

Генетические данные представляют собой особый тип персональных данных, поскольку они неизменяемы, носят по своей природе «семейный» характер, могут использоваться для прогнозирования будущего состояния здоровья и не могут быть полностью анонимизированы. В условиях значительного прогресса, которого Индия достигает в реализации своих геномных целей в рамках проекта Genome India, а также развития персонализированной медицины, существующая правовая архитектура регулирования геномных данных становится актуальной конституционной, законодательной и этической проблемой. В статье проводится доктринальный и сравнительно-правовой анализ действующей нормативной базы регулирования геномных данных в Индии, а именно: решения по делу Justice K.S. Puttaswamy (Retd.) v Union of India (2017), Закона о защите цифровых персональных данных 2023 г. (Digital Personal Data Protection Act, DPDP, 2023), Правил к Закону о защите цифровых персональных данных 2025 г. (Digital Personal Data Protection Rules, DPDPR, 2025), а также Национальных этических руководящих принципов Индийского совета медицинских исследований (ICMR) 2017 г.

При сравнении индийской правовой системы автор опирается на Общий регламент по защите данных Европейского союза (GDPR), Закон США о недискриминации генетической информации (Genetic Information Nondiscrimination Act, GINA), а также институциональные модели управления, такие как UK Biobank и Genomics England. В исследовании выявляются шесть ключевых пробелов в ин-

✉ Email: advniteshmehra@gmail.com

дийском регулировании: отсутствие особой категории *sui generis* для генетических данных, недостаточность модели информированного согласия, не приспособленной для долгосрочных геномных исследований, отсутствие установленных законом сроков хранения и удаления данных, отсутствие закона о недопустимости генетической дискриминации, структурные уязвимости в регулировании трансграничной передачи данных, а также полное отсутствие нормативной базы для предиктивной геномики, основанной на искусственном интеллекте. В заключение предлагаются основанные на эмпирических данных рекомендации по принятию специального Закона о защите генетических данных, Закона о недискриминации по генетическому признаку и создания Национального регулятора геномных данных.

Ключевые слова: генетические данные, защита данных, конфиденциальность, генетическая дискриминация, информированное согласие, Индия

Для цитирования: Мехра, Н. (2026). Генетическая конфиденциальность и защита данных в Индии: новые правовые вызовы в эпоху геномных исследований. *Lex Genetica*, 5(2), 91–120. (In Russ.). <https://doi.org/10.17803/lexgen-2026-5-2-91-120>

Поступила в редакцию: 10.03.2026

Получена после рецензирования и доработки: 03.04.2026

Принята к публикации: 01.05.2026

Introduction

The exponential development of genomics is one of the main drivers behind the revolutionary changes that modern medicine, biotech, and biomedical research have undergone in the recent past. New approaches to genome analysis, such as high-throughput DNA sequencing, genome-wide association studies, precision medicine, and genetic editing techniques, lie behind significant research progress in understanding the role of genetics in both health and diseases (Tabor et al., 2011; Knoppers et al., 2014). Moreover, when considering the ever-growing availability and decreasing costs of genetic technology, it becomes clear that the utilization of genetic information has become vital for diagnosis, medicine, public health, and biomedical research.

As the application of genomic technologies to healthcare and biomedical research

becomes more widespread, there is an unprecedented need for the collection, processing, analysis, storage, and use of genetic information in scientific research. While such developments are expected to contribute to scientific and medical breakthroughs in disease prevention and treatments, multiple legal and ethical concerns are associated with the governance and regulation of genetic information (Knoppers et al., 2014; Phillips et al., 2021).

An additional complexity arises from the inherently familial nature of genetic information (UNESCO, 2003). For example, disclosure of genetic data by an individual may inadvertently reveal biological information regarding relatives who have neither undergone genetic testing nor consented to disclosure of such information. Issues of genetic

privacy thus extend beyond individual autonomy to raise broader concerns regarding familial privacy, collective interests, and intergenerational rights. Unauthorized access to or misuse of genetic information may produce consequences that affect entire family networks (Erich et al., 2018).

Meanwhile the increasing commercialization of genetic information has further complicated these concerns, creating new tensions between making scientific discoveries, advancing economic interests, and protecting individual rights. In response some countries have created laws and regulations to control the collection, processing, and use of genetic information. Laws such as The European Union's General Data Protection Regulation (GDPR)¹ and The United States Genetic Information Nondiscrimination Act (GINA)² confirms the recognition on the part of many countries that genetic data needs special legal protection due to its uniquely sensitive nature.

In India, concerns relating to genetic privacy have gained renewed significance following the case of Justice K.S. Puttaswamy v. Union of India, in which privacy was recognized as a fundamental right. The Supreme Court further emphasized that individual autonomy provides an essential foundation for contemporary data protection discourse (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017). Recently India enacted a law called the Digital Personal Data Protection Act, 2023³. While this is a significant step

towards regulating and protecting personal data, it remains unclear whether these rules are adequate for the special challenges of genetic and genomic information. Unlike some countries, India does not have a special set of normative rules aimed specifically at ensuring genetic privacy, preventing genetic discrimination, and governing the use of genomic databases.

In terms of substantial literature concerning privacy, bioethics, and data protection, limited scholarly attention has been devoted to the Indian legal context (Solove, 2006). The majority of scholars fail to address the legal issues that arise in connection with genetic technologies. This gap is particularly essential in the light of the rapid expansion of genomic research initiatives and cross-border data flows.

The present work examines whether the current legal framework is adequate to regulate and protect genetic information. The article also highlights challenges related to informed consent, genetic discrimination, and data governance through a comparative analysis of foreign legal approaches. Genetic information represents a unique category of personal data requiring a dedicated regulatory framework capable of supporting scientific progress while protecting privacy, autonomy, and human dignity.

Research Objectives

The specific objectives of this study are as follows:

¹ Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR). *EUR-Lex*. Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html>

² *The Genetic Information Nondiscrimination Act of 2008*. Available at: <https://www.govinfo.gov/content/pkg/PLAW-110publ233/html/PLAW-110publ233.htm>

³ *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023. (2023, August 11). *Gazette of India*, pt. II, sec. 1 Available at: <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>

1. To examine the nature and significance of genetic data and assess the extent to which its unique characteristics necessitate enhanced legal protection beyond that afforded to conventional forms of personal information.

2. To critically examine the existing legal and regulatory framework governing genetic information in India, with particular reference to constitutional privacy protections, the Digital Personal Data Protection Act, 2023, and relevant biomedical research guidelines.

3. To identify and analyze the principal legal and ethical challenges arising from the collection, storage, processing, and dissemination of genetic information, with particular emphasis on privacy, informed consent, data security, and the risk of genetic discrimination.

4. To comparatively examine international legal and regulatory approaches to the governance and protection of genetic information, with particular reference to the European Union, the United States, and the United Kingdom.

5. To critically assess the extent to which the current Indian legal and regulatory framework effectively responds to the distinctive privacy, governance, and ethical challenges posed by developments in genomic research and emerging genetic technologies.

6. To develop evidence-based legal and policy recommendations for strengthening the governance and protection of genetic information while fostering responsible scientific innovation, strengthening biomedical research, and pursuing public health objectives.

Literature Review

Genetic data has become one of the most valuable forms of personal information in the modern digital age. Unlike ordinary

personal or medical data, genetic information is persistent, unique to every individual, and capable of revealing sensitive details about a person's health, ancestry, and biological relationships. The increasing use of genome sequencing, genetic testing, and biotechnology research has created new opportunities in healthcare and scientific development. However, it has also raised serious concerns regarding privacy, consent, discrimination, and misuse of data.

Genetic information differs fundamentally from other categories of personal data. A substantial body of scholarship emphasizes that genetic information possesses characteristics that distinguish it from other categories of personal data. Unlike conventional health records, genomic data are permanent, uniquely identifiable, predictive, and inherently relational, revealing information not only about the individual but also about biologically related family members (Knoppers et al., 2014; Phillips et al., 2021). Because genetic variants remain stable throughout life and may generate new clinically relevant information as scientific knowledge evolves, scholars argue that traditional data protection principles require adaptation when applied to genomic information (Kaye, 2012).

Genetic Data as a Permanent Biological Identifier

Researchers highlight the fact that genetic information functions as a permanent biological fingerprint. Unlike health records that can change over time, DNA remains largely unchanged throughout a person's life. Consequently, a breach of genetic data can affect not only the individual concerned, but also family members and future generations. Such disclosures may reveal hereditary dis-

eases, genetic disorders, and other biological characteristics that individuals may prefer to keep private.

Development of Genetic Data Protection in India

Historically, India has not possessed a comprehensive legal framework specifically aimed at governing genetic data. The protection of such information was instead primarily derived from the Information Technology Rules, 2011, and ethical guidelines issued by the Indian Council of Medical Research (ICMR). While these instruments provide basic safeguards, they have proven insufficient to address the complexities associated with genomic research and large-scale data collection initiatives such as the Genome India Project.

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) represents a significant development in India's privacy regime. The Act requires free, informed, and specific consent before processing personal data and places certain obligations upon data fiduciaries to use information only for authorized purposes. This framework provides a foundation for regulating genetic information collected by hospitals, biobanks, research institutions, and direct-to-consumer genetic testing companies.

Legal scholars increasingly conceptualize genetic privacy as extending beyond conventional informational privacy. Solove (2006) argues that privacy cannot be understood solely through secrecy but should also encompass control over personal information and protection against inappropriate use. Building upon this approach, genomic privacy has been described as involving informational autonomy, bodily integrity, decisional freedom, and protection against misuse

of biological identity (Dove et al., 2022; Phillips et al., 2021).

Challenges of Genetic Data Anonymization

A major theme in the contemporary literature emerges in terms of the challenge of anonymizing genetic data. Scholars argue that complete anonymization of genomic information is practically impossible. Even when names and personal identifiers are removed, genetic sequences can often be linked back to individuals through publicly available databases, genealogical records, or other datasets. This creates significant risks of re-identification and highlights the limitations of traditional privacy protection methods.

Although anonymization has traditionally been regarded as an important privacy safeguard, numerous studies have demonstrated that complete de-identification of genomic information is extremely difficult. Gymrek et al. (2013) showed that supposedly anonymous genomic datasets could be re-identified by combining publicly available genetic and genealogical information. Subsequent studies confirmed that advances in computational methods continue to increase re-identification risks despite technical anonymization measures (Erich, Narayanan, 2014; Naveed et al., 2015).

Genetic Discrimination and Legal Gaps

Several studies point out that India lacks a dedicated law prohibiting genetic discrimination. In countries such as the United States, legislation like the Genetic Information Non-discrimination Act (GINA) prevents employers and insurance companies from using genetic information to discriminate against individuals. By contrast, India currently relies on constitutional principles and judicial in-

interpretations rather than specific legislation to address such concerns.

Genetic discrimination has become another important topic in contemporary scholarship. Existing studies demonstrate that genetic information may influence decisions concerning employment, insurance, education, and access to healthcare even in the absence of manifested disease (Joly et al., 2020). Although legal instruments such as the United States Genetic Information Nondiscrimination Act (GINA) address some of these concerns, scholars continue to debate the adequacy of existing legal protections in light of expanding genomic technologies.

Community-Level Privacy Concerns

India's social structure presents unique challenges in genetic research. Many communities are endogamous, meaning that genetic characteristics are concentrated within specific groups. As such, research findings concerning one individual may indirectly reveal information about an entire community. Arguing that traditional individual consent models are insufficient, scholars therefore advocate the inclusion of community-level protections in genetic governance frameworks.

Although the existing literature has extensively examined genetic privacy, genomic governance, informed consent, and comparative regulatory approaches, relatively limited attention has been devoted to the interaction between India's constitutional privacy jurisprudence, the Digital Personal Data Protection Act, 2023, and emerging genomic governance initiatives. Existing studies generally examine these issues separately, whereas little research integrates constitutional law, data protection, biomedical ethics, and comparative legal analysis into a unified

regulatory framework. The present study addresses this gap by examining whether India's existing legal framework adequately protects genetic information in light of international regulatory developments.

Methodology

The present study utilizes a doctrinal, comparative legal analysis methodology to examine the global and domestic regulatory frameworks governing human genetic data. The research is executed in three integrated phases, beginning with an international mapping of diverse governance models. This phase tracks the evolution of soft law through successive UNESCO instruments, evaluates the European Union's GDPR, assesses the anti-discrimination focus of the United States' GINA, and analyzes the governance frameworks utilized by the UK Biobank and Genomics England.

The second phase transitions to a localized, doctrinal appraisal of India's fragmented regulatory landscape. The constitutional evolution of informational autonomy and bodily integrity is considered under Article 21 following the Justice K.S. Puttaswamy (2017) landmark ruling. In addition, the statutory reach and limitations of the Digital Personal Data Protection (DPDP) Act, 2023, are evaluated along with the non-statutory guidelines issued by the ICMR and the Genome India Project.

The final research phase synthesizes these comparative legal traditions against a broader socio-technical backdrop. Contrasting the consent-centric design of the DPDP Act with Russia's Federal Laws No. 24-FZ and No. 152-FZ, the study exposes a shared legislative gap where state sovereignty is prioritized over individual protections against genetic discrimination. The methodology also

evaluates how Privacy-Enhancing Technologies (PETs), including Federated Learning, differential privacy, and secure multi-party computation, can facilitate international data sharing while balancing national sovereignty with collaborative innovation.

Legal Framework

Genetic information regulation in India at present can be interpreted through the prism of constitutional considerations, data protection laws, and medical guidelines on a specific sector. In the absence of a specific legal mechanism regulating genetic data and ensuring its privacy in India, there are several legal and regulatory measures that provide certain protections for such data. These include constitutional right to privacy, Digital Personal Data Protection Act, 2023, and ethical guidelines on biomedical and genetic research⁴. Taken together these form the foundation on which genetic information in India is governed, collected, processed, and protected. This part of the article will focus on the analysis of these relevant constitutional, statutory, and biomedical legal or regulatory regimes with regard to genetic information.

Constitutional Dimensions of Genetic Privacy and Informational Autonomy

When considered as a constitutional right, genetic privacy in India should be discussed

in relation to privacy jurisprudence that has evolved based on Article 21 of the Indian Constitution. Although there are no explicit constitutional provisions protecting genetic information as an individual category of data protected by the constitution, the concepts of privacy, dignity, autonomy, and the right to control information play an important role in its protection (e.g. *Justice K.S. Puttaswamy (Retd.) v. Union of India*⁵). Privacy jurisprudence in India shows how the scope of privacy protections provided by the constitution has expanded over time through judicial decisions that protect the right of citizens against any unnecessary intrusions into their personal lives. It is within precisely this context that the discussion on the constitutional foundations of privacy becomes crucial.

Evolution of the Right to Privacy in India

Early cases like *Kharak Singh v. State of Uttar Pradesh* (1962)⁶ and *Gobind v. State of Madhya Pradesh* (1975)⁷ paved the way for the emergence of the jurisprudence of privacy by recognizing that certain parts of a citizen's life should be protected against unnecessary state intervention. Later on, in *R. Rajagopal v. State of Tamil Nadu* (1994)⁸, the Apex Court held that an individual had a fundamental right to protect his or her personal information from publication, thus establishing informational privacy as an essential part of per-

⁴ Indian Council of Medical Research. (2017). *National Ethical Guidelines for Biomedical and Health Research Involving Human Participants*. Available at: https://www.icmr.gov.in/icmr/object/custom_data/pdf/resource-guidelines/ICMR_Ethical_Guidelines_2017.pdf

⁵ *Justice K.S. Puttaswamy (Retd.) V. Union of India* (2017). Available at: <https://recordoflaw.in/justice-k-s-puttaswamy-ret-d-v-union-of-india-2017/>

⁶ *Kharak Singh v. State of Uttar Pradesh* (1962). Available at: <https://recordoflaw.in/kharak-singh-v-state-of-uttar-pradesh-1962/>

⁷ *Gobind v. State of Madhya Pradesh* (1975). Available at: <https://bnblegal.com/landmark/govind-v-state-madhya-pradesh-anr/>

⁸ *R. Rajagopal v. State of Tamil Nadu* (1994). Available at: <https://recordoflaw.in/r-rajagopal-ors-v-state-of-tamil-nadu-ors/>

sonal liberty. In the same vein, *People's Union for Civil Liberties v. Union of India* (1997)⁹, which considered the issue of telephone tapping, reiterated that any monitoring and interception of an individual's personal communication had to meet constitutional guarantees. All of these cases have helped establish privacy as an emerging constitutional principle tied to personal dignity and liberty (Chatterjee, NS, 2022). Nevertheless, the exact status of the right to privacy under the Constitution remained unclear prior to the landmark case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017).

Justice K.S. Puttaswamy and the Constitutionalization of Informational Privacy

The Supreme Court conclusively settled the constitutional position of privacy in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where a nine-judge bench ruled unanimously that privacy was a fundamental right provided under Part III of the Constitution. In particular, privacy was established as an inseparable constituent part of the concept of "life" and "personal liberty" outlined in Article 21, as a fundamental aspect of individual autonomy. It is significant to note that, according to this decision, informational privacy was officially regarded as an independent constitutional value. As such, people are expected to manage their own personal data with care.

Technological developments, along with the digitization of people's personal information, have led to increased dangers in the sphere of collection, profiling, and surveillance of data. Informational privacy is

necessary to mitigate risks faced by individuals both from states and non-state entities able to exercise excessive power over personal information. It should be pointed out that the normative basis of modern legislation is formed according to data-protection principles of autonomy, self-determination, dignity, and consent. This idea becomes relevant especially while considering the peculiarities of genetic information.

Genetic Privacy as an Extension of Constitutional Privacy Protections

Genetic information is distinct from other personal information due to its lasting nature, predictive potential, and intrinsic familial dimension (Nakta, Dahiya, 2024). Since, unlike other forms of information, genetic information can reveal past and future medical information, familial relationships, ancestral heritage, and inherited characteristics, it involves not only personal but also familial and intergenerational privacy issues. From the standpoint of constitutional law, there are worries about informational autonomy, bodily integrity, dignity, and decision-making liberty in regard to the unlicensed harvesting, use, disclosure, and commercialization of genetic information.

The above-mentioned worries apply specifically to genomic information collections, genomic research, direct-to-consumer testing services, and precision medicine programs. Therefore, the constitutional doctrines of informational, autonomy, and human dignity recognized by the Supreme Court may be interpreted as encompassing genetic information.

⁹ *People's Union for Civil Liberties ... vs Union Of India (Uoi) and Anr.* on 18 December, 1996. Available at: https://indiankanoon.org/doc/31276692/?utm_source=chatgpt.com

Genetic Information and India's Emerging Data Protection Regime

Whereas the constitutional law on privacy constitutes the basis for the protection of genetic data in India, the regulation of personal data protection is governed under statute law. The recent passage into law of the Digital Personal Data Protection Act, 2023, marks a milestone for the regulation of digital personal data in this country. The Act provides a comprehensive legal framework for the collecting, processing, storage, and transmission of personal data. Even though the Act does not make any specific mention of genetic data as a specific kind of personal data, its scope of application to genomic data in various activities such as biomedical research, genetic analysis, personalized medicine, and large-scale genomic databases is clear. For this reason, it becomes crucial to analyze the Digital Personal Data Protection Act in order to establish whether India's present data protection regime can protect genetic data in a world increasingly driven by data and genomic sciences.

Applicability of the Digital Personal Data Protection Act, 2023 to Genetic Information

Personal Data, as per Section 2(t) of the Act, means any data about an individual who can be identified by or from such data. Since genetic data consists of unique biological information that can be used to distinguish between individuals, genomic data falls within the scope of personal data (Hanspal, 2025). This is particularly significant given the growing role of genomics in healthcare, medical research, precision medicine, and direct-to-consumer genetic testing. Genomic datasets are highly sensitive, as they contain information relating to medical conditions,

disease risks, ancestry, and biological relationships.

The application of the DPDP Act to genetic data is therefore important in ensuring that genomic information is collected and processed under legally binding rules. However, the Act adopts a technology-neutral and category-neutral approach. Unlike the European Union's General Data Protection Regulation (GDPR), which expressly recognizes genetic data as a special category of personal data requiring enhanced protection, the DPDP Act does not distinguish genetic information from other forms of personal data (Regulation (EU) 2016/679, Art. 9(1)). Consequently, genomic information remains regulated under the Act's general data protection framework.

Consent and Processing of Genetic Data

The concept of consent is key to the regime created under the Digital Personal Data Protection Act, 2023. Consent must be free, specific, informed, unconditional, and unambiguous. Further, Data Principals should be properly notified about the kinds of personal information to be processed, the purposes of processing, and their rights under the Act. These requirements reflect the principles of informational autonomy and self-determination recognized in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017).

The importance of informed consent is even greater when personal information relates to genetic data. Genetic information is permanent and may reveal not only current health status but also future disease risks and familial relationships.

These characteristics make informed consent particularly challenging. For example, participants in genomic research may consent to the collection of their genetic infor-

mation for a specific project without being aware of subsequent uses, further processing, data sharing, or cross-border transfers. Recent scholarship has therefore emphasized the importance of dynamic consent models capable of adapting to the evolving nature of genomic research. While the inclusion of informed consent provisions in the DPDP Act is an important achievement, their practical application remains controversial.

Obligations of Data Fiduciaries

One of the key provisions of the Digital Personal Data Protection Act, 2023, is a set of data-related rights designed to provide individuals with greater control over their personal information. Under the DPDP Act, the Data Principal has important rights, including the right to obtain information about personal data processing, the right to correction and erasure of personal data, the right to file complaints, and the right to nominate a person to exercise these rights in the event of death or incapacity.

The significance of these rights becomes more pronounced in the case of genomic data. A patient has the right to know how genetic data are collected, processed, and shared by hospitals, research organizations, genetic testing agencies, or biotechnology companies (Dove et al., 2022). The rights to correction and erasure also provide data subjects with a degree of control over their personal information.

Individual rights relating to genomic data are complemented by the duties of Data Fiduciaries. Under the Act, Data Fiduciaries must ensure lawful data processing, provide adequate notice, implement reasonable security measures, and promptly report data breaches. Given the implications of genomic

data for healthcare, insurance, employment, and familial relationships, compliance with these obligations is particularly important.

Together, the rights of Data Principals and the duties of Data Fiduciaries form the legal basis for protecting genetic information in India. Although the Act does not specifically regulate genomic data, its rights-based approach provides an important legal framework for addressing privacy, transparency, accountability, and informational autonomy.

Biomedical Governance and the Regulation of Genomic Research

Though constitutional jurisprudence on the issue of privacy and data protection laws are key legal instruments that help protect genetic information, the governance of genomic information involves other factors that extend beyond privacy laws. The generation, storage, and usage of genetic information takes place within institutions such as biomedical research laboratories, hospitals, genomics databases, and genomics technology projects. Within the Indian context, the governance of genomic research involves not only data protection and ethical guidelines but also various regulations related to clinical research and genomics programs initiated by the government. Consequently, a critical analysis of the regulation of biomedical research and genomic technologies in India becomes necessary.

Ethical Stewardship of Genomic Research Governance

Ethical governance of genomic research in India has been mainly influenced by the National Ethical Guidelines for Biomedical and Health Research Involving Human Participants issued by the Indian Council

of Medical Research (ICMR) in 2017. The Guidelines provide the primary ethical framework for biomedical research involving human participants and have growing relevance to genomic studies, biobanking, and the collection and use of genetic data. Reflecting advances in genomic technologies and data-driven biomedical research, they expanded their scope to cover research involving biological materials, biobanks, datasets, and genomic technologies.

The principle of respect for persons, which lies at the core of the Guidelines, encompasses informed consent, personal autonomy, privacy, confidentiality, and additional protections for vulnerable groups (Indian Council of Medical Research, 2017). In genomic research, informed consent is particularly important because genetic information may affect not only participants but also their biological relatives. Researchers are therefore required to inform participants about the purpose of the study, potential risks and benefits, future use of biological materials, data sharing, and confidentiality measures. The Guidelines also recognize that genetic information may reveal sensitive information about participants, their relatives, and even communities.

An important aspect of the Guidelines is their regulation of biobanks and biological repositories. They establish ethical standards for the collection, storage, transportation, and future use of biological samples and associated data, while emphasizing confidentiality, community participation, benefit sharing, and responsible dissemination of research findings (Balagurunathan, Sethuraman, 2024).

Regulatory Oversight of Gene Therapy and Genetic Innovation

The emergence of gene-editing technologies and gene-based therapies has cre-

ated new opportunities for the treatment of previously intractable genetic disorders. At the same time, these technologies raise complex ethical, scientific, and regulatory issues, including safety, efficacy, long-term health effects, and the potential misuse of genetic interventions. In response, the Indian Council of Medical Research (ICMR), together with the Department of Biotechnology (DBT), published the National Guidelines for Gene Therapy Product Development and Clinical Trials (2019).

The Guidelines establish the regulatory framework for the research, development, evaluation, and clinical application of gene therapy products in India. They cover preclinical research, clinical trials, ethical review, risk assessment, patient safety, and post-trial follow-up.

An important element of the Guidelines is the protection of human participants. Given the potential for irreversible effects of gene therapy, researchers and sponsors must ensure strict compliance with safety standards before clinical application. The Guidelines also distinguish acceptable applications of genetic modification from ethically unacceptable practices, thereby shaping India's regulatory approach to gene therapy.

National Genomics Programs and Architecture of Data Governance

The field of genomics in India has made great progress due the emergence of many genomics projects within the country that seek to promote biomedical research and precision medicine studies. Some of the most important projects are those whose significance in the governance of genomics in India is already widely recognized. For example, the Genome India Project, which seeks to construct a reference genome of India, was able

to gather 20,000 biological samples from 83 communities to achieve the whole-genome sequencing of 10,000 people.

The scientific relevance of such programs lies in their capacity for increasing knowledge of genetic variants among specific populations, improving disease prediction and developing individualized treatment and therapy for patients. In the past, there has been an uneven distribution of people participating in global genomics databases with the result that most data were related to people of European origin only. As a result, there were considerable knowledge gaps about other groups, including those residing in South Asia. Through the establishment of the Genome India Project, scientists will be able to gather genetic information that corresponds to the highly genetically diverse population of India.

Despite their high scientific potential, huge genomic databases raise serious governance issues regarding privacy, confidentiality and data security, including the obtaining of informed consent and data exchange across borders (Barman, Sarmah, 2025). Building large genomic databases requires special governance mechanisms concerning data collection, processing, de-identification, and further analysis. This problem becomes crucial due to the unique and irrevocable nature of genetic information, which may indicate some details about the data subject's biological relatives and offspring. Therefore, any governance of genomic databases should include data protection norms, ethics, and responsibility.

International standards and comparative regulatory approaches

UNESCO International Instruments

The first of these three successive UNESCO documents establishes the framework for

the international norms governing genetic data, each document providing a progressively more detailed articulation of the ethical and legal responsibilities of member states as genome science developed.

The Universal Declaration on the Human Genome and Human Rights (1997) is the first international attempt to control the linkage between genetics and human rights. The Declaration, unanimously adopted by UNESCO's General Conference and endorsed by the United Nations General Assembly in 1998, describes the human genome as "the heritage of humanity". Against this background, it condemned practices which are "contrary to human dignity", such as germ-line interventions and reproductive cloning (UNESCO, 1997, Arts. 1, 11, 24). Most importantly, Article 6 prohibits discrimination on the basis of genetic characteristics, which violates human rights and fundamental freedoms. However, this provision is a normative standard that is yet to be adopted in full by many national legal systems, including India.

The International Declaration on Human Genetic Data, which was unanimously adopted at UNESCO's 32nd General Conference on 16 October 2003, is the most comprehensive international document specifically related to the collection, processing, storage, and use of human genetic data (UNESCO, 2003). The Declaration lays out a number of requirements, including informed consent, confidentiality, data subject access, nondiscrimination, and benefit-sharing, mandating that states ensuring compliance be supervised by independent, multidisciplinary, pluralist ethics committees (UNESCO, 2003, Arts.). 8, 14, 19, 22). The "special status of human genetic data" (1(b) of the article), understood in terms of its particular sensitivity, its potential

to affect other family members and descendants, and its capacity to predict future health states, clearly acknowledges the issues that have been on the agenda of domestic lawmakers (immutability and issues related to family members and descendants). However, unlike the GDPR, the Declaration does not establish individual rights; the fact that the Declaration is a “soft law” instrument does not mean that compliance is a matter of choice, but rather that many member states have yet to implement the Declaration into domestic law (Feeney, 2024).

The Universal Declaration on Bioethics and Human Rights (2005), which broadened the scope of the UNESCO to include biomedical research as a whole, emphasized the importance of human dignity, autonomy, benefit to the individual or the community, and non-maleficence (UNESCO, 2005, Arts. 3–8). While it is less specific to genetic data than the Declaration of 2003 is, it offers interpretive guidance to reading the consent and privacy obligations of all three instruments.

As a Member State of UNESCO, India has political and moral commitments under all three instruments. However, the implementation gap remains significant: the DNA Technology (Use and Application) Regulation Bill, 2019, which failed to become law, did not reference the UNESCO Declaration on Human Genetic Data; there is no mention of it in the Digital Personal Data Protection (DPDP) Act, 2023; and no subsequent legislation has been proposed to domesticate the obligations under the Declaration. This creates a legal lacuna between India’s international obligations and its internal legal framework, which is directly addressed by the recommendations in the article.

European Union

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is the most architecturally complex data protection regime for genetic data that is in effect anywhere today. While it does not purport to be directly applicable to the Indian regulatory context, it serves to provide categories for the regulatory debate, whose lack of representation in India’s Digital Personal Data Protection Act (DPDPA), 2023, is the essence of the present work’s normative critique.

Article 9(1): The Special Category Prohibition

The processing of genetic data, as defined in Article 4(13) 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 and which result, in particular, from an analysis of a biological sample from the natural person concerned,” is subject to a *prima facie* prohibition under Article 9(1). Since this is a general prohibition, processing is only lawful if the controller is able to specify a valid exception under Article 9(2). This default-prohibition structure is superior to that of the DPDPA, which is consent-centric and opt-in, because it places a burden on the data controllers to justify data processing *ex ante*, rather than it being justified if the data principal has not objected.

The ten exceptions in Article 9(2) include explicit consent, vital interests and public health and scientific research. Article 9(2)(j) is the most operationally relevant exception for genetic research, due to its provision allowing processing for “historical, scientific and statistical purposes or for the purpose of the ar-

chiving of information in the public interest”. While the consent framework in the DPDPA (Regulation (EU) 2016/679, Art. 6, 9(2)) requires controllers to establish only a lawful basis, a dual layer analysis is required when it comes to Article 9(2) exception. The dual layer analysis is required for controllers when applying Article 9(2) exception, but not when applying Article 6 on a lawful basis (Peloquin et al., 2026).

Article 89: Research Derogations and Safeguards

Subsequent to this, Article 89 of the GDPR allows member states to derogate from various data subject rights, such as the rights to access, erasure and portability, as long as “appropriate safeguards” are in place (Regulation (EU) 2016/679, Art. 89(1)). The GDPR, which does not contain a prescriptive list of the safeguards, but rather “any safeguards necessary to ensure respect for the principle of data minimization”, includes at least pseudonymization where feasible (Regulation (EU) 2016/679, Art. 89(1)). The resulting uncertainty in regulation has been signaled in the academic literature, as the concept of pseudonymization does not necessarily preclude re-identification; thus, the question of what constitutes “appropriate safeguards” in the context of WGS is a normative one that has not yet been resolved (Dove et al., 2022).

The European Data Protection Board (EDPB) has already issued several guidelines on the issue, the latest being the Guidelines on consent and scientific research, while the 2026 draft Guidelines on the processing of personal data for scientific research purposes followed. The 2026 Guidelines state that broad consent for future research that has not been specified at the time of data

collection may be permissible in cases when the research question cannot be defined at the time of collection with the caveat that this must be carried out within the framework of robust governance accompanied by clear communication with participants (Peloquin et al., 2026). The Guidelines use the term “almost always” when referring to the requirement for a Data Protection Impact Assessment (DPIA) under Article 35 in the context of research using AI, or processing of large genetic datasets (Peloquin et al., 2026). While not binding in India, these EDPB positions represent global best practice suitable for use as a yardstick in India’s DPDPA Act research exemption of Section 17(2)(b).

Article 9(4): Member State Augmentation

Article 9(4) provides member states with the power to “maintain or introduce additional requirements, including limitations, with respect to the processing of genetic data, biometric data or health data”. Some EU member states have already used this power, such as France, where the hosting of health data must be certified, and Germany, where the hosting of health data in an employment context is added. The GDPR’s design, in this case, is therefore a regulatory floor, not a ceiling; a design principle that could be incorporated into India’s genetic research legislation to allow states with large biomedical research ecosystems, such as Tamil Nadu or Maharashtra, to complement a national genetic data protection law.

Institutional Enforcement

Enforcement of GDPR relies on an independent supervisory system, consisting of Data Protection Authorities (DPAs) in each member state working alongside a coordinating

body, the European Data Protection Bureau (EDPB). Violations of Article 9 are to be sanctioned at the higher level, up to EUR 20 million or 4% of global annual turnover, Art. 83(5)). The GDPR is thus a quadripartite system of substantive protection, procedural protection, institutional review and deterrent enforcement, which the Indian DPDP Act only partially emulates.

United States

In the United States, genetic data protection is not addressed in a holistic manner, but rather primarily from an anti-discrimination perspective. In 2008 the Genetic Information Nondiscrimination Act (GINA) was passed, banning the use of genetic information in two particular ways: in health insurance underwriting (Title I) and in employment decisions (Title II) (Genetic Information Nondiscrimination Act, 2008, Pub. L. 110–233).

Scope and Operation

Title I bans health insurance discrimination based on an individual's genetic information in determining eligibility, in setting premiums and in imposing pre-existing condition exclusions. Employers, employment agencies, labor organizations and training programs are prohibited from considering the genetic information of any individual in their hiring, firing, compensation, or establishing terms and conditions of employment. GINA broadens the definition of genetic information to encompass family health history, the manifestation of disease in family members, as well as the genetic tests conducted on a family member, a dimension of genetic data that is not always covered by data protection laws (GINA, 2008 § 201(4)).

Structural Limitations

The sectoral nature of GINA, although innovative when it was enacted in 2008, is seriously flawed and in some ways has restricted the scope of its application as a model for modern Indian legislation. First, GINA explicitly excludes life insurance, disability insurance, and long-term care insurance from its scope; this is particularly important because the Indian insurance industry has not yet engaged in genetic risk profiling, and so is vulnerable to the kind of actuarial discrimination that GINA is supposed to prevent, and which it does permit. Second, GINA includes an exception from the requirement for mandated disclosure for employers who wish to use a “wellness program” to request disclosure of genetic information with written consent (GINA § 202(b)(2)), which critics argue leads to a coercive disclosure environment for employees. Third, GINA, as a single anti-discrimination law, does not mandate that genetic data be collected, stored, or used for secondary purposes functions that are imperfectly provided for by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and, in the case of federally-funded research, by the Common Rule (45 C.F.R. Part 46).

State-Level Supplementation

GINA's inadequacy in addressing the issue at the Federal level has led to a significant amount of state-level legislation. California's Confidentiality of Medical Information Act (CMIA) also provides genetic protections for life insurance and disability insurance, while Illinois' Genetic Information Privacy Act (GIPA) does the same for group life insurance, and several states have laws that provide genetic protections for direct-to-consumer genetic

testing data. While highlighting the need for a unified approach to genetic privacy, this patchwork approach also demonstrates the regulatory burden and overlap in protection that can be created by piecemeal legislative responses, lessons which India should learn to internalize for its own benefit by having a more streamlined federal approach to genetic privacy.

United Kingdom

The UK has built up a genomic data governance ecosystem which is unique in its focus on institutional design, multi-level consent structures, and the co-articulation of research aspirations and public trust. The regulatory architecture is based on the Data Protection Act 2018¹⁰ (incorporating UK GDPR), the Human Tissue Act 2004, and a set of sector-specific ethical governance structures created by NHS England and Genomics England.

The UK Biobank, which was launched in the UK in 2006 as a large-scale biomedical resource of genetic and lifestyle data from 500,000 volunteers, is the world's benchmark for population-level genomic governance. Its ethical architecture is based on three principles: a broad consent framework that is collected at enrolment; an independent Data Access Committee (DAC) that reviews every research proposal in accordance with a standardized set of criteria covering scientific merit, public benefit, and minimization of data; and contractual data sharing agreements that ensure that data are used only for purposes approved by the Data Access Committee, that do not attempt to re-identify participants, and that involve returning

data to UK Biobank at project completion. The DAC model separates the consent process (which is done once at enrolment) from the access process (which is done on a case-by-case basis for each research request), and allows secondary use of genetic data without necessarily asking the participant to re-consent, while still affording independent governance oversight. The "trustee model" of data governance has gained considerable support in the scholarly literature as an alternative to opt-in or opt-out in cases where uses of data for future research are not specified at the time of data collection (Dove et al., 2022).

Genomics England and the 100,000 Genomes Project

The 100,000 Genomes Project was launched by Genomics England in 2012 and completed in 2018, in which 100,000 genomes from National Health Service (NHS) patients with rare diseases and some cancer types were sequenced. The consent structure for the project is tiered; in consenting to their data being used for broad genomic research, individuals participating in the project have the option to allow their data to be used for further research (genomics research that goes beyond clinical care) with the potential to withdraw at any time without impacting clinical care (consent to further research), and the potential to withdraw from the program at any time without impacting clinical care (broad genomic research). There are governance issues over the control of data, particularly with the NHS Genomic Medicine Service (GMS), which was created in 2018 and has since introduced genomic sequencing into clinical pathways. There are

¹⁰ *Data Protection Act 2018*. Available at: <https://www.gov.uk/government/collections/data-protection-act-2018>

governance issues over the control of data – in particular with the NHS Genomic Medicine Service (GMS), launched in 2018, which has integrated genomic sequencing into routine clinical pathways – creating issues of data governance that sit between clinical records (which are governed by the Data Protection Act 2018) and research data (which are governed by the UK GDPR Article 89 derogations). The MHRA and NHS England have worked together to provide guidance on the use of genomic data for both clinical and research purposes, separating each purpose and ensuring that research-purpose processing meets the Article 89 safeguard requirements, which India's institutions (the Indian Council of Medical Research and the Central Drugs Standard Control Organization) have not followed.

Human Tissue Act 2004 and Data Protection Act 2018

In England, Wales and Northern Ireland, the Human Tissue Act 2004¹¹ governs the taking, holding, using, and destroying of human tissue, which includes tissue samples for genetic processing. In providing for a licensing regime for tissue banks, the Act specifies “appropriate consent” for each of the various categories of use (Human Tissue Act, 2004, Sch. 1). Most significantly, the Act provides for enforceable offences for the use of tissues without proper consent, a criminal law safety net which is missing from the Indian framework in which the guidelines of the ICMR are voluntarily enforceable. The Data Protection Act 2018 builds on the UK GDPR with sector-specific provisions, such as Schedule 1, Part 1, which defines “research, public inter-

est, or official functions” as one of the large public interests for processing special category data, which includes genetic information (Data Protection Act 2018, Sch. 1, Part 4).

Comparative analysis

The above analysis of international instruments and comparative jurisdictions leads to the following five structural lessons of immediate relevance for India's legislation.

First, the architecture of Article 9 of GDPR clearly demonstrates that the protection of genetic data requires a special status for the data as a special category, which, by default, should be subject to a prohibition on processing unless specific legal grounds are given. Genetic data (including genomic and proteomic data) should be included in an express special category schedule of the DPDP Act for India, where consent should be especially informed. DPIAs must be conducted before processing, and independent ethics committees must oversee the processing of such data. In the absence of genetic-specific provisions, a general data protection statute leads to compliance fragmentation. Singapore's parallel failure to set up a special category framework under the PDPA, and the reliance on the HBRA as a gap-filling mechanism, is a good illustration of this argument.

Second, Indian law contains no provisions comparable to those of GINA, creating a significant normative gap. An “India-GINA” that extends protection to health insurance, life insurance, and employment, while addressing GINA's limitations regarding long-term care insurance and disability insurance, would facilitate the domestic implemen-

¹¹ *the Human Tissue Act 2004*. Available at: <https://www.legislation.gov.uk/ukpga/2004/30/part/1>

tation of the non-discrimination principles enshrined in the UNESCO Declaration on Human Genetic Data (2003) and the equality guarantees implicit in the Puttaswamy proportionality framework.

Third, the HBRA biobank governance model that features mandatory IRB approval, statutory licensing of tissue banks, independent data access committees, technical access controls and a prohibition on re-identification offers an operational institutional blueprint to India's proposed National Biobank and Genomic Data Regulatory Authority. The current governance mechanism of the GenomeIndia Project, which rests on voluntary ICMR guidelines and involves no statutory obligations, is clearly inadequate.

Fourth, the combination of the UK Biobank DAC model and the NPM governance architecture in Singapore¹² provides an example of a broad consent collected at enrolment that can be aligned with responsible secondary use through independent access oversight by criteria. The prospective nature of longitudinal genomic research is not captured by the consent framework established in India, which is based on the requirement for "free, specific, informed, unconditional, and unambiguous" consent in the DPDP Act, and thus should be supplemented by dynamic consent mechanisms proposed in the recommendations set forth in this article.

Fifth, the successive instruments of UNESCO show that the international community has been aware of the particular dangers of genetic data since 1997, almost 30 years

before the enactment of the DPDP Act. India's continued failure to implement the principles of the Declaration through dedicated legislation does not just imply a lack of legal formality; rather, it has also been a regulatory stance that has favored the scientific utilization of the immense genetic diversity of India over the legal protection of the people who represent India's diversity.

Key Legal and Ethical Challenges

Informed Consent

While consent lies at the heart of data protection law, its application to genetic data exposes fundamental conceptual inadequacies in India's existing framework. The Digital Personal Data Protection Act, 2023 (hereinafter "DPDP Act") defines valid consent as "free, specific, informed, unconditional, and unambiguous" (Digital Personal Data Protection Act, 2023, s. 6). This formulation, borrowed largely from the GDPR, does not really fit the research context. A person who agrees to have their genome sequenced to study heart disease cannot really anticipate that the same data might be used later for pharmacogenomic drug trials, ancestry profiling, or machine learning-based disease prediction, applications that are not merely unforeseen, but may not yet exist at the time of consent (Tavani, 2004). The problem that emerges here is not so much to do with the process itself as with how we think about it: informed consent assumes we can know and tell people about uses of their data. In practice, genomic research often makes this impossible.

¹² Agency for Science, Technology and Research. *National Precision Medicine (NPM) programme*. Genome Institute of Singapore. Available at: <https://www.a-star.edu.sg/gis/our-science/precision-medicine-and-population-genomics/npm>

The traditional way of getting consent for an event is not compatible with biobank research that goes on for decades and uses genetic samples many times (Kaye, 2012). The Indian Council of Medical Research (ICMR) National Ethical Guidelines for Biomedical and Health Research (2017) partially acknowledge this by introducing “broad consent” as a mechanism for biobank research which permits consent for an undefined range of future research within a specified domain (Indian Council of Medical Research [ICMR], 2017). The broad consent model, then, represents a compromise arising from the conflicting demands of ethics review boards, which often prefer case-by-case consent, and the practical need for the long-term access to data afforded by large-scale population genomics, for which continuous re-consent is scientifically impractical (Knoppers, 2010). The problems inherent in this broad consent model in terms of the solution it presents to the aforementioned tension may allow it to act less as an affirmation of autonomy and more as a *carte blanche* waiver of individual rights, especially when the subject is lacking the necessary scientific and digital literacy skills with which to fully comprehend the implications of broad consent (Tavani, 2004).

Responding to exactly these problems, the more complex system of dynamic consent has arisen. Dynamic consent systems enable research subjects to maintain and update their preferences regarding the use of their data using digital interfaces, receiving information about new uses as they become available, and potentially withdrawing their consent for some projects, while remaining a participant in others (Kaye, 2012). An appropriate response to the crisis of governance

in genomics will not be to make modifications to existing frameworks of consent, but rather to develop a system of “e-governance” that includes technological tools to facilitate compliance together with legally robust forms of accountability designed to operate on the global scale at which genomics data is increasingly being shared.

The DPDP Act contains no such provisions as dynamic consent, while the DPDP Rules, 2025 do not establish it even for any category of sensitive data. The lack of it is of particular concern given India’s stated goals under the GenomeIndia Project, which seeks to sequence 10,000 Indian genomes to conduct population level research.

A survey of 10,881 adults in Japan found that individuals expected much higher protections in place if their genetic and clinical data were to be shared along with their family members’ data than if it was only individual data sharing (Takashima et al., 2018). The study is based on an intuitive, yet complex, concept: genetic data has inherent familial privacy implications. That is, the sequencing of one person’s genome simultaneously provides probabilistic health data, familial information, and lineage information about the biological relatives of the individual sequenced, who may have not given their consent to any research involvement (Navied et al., 2015). The Indian approach is ill-equipped for the problem, in that it does not even acknowledge genetic data as a unique, sensitive category under the DPDP Act.

Specific threats associated with the challenge of re-identification include attacks via pseudo-anonymized sequences, attacks exploiting phenotype inference via aggregated GWAS data, and “kin privacy breaches” in which a shared genome of a non-consent-

ing relative is reconstructible through linkage disequilibrium given the genome of a relative. Such attacks are not just speculative. Gymrek et al. (2013) found they could re-identify individuals through supposedly anonymized genomic datasets by using the relationship between Y-chromosome markers and genealogical databases. The consequences of this finding for India are clear. If anonymized genomic data cannot be safely de-identified, then a framework like that set out in the DPDP Act, which specifically excludes anonymized data from its ambit as “personal data”, will be of little value to researchers – and more importantly to individuals – conducting genetic research.

Lastly, although the DPDP Act states an individual has the right to withdraw consent (s6(4)) once their genetic data has become a part of a combined data set, has been fed through training a computational model, or been given to an international research consortium, it may be impossible for them to achieve that right. Ensuring that an individual is completely withdrawn from research is one of three problems, the other two being ensuring anonymity and providing sufficient information for the informed consent process. That the withdrawal of one family member's data from a familial study may weaken the scientific utility of the dataset may produce institutional pressure not to withdraw. The DPDP Act lacks a provision to deal with withdrawal in situations such as these; moreover, there is no provision for redress if withdrawal is impossible.

Storage, Retention, and Security of Genetic Information

A general duty not to retain personal data longer than is necessary for its purpose of processing has been imposed upon data

fiduciaries by the DPDP Act (s. 8(7)). No time limit for storage of genetic data is defined in the DPDP Act, while the DPDP Rules, 2025, contain no sector-specific clauses for genomic datasets, a situation contrary to the position under the GDPR, which has dedicated guidance by the European Data Protection Board on storage limitation in the context of special category data, including genetic data.

This lack of statutory limits for data retention in the context of genetic data is made more acute due to the fact that a genomic dataset is permanent and perpetually of growing value. This factor is not adequately captured by general principles of data minimization. Indeed, as Naveed et al. (2015) observe, one of the six unique features of genomic data is that its information value never declines; unlike blood pressure or glucose readings, a genomic dataset archived for fifty years holds the same information value in relation to health predisposition, kinship, or heritage as when it was created (Naveed et al., 2015). Permanence is not merely a fact; it is a matter for the law: a legal framework treating the storage period of a genomic dataset no differently from a transactional one demonstrates a fundamental problem in terms of understanding the specific nature of the data.

The prospectivity of genetic data – represented by its capacity to yield previously unknowable information as science advances – means its retention does not necessarily pose diminishing, but ever-increasing risks, about which no provision of the DPDP Act or the DPDP Rules, 2025, makes any mention.

Compounding these risks, there are no legally mandated minimum-security standards for genetic data at Indian biobanks and

genomic research institutions. While data fiduciaries designated Significant Data Fiduciaries are required to appoint DPOs and conduct DPIAs under the DPDP Act (s.10), these criteria were widely defined and discretionary, and it is questionable whether a majority of genomic research institutions will qualify on mere volume alone. The DPDP Rules, 2025 are not clearer in this regard.

Beyond issues of data security during retention and transfer, the technical limitations of anonymization additionally compromise the security of stored genetic data. It has been proven empirically that genetic data is re-identifiable after purportedly anonymization by comparing anonymized sequences to publicly available genealogical data and general demographic information (Gymrek et al., 2013). This has a direct legal consequence, which Indian law does not reflect; indeed, genetic data cannot be fully anonymized, since, unlike other medical data, it is a unique marker pointing to a single individual. Claiming that anonymized genetic data falls outside the scope of data protection law is therefore scientifically demonstrably false; nevertheless, the definitions of personal data and anonymization in the DPDP Act ignore this. No provision requires data fiduciaries to attempt adversarial re-identification testing prior to publishing research datasets.

This leads into a deeper problem with regard to the GDPR's right of erasure: the possibility coexisting under the GDPR's special category protections of processing genetic data for scientific research purposes and the existence of indefinite deletion rights means that legal reasoning cannot find a way forward on balancing the two. Where the GDPR's system is struggling to find adequate legal pathways to balance these rights and inter-

ests through the complex interplay of special category data, derogations for scientific research (Art. 89(1)), and guidance from supervisory authorities, the Indian framework, which does not even recognize genetic data as a distinct special category of personal data, struggles at a much more fundamental level. The missing safeguards of data retention period, security standards, and a scientifically based anonymization doctrine need specific legislative action, not the application of general DPDP Act principles.

Genetic Discrimination

Of all the challenges identified in this article, the absence of any anti-discrimination framework for genetic data is perhaps the most consequential regulatory failure in India's current legal landscape.

Employment and Insurance Discrimination

No Indian law, in the context of employment, prohibits an employer from asking for the genetic information of a job applicant or from using a candidate's genetic predisposition for a disease to make hiring/firing/promotion decisions. The lack of a comprehensive regulatory framework to address the issues surrounding genetic discrimination is all the more apparent in light of legislative approaches that more mature jurisdictions have adopted. The Genetic Information Non-Discrimination Act (GINA) in the United States prohibits employers from using genetic information in employment decisions under Title II, along with a prohibition on health insurers from using genetic information for underwriting under Title I (Genetic Information Non-Discrimination Act, 42 U.S.C. 2000ff, 2008). Canadian legislation criminal-

izes the compelling of genetic test disclosure as a pre-condition for receiving services or goods (Genetic Non-Discrimination Act, 2017) with criminal penalties reaching C\$1 million or 12 months imprisonment (Joly et al., 2020). The European Union's General Data Protection Regulation prohibits the processing of genetic data unless specific conditions are met, including explicit consent, while the Council of Europe's Recommendation CM/Rec(2016)8 forbids insurers from demanding genetic tests or from providing cover based on disclosure of prior test results (Joly et al., 2020). No equivalent Indian statute or legislative measure exists to prevent either occupational or insurance genetic discrimination.

The clear danger this lack of protection creates is not hypothetical. Joly et al. (2020) note that the first instances of genetic discrimination, which occurred within the health insurance and employment sectors, include discrimination on the basis of the sickle-cell trait status among potential insurance/job applicants; moreover, in North America and Europe, the passage of decades of multiple legislative enactments has only led to partial protection. As direct-to-consumer genetic tests become more popular in the Indian market and the results of research from biobanks are more extensively used by actuaries, insurers and employers will obtain ever-increasing power to profile citizens genetically without any legislative constraints. The Insurance Regulatory and Development Authority of India has not introduced any binding guidelines with regard to the usage of genetic information for insurance underwriting, while the DPDP Act makes no specific prohibition of the discriminatory use of sensitive personal information in the insurance or employment sectors.

Existing Indian constitutional law offers some—albeit inadequate—protection. Article 14 (right to equality) and Article 15 (prohibition of discrimination) of the Indian Constitution applies to State action and not generally to private parties. Additionally, genetic predisposition is not a recognized classification of discrimination under the constitutional framework. While a 2018 decision by the Delhi High Court established that insurance policies cannot exclude coverage for genetic disorders (*M/S United India Insurance v. Jai Parkash Tayal*, RFA 610/2016, 2018, grounded on a right to health argument derived from Articles 14 and 21 of the Constitution), this judgment was ultimately limited by the Supreme Court to public sector employees (*M/S United India Insurance Co. V. Jai Prakash Tayal*, SLP 29590/2018, 2018). As Joly et al. (2020) highlight in their global survey of genetic discrimination legislation: “Reliance on general privacy, disability or anti-discrimination principles is always likely to create patchy and incomplete protections since such general principles were not drafted to cater to the specific risk profiles posed by genetic information”.

Joly et al. (2020) demonstrate that the piecemeal approach to genetic discrimination in many jurisdictions has failed to offer robust protection even in the sectors of insurance (particularly long-term care and life insurance) and employment, noting that it has failed to address various types of discriminatory practices. In India, not even such an indirect form of protection exists. This legislative void allows for the expanding clinical and commercial use of genomic data to proceed in the absence of adequate legal mechanisms to protect individuals from discrimination based on it in two crucial sectors: insurance and employment.

Law Enforcement and the Criminal Justice System

The DNA Technology (Use and Application) Regulation Bill, 2019, which lapsed without being legislated, envisaged the creation of National and Regional DNA Data Banks where indices on “crime scene,” “suspects,” “undertrials,” “missing persons,” and “volunteers” would be stored (Clause 25). In particular, the notion of an index on “suspects,” allowing for the storage of DNA profiles of individuals not convicted of an offense, constituted a serious constitutional concern under Articles 20 and 21 of the Constitution, transgressing both the right against self-incrimination and the right to privacy identified in Puttaswamy.

The most structurally troubling is the possibility of familial DNA searches; a process by which law enforcement agents use DNA at the crime scene not to match the profile exactly but partially with a database so as to find a biological relative to the actual offender. This technique, which has been used extensively in many jurisdictions, has faced much criticism for their disproportional impact on ethnic and racial minorities, whose profiles disproportionately feature in forensic databases (Greely et al., 2006). In the Indian context, where caste and tribal identities correlate with specific genetic markers, such familial DNA searches in the absence of a regulatory framework carried the high risk of genetically reinforcing caste-based surveillance.

Cross-Border Transfer of Genomic Data and Data Sovereignty

The DPDP Act will allow free and easy transfer of data internationally through whitelisting, with the Central Government be-

ing held responsible for notifying to which countries personal data may be transferred (Section 16). The issue with the whitelisting mechanism is that no parameters exist to govern the whitelisting of countries, nor is there any indication within the DPDP Rules, 2025, concerning how they should provide effect to the provisions of Section 16 and its complexities relating to sensitive genomic data.

The potential threat of genomic data being used to jeopardize national security should not be underestimated. India’s vast and genetically diverse population comprising over a thousand endogamous groups and sub-populations represent a scientific resource of great strategic significance. Unfettered access by foreign entities to Indian genomic data en masse could theoretically lead to the development of drugs targeting certain ethnicities, biological weapons targeting certain gene compositions, or espionage conducted using the data from surveillance of the population’s genetic profiles. Fortunately, this aspect has not been overlooked. China’s Human Genetic Resources Administration Regulations (2023) adopt precisely the opposite approach, placing tight controls on exports of human genetic resources data, and requiring governmental authorization for international transfer of such data (Ministry of Science and Technology of China, 2023). The Indian legislation has not erected similar safeguards.

The contradiction between open science, which highly advocates unfettered access to and transfer of genomic data for international research, and the concept of data sovereignty does indeed appear to pose an intractable issue for Indian legislation. A compromise, which, unlike China’s overly restrictive policy, has already attracted crit-

icism for impeding scientific collaboration, can be achieved by introducing data protection impact assessments prior to the international transfer of genomic data, permitting the conditional rather than outright approval of the transfer, and enacting binding data governance agreements between international research institutions. However, none of these provisions were included in the current Indian legislation.

Emerging Issues: AI, Algorithmic bias and predictive genomics

The integration of ML and AI into genomic research have thrown up qualitatively new legal and ethical challenges, which the current Indian law is inadequately prepared to meet.

The use of polygenic risk scores (PRS) – statistical models which combine multiple thousands of genetic markers into a single value predicting risk for complex traits such as IQ, educational outcomes, cardiovascular disease or psychiatric conditions – is already widespread in clinical and commercial contexts (Khera et al., 2018). Their application in insurance underwriting, employment profiling, and education selection represents an unprecedented form of discriminatory prediction, since it predicts what individuals will likely do and experience based on what their genomes say and not on the consequences of their past actions. However, India has so far failed to provide any framework to regulate their use.

The issues surrounding algorithmic bias are acutely relevant to India. Most PRS models were trained primarily on data collected from Caucasians, the majority ethnic group that constitutes the bulk of genome data repositories worldwide (Martin et al., 2019). When applied to Indian populations with their

uniquely diverse genetic background, which has evolved over thousands of years of endogamy and population stratification, it generates discriminatory predictions. This does not provide evidence of malicious intent, but does indicate a structurally ingrained flaw in the data training mechanism that is prone to making prejudiced classifications. The DPDP act does not currently include any provision mandating algorithmic audits for genomic AI applications in India, let alone any other sector-specific legislation for that purpose.

A different type of legal problem arises in the form of the advent of genome editing tools such as the CRISPR-Cas9 and other similar technologies. Such technologies clearly go beyond the boundaries of data protection to enter into the realm of transgenerational rights. Germline editing, which involves making heritable genetic alterations to an embryo, thus infringes on the genetic privacy and autonomy of individuals who, since they do not yet exist, cannot consent to these changes. Indian legislation currently has no specific rules about germline modifications, the transmission of changes to later generations or the rights of children with genetically edited genomes. This legislative vacuum, however, will not remain tenable with advances in the field.

Discussion

Genetic Privacy as a Fundamental Concern

The growth of genomic research has created a tension between scientific advancement and privacy protection. Genetic information is fundamentally different from ordinary personal data because it cannot be changed or replaced once exposed. A breach may create lifelong consequences and affect multiple generations.

Adequacy of the DPDP Act, 2023

The DPDP Act represents an important step towards protecting personal data in India. However, the Act, which was designed as a general data protection law, does not contain provisions specifically tailored to genetic information. As a result, issues such as genomic profiling, hereditary information, genetic discrimination, and familial consent remain inadequately addressed.

Problems with De-Identification

The assumption that removing personal identifiers is sufficient to protect privacy has become increasingly questionable. Scientific evidence demonstrates that DNA data can often be re-linked to individuals through advanced computational techniques. Therefore, traditional anonymization methods cannot fully protect genetic information.

Risk of Genetic Discrimination

One of the most significant legal concerns is the possibility that employers, insurers, or other organizations may use genetic information to make decisions regarding employment, insurance coverage, or financial benefits. Such practices can create unfair disadvantages for individuals, who merely possess a genetic predisposition to certain medical conditions.

Community and Cultural Implications

India's unique demographic structure introduces additional concerns. Publication of genetic information associated with specific communities may reinforce stereotypes, encourage social stigma, or lead to discrimination against vulnerable groups. Existing consent mechanisms, which focus primarily on individuals, do not adequately consider collective privacy interests.

India-Russia Cooperation and Data Sovereignty

India and Russia share a common commitment to protecting sensitive biological information. Their legal frameworks prioritize data localization and sovereign control over genetic resources. While this approach enhances security, it also creates barriers to international scientific cooperation. Therefore, innovative technological solutions are necessary for balancing privacy with research objectives.

Importance of Privacy-Enhancing Technologies

Federated learning, differential privacy, and secure computation techniques provide an effective middle path. These methods allow researchers to generate valuable insights while ensuring that raw genetic information remains within national borders. Such technologies may become central to future international genomic research frameworks.

The Conflict between state sovereignty and international collaboration

The tightening legal landscapes in India and Russia reveal a growing tension between national data sovereignty and international scientific advancement. While India relies on the generalized, consent-driven architecture of the DPDP Act 2023, Russia treats genomic data as a strict matter of national security, governed by Federal Law No. 24-FZ On State Genomic Registration, as well as rigid data localization mandates under Federal Law No. 152-FZ. Furthermore, executive initiatives like Russia's Federal Research Programme for Genetic Technologies (Presidential Decree No. 680) provide a direct sovereign parallel to the Genome India Project,

demonstrating how both nations map their populations' DNA under entirely separate administrative structures.

This hyper-focus on national oversight exposes a shared legal gap: both countries heavily prioritize state sovereignty and biosecurity over individual civil protections against genetic discrimination. Consequently, these strict data borders create severe legislative bottlenecks for international partnerships, as raw genomic data can no longer be legally or physically shared across borders. This institutional friction provides a powerful legal justification for moving away from legacy data-transfer models and shifting aggressively toward decentralized, privacy-preserving technologies.

Recommendations

Enact a Dedicated Genetic Data Protection Law

India should introduce specialized legislation specifically regulating the collection, storage, processing, sharing, and deletion of genetic information. Such legislation should supplement the DPDP Act and address the unique characteristics of genomic data.

Introduce a Genetic Non-Discrimination Act

A separate law should prohibit employers, insurance companies, educational institutions, and financial organizations from using genetic information to discriminate against individuals. This would strengthen constitutional guarantees of equality and dignity.

Establish Community-Level Consent Mechanisms

For research involving tribal populations, indigenous groups, or genetically distinct communities, ethical approval should in-

clude community consultation and collective consent mechanisms in addition to individual consent.

Strengthen Biobank Governance

National biobanks and genomic repositories should adopt advanced cybersecurity measures, regular audits, encryption standards, and transparent accountability mechanisms to prevent unauthorized access.

Promote Synthetic Data Models

Researchers should be encouraged to use synthetic datasets that replicate statistical patterns without exposing real individuals' genetic information. This would significantly reduce privacy risks while supporting scientific research.

Create Specialized Regulatory Authorities

A dedicated genetic data protection authority should be established to monitor compliance, investigate breaches, and formulate sector-specific guidelines.

Encourage Privacy-Enhancing Technologies

Government agencies should actively promote federated learning, local differential privacy, and secure multi-party computation as standard practices for genomic research.

Strengthen India-Russia Research Agreements

Future bilateral agreements should mandate secure technological frameworks rather than unrestricted data sharing. Research collaborations should rely on federated systems that allow joint analysis while preserving national sovereignty.

Implement Joint Regulatory Audits

Compliance with privacy standards and prevent misuse of genetic information.

Increase Public Awareness

Citizens should be educated about the risks and benefits of genetic testing, informed consent, and privacy rights. Public awareness is essential for responsible participation in genomic research.

Conclusion

With the fast-paced progress currently taking place in genomics and genetic engineering, immense opportunities are presented in scientific development and medical care. Nevertheless, the accumulation of genetic material creates various legal and ethical implications surrounding privacy, informed consent, data protection, discrimination,

and data flows across borders. Considering the specific characteristics of genetic data, such as the sensitivity, predictability, and familiarity of the data, existing legal instruments to protect individuals' personal data may prove insufficient.

As illustrated by the above analysis, genetic information is currently subject to constitutional protections and legislation in India, specifically the Digital Personal Data Protection Act of 2023, as well as sector-specific biomedical regulations and guidelines. However, the existing mechanisms fail to consider the special nature of genomics. Genetic information poses distinct legal issues that cannot be fully addressed by the existing legal frameworks. In light of these findings, there is a necessity to establish a separate framework that will acknowledge the peculiarities of genetic data.

REFERENCES

- Balagurunathan, Y., Sethuraman, R.R. (2024). An analysis of ethics-based foundation and regulatory issues for genomic data privacy. *Journal of the Institution of Engineers (India): Series B*, 105(4), 1097–1107. <https://doi.org/10.1007/s40031-024-01058-3>
- Barman, B., Sarmah, S. (2025, February). Data Privacy and Security in Healthcare Systems Using Blockchain: A Review. In: *2025 3rd International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC)* (pp. 213–218). IEEE. <https://doi.org/10.1109/isacc65211.2025.10969312>
- Chatterjee, S., Sreenivasulu, N.S. (2022). Artificial intelligence and human rights: a comprehensive study from Indian legal and policy perspective. *International Journal of Law and Management*, 64(1), 110–134. <https://doi.org/10.1108/IJLMA-02-2021-0049>
- Staunton, C., Slokenberga, S., Parziale, A., Mascalzoni, D. (2022). Appropriate safeguards and Article 89 of the GDPR: Considerations for biobank, databank and genetic research. *Front. Genet*, 13, 719317. [10.3389/fgene.2022.719317](https://doi.org/10.3389/fgene.2022.719317)
- Erlich, Y., Shor, T., Pe'er, I., Carmi, S. (2018). Identity inference of genomic data using long-range familial searches. *Science*, 362(6415), 690–694. <https://doi.org/10.1126/science.aau4832>
- Feeney, O. (2024). Catching the next wave? The relationship between UNESCO and developments in genomics. *European Journal of Human Genetics*, 32, 605–606. <https://doi.org/10.1038/s41431-024-01621-y>
- Gymrek, M., McGuire, A.L., Golan, D., Halperin, E., Erlich, Y. (2013). Identifying personal genomes by surname inference. *Science*, 339(6117), 321–324. <https://doi.org/10.1126/science.1229566>

- Hanspal, M.S. (2025). The Digital Personal Data Protection Act, 2023: Key Provisions, Issues, and Future Directions. *Journal of Law*, 6(2), 12–23. <https://doi.org/10.53361/dmejl.v6i02.02>
- Indian Council of Medical Research. (2017). *National Ethical Guidelines for Biomedical and Health Research Involving Human Subjects*. Chapter 7. ICMR.
- Joly, Y., Dupras, C., Pinkesz, M., Tovino, S.A., Rothstein, M.A. (2020). Looking beyond GINA: policy approaches to address genetic discrimination. *Annual Review of Genomics and Human Genetics*, 21(1), 491–507. <https://doi.org/10.1146/annurev-genom-111119-011436>
- Kaye, J. (2012). The tension between data sharing and the protection of privacy in genomics research. *Annual Review of Genomics and Human Genetics*, 13(1), 415–431. <https://doi.org/10.1146/annurev-genom-082410-101454>
- Knoppers, B.M. (2010). Consent to “personal” genomics and privacy. *The EMBO Reports*, 11(6), 416–419. <https://doi.org/10.1038/embor.2010.69>
- Knoppers, B.M., Harris, J.R., Budin-Ljøsne, I., Dove, E.S. (2014). A human rights approach to an international code of conduct for genomic and clinical data sharing. *Human Genetics*, 133(7), 895–903. <https://doi.org/10.1007/s00439-014-1432-6>
- Nakta, V., Dahiya, S. (2024). Genetic jurisprudence: reimagining Indian legal system's approach to DNA evidence and privacy protections. *Panjab University Law Review*, 63(1), 130–146. <https://pulr.puchd.ac.in/index.php/pulr/article/view/280>
- Naveed, M., Ayday, E., Clayton, E.W., Fellay, J., Gunter, C.A., Hubaux, J.P., ... Wang, X. (2015). Privacy in the genomic era. *ACM Computing Surveys (CSUR)*, 48(1), 1–44. <https://doi.org/10.1145/2767007>
- Peloquin, D., Machin, E., Aurelius, L. (2026, April 24). The European Data Protection Board releases new guidelines on the processing of personal data for scientific research. *Ropes & Gray LLP*. Available at: <https://www.ropesgray.com/en/insights/alerts/2026/04/the-european-data-protection-board-releases-new-guidelines-on-the-processing-of-personal-data>
- Phillips, A., Borry, P., Van Hoyweghen, I., Vears, D.F. (2021). Disclosure of genetic information to family members: a systematic review of normative documents. *Genetics in Medicine*, 23(11), 2038–2046. <https://doi.org/10.1038/s41436-021-01248-0>
- Solove, D.J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564. <https://doi.org/10.2307/40041279>
- Tabor, H.K., Berkman, B.E., Hull, S.C., Bamshad, M.J. (2011). Genomics really gets personal: how exome and whole genome sequencing challenge the ethical framework of human genetics research. *American Journal of Medical Genetics Part A*, 155(12), 2916–2924. <https://doi.org/10.1002/ajmg.a.34357>
- Takashima, K., Maru, Y., Mori, S., Mano, H., Noda, T., Muto, K. (2018). Ethical concerns on sharing genomic data including patients' family members. *BMC Medical Ethics*, 19(1), 61. <https://doi.org/10.1186/s12910-018-0310-5>
- Tavani, H.T. (2004). Genomic research and data-mining technology: Implications for personal privacy and informed consent. *Ethics and Information Technology*, 6(1), 15–28. <https://doi.org/10.1023/B:ETIN.0000036156.77169.31>
- UNESCO. (1997). *Universal Declaration on the Human Genome and Human Rights*. UNESCO General Conference, 29th Session. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000110220>
- UNESCO. (2003). *International Declaration on Human Genetic Data*. UNESCO General Conference, 32nd Session (32 C/Res 22). Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000136112>
- UNESCO. (2005). *Universal Declaration on Bioethics and Human Rights*. UNESCO General Conference, 33rd Session. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000146180>
- Wang, T., Liu, L. (2009). From Data Privacy to Location Privacy. In: *Machine Learning in Cyber Trust* (pp. 217–246). Springer, Boston, MA. https://doi.org/10.1007/978-0-387-88735-7_9

Nitesh Mehra

Genetic Privacy and Data Protection in India:

Emerging Legal Challenges in the Age of Genomic Research

INFORMATION ABOUT THE AUTHOR:

Nitesh Mehra, Advocate Member Executive, Delhi High Court Bar Association (DHCBA)
NMA Law Offices, New Delhi, India

СВЕДЕНИЯ ОБ АВТОРЕ:

Нитеш Мехра, адвокат, член исполнительного комитета Ассоциации адвокатов Высокого суда Дели (ДНСВА), юридическая фирма NMA, Нью-Дели, Индия