Journal of Advances in Developmental Research (IJAIDR)
E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Genomes, Consent, and the Law: Navigating the DPDP Act, 2023 and Global Standards

Dr. Subholaxmi Mukherjee

Assistant Professor of Law, ICFAI University, Tripura

Abstract

The rapid advancement of genomic technologies has ushered in an era where personal genetic information is both a key to medical innovation and a source of profound privacy and ethical challenges. Unlike conventional personal data, genomic data is immutable, predictive, and relational, implicating not only the individual but also families, communities, and populations. India's **Digital Personal Data Protection Act (DPDP Act), 2023** represents a milestone in the regulation of personal data, yet its **single-tier, individual-centric framework** is insufficient for the complexities of genomic information. This article critically examines the nature of genomic data, explores the limitations of the DPDP Act in the context of genetic privacy, and compares global standards from the European Union, the United States, UNESCO, OECD, and selected Asia-Pacific jurisdictions. Through a multidisciplinary lens, encompassing ethical, legal, technological, and social considerations, the study identifies the challenges in genomic governance and offers detailed policy recommendations. These include recognizing genomic data as sensitive, implementing tiered and relational consent, strengthening research oversight, safeguarding minors, ensuring equitable access, and protecting bio-sovereignty. Aligning India's framework with global best practices while contextualizing for national realities is essential for **ethical, secure, and socially responsible management of genomic data**.

Keywords: Genomic Data, Digital Personal Data Protection Act 2023, Consent, Genetic Privacy, Relational Privacy, Bioethics, Data Protection, Global Standards, Biosecurity, Tiered Consent

1. Introduction

Why Genomic Data Requires a New Legal Language

Genomic data is not merely another category of personal information. It is the biological script of human identity and kinship. Unlike passwords or demographic details, genetic data:

- **Cannot be changed.**
- **Is inherently shared with blood relatives.**
- **Predicts future health outcomes.**
- **Reveals ancestral, ethnic, and population-level traits.**
- **Creates possibilities for discrimination, stigmatization, and surveillance.**

In the last decade, the global genomic ecosystem has transformed. Genome sequencing costs have dropped exponentially; AI-assisted genome interpretation is now routine; and commercial companies such as 23and Me, Ancestry DNA, and Indian genetic-wellness startups collect millions of profiles. Governments

too have invested in large-scale genomic databases—such as India's Genome India Project, the UAE Emirati Genome Programme, the UK Biobank, and China's population-scale sequencing initiatives.

With large pools of genomic data now feeding health research, pharmacogenomics, forensic systems, and predictive algorithms, legal scholars have begun to ask a pressing question:

Are existing data-protection statutes equipped to regulate genomic data?

The DPDP Act, 2023 is India's first cross-sectoral data-protection law. Unlike GDPR, it does not single out genetic data or any other "sensitive personal data." All personal data—whether trivial or deeply sensitive—is treated equally except in areas where the government issues exemptions. This raises difficult questions:

- Should genomic data be treated the same as email addresses?
- Is consent meaningful when individuals cannot foresee downstream uses of genetic information?
- Can genetic data collected from one person be used without consent of biological relatives?
- Should India allow cross-border transfers of genomic data to jurisdictions with weaker privacy protections?

These questions cannot be answered without understanding genomic data's special nature. This article argues that genetic information requires **enhanced, relational, contextual, and ongoing consent**, not merely one-time approval. It must be protected by a regulatory ecosystem that recognizes its collective and predictive qualities.

2. The Nature of Genomic Data: Beyond Individual Privacy

Genomic data represents one of the most intimate and sensitive categories of personal information known to modern science. Unlike conventional data, which often reflects past actions or choices, genomic data is inherently predictive, relational, and immutable. Its unique characteristics challenge traditional privacy frameworks and demand a rethinking of consent, control, and governance.

2.1 Genomic Data as Immutable, Predictive, and Shared

Conventional personal data—such as browsing history, location logs, medical records, or retail purchase patterns—is largely reactive. It describes what has already occurred or been recorded. Genomic data, in stark contrast, is inherently **prospective**: it offers insights not only into an individual's current state of health but also into potential future conditions and susceptibilities. For instance, a single genome sequence can indicate predispositions to diseases such as breast cancer (BRCA1/BRCA2 mutations), Huntington's disease, Alzheimer's, or various metabolic and autoimmune disorders—often **long before any symptoms manifest**.

Beyond its predictive power, genomic data is **fundamentally shared**. Each individual's genome contains genetic information inherited from parents and passed on to offspring. Consequently, analyzing one person's genome inherently reveals information about close relatives, creating a **network of privacy implications** that extends beyond the individual. Consider these dimensions:

- **Familial Implications:** A woman undergoing genomic testing may uncover BRCA1 mutations, inadvertently revealing her father's and siblings' elevated cancer risks, even if they did not consent. Similarly, a child's genome provides a partial blueprint of both parents' genetic makeup.
- **Ancestral and Population Information:** Genomic data links individuals to ethnic groups, subpopulations, and geographic ancestry, sometimes revealing sensitive information about communities at large. For instance, certain variants associated with disease prevalence may be overrepresented in specific tribes or communities.

- **Biometric Identification:** Every human genome is effectively a unique identifier. Unlike passwords, email IDs, or national identification numbers, a genome is immutable and cannot be changed if compromised. This permanence amplifies the stakes for privacy breaches.
- **Predictive and Permanent Nature:** Genetic information persists for life. While conventional personal data can often be altered, anonymized, or deleted, the genome is a permanent biological record with implications for identity, health, and familial privacy.

This combination of **immutability, shared ownership, predictive capacity, and permanence** places genomic data at the intersection of multiple rights and societal interests. Its use implicates:

- **Individual privacy**, by revealing intimate health and behavioral information;
- **Familial privacy**, as genetic relatives' information is often indirectly exposed;
- **Community-level rights**, when population-specific traits are studied or disclosed;
- **Public health considerations**, where aggregated genomic data may be used for disease surveillance or epidemiology; and
- **Biosecurity risks**, including potential misuse in bioweapons research or discriminatory profiling.

These factors illustrate why **simplistic, one-time consent frameworks**—such as those often assumed under general data-protection laws—are insufficient for genomic data. The unique characteristics of this data type demand **contextual, ongoing, and relational consent mechanisms**.

2.2 Relational Privacy: Genomics Challenges the Individual-Centric Model

Traditional data-protection paradigms, including those embedded in the DPDP Act, are **individual-centric**: they assume that data belongs to the individual, and that the individual has the sole authority to consent to its use. Genomic data challenges this model because it is inherently **co-owned by genetic relatives**, making privacy a **relational concept** rather than purely individual.

Some illustrative examples include:

- **Unintentional disclosure of familial risk:** A person consenting to genomic sequencing may reveal heritable disease risks of family members without their knowledge.
- **Children and inherited traits:** A child's genome contains half of each parent's genetic code. Parental consent for testing affects not only the child but indirectly the parent's privacy as well.
- **Community-level disclosure:** Certain genetic variants are highly correlated within populations. Discovery of a disease-linked allele in one individual could inadvertently stereotype an entire community or ethnic group, exposing them to stigma, discrimination, or socio-economic disadvantage.

These relational dynamics highlight a **gap in the DPDP Act**, which primarily recognizes individual consent and control. A law designed around individual autonomy cannot fully address the complexities of **collective genetic privacy**, necessitating a more nuanced approach that considers **familial and community dimensions** in consent and governance.

2.3 Genomic Data as a Tool for Discrimination and Surveillance

The predictive power of genomic data, while offering immense scientific and medical benefits, also introduces significant risks of **misuse and discrimination**. Genomic profiles can potentially reveal not only health risks but also behavioral tendencies, cognitive capacities, addiction susceptibility, physical traits, and reproductive outcomes. In the absence of robust safeguards, this information could be exploited in numerous ways:

- **Insurance Discrimination:** Companies might use genetic risk profiles to deny coverage or increase premiums for individuals predisposed to chronic illnesses.

- **Employment Bias:** Employers could screen candidates for genetic predispositions to mental health conditions or other traits, effectively introducing new forms of workplace discrimination.
- **Denial of Services:** Access to loans, education, housing, or social services could be biased based on genetic data.
- **State Surveillance:** Governments could employ genetic databases for population control, predictive policing, or profiling vulnerable groups.
- **Targeting of Ethnic or Indigenous Groups:** Aggregated genomic data could stigmatize entire communities or be used to justify discriminatory policies.
- **Bioweapon Development:** Malicious actors could exploit genetic data to develop targeted biological weapons against specific populations or individuals.

International standards such as the **EU GDPR**, the **Genetic Information Nondiscrimination Act (GINA) in the U.S.**, and UNESCO's bioethics declarations explicitly recognize these dangers. They impose heightened consent, explicit protections, and anti-discrimination obligations for genomic data. By contrast, the **DPDP Act does not explicitly identify these risks**, leaving Indian citizens vulnerable to potential misuse of their genetic information. This underscores the urgent need for **enhanced protections, explicit recognition of genomic sensitivity, and mechanisms to prevent both individual and systemic harm**.

Genomic data represents a **new frontier of privacy law**, one that transcends traditional categories of personal information. Its **immutable, predictive, and relational nature**, combined with its potential for **discrimination and surveillance**, renders conventional consent frameworks inadequate. A robust legal approach must account not only for the individual but also for familial, community, and societal dimensions of privacy. Failure to recognize these dimensions risks **ethical violations, legal gaps, and societal harm**, making it imperative that Indian law evolves to reflect the unique characteristics of genomic data.

3. Genomic Data Through the Lens of the DPDP Act, 2023

The **Digital Personal Data Protection Act, 2023 (DPDP Act)** represents India's first cross-sectoral effort to regulate personal data, marking a critical step in the evolution of digital governance. Unlike prior drafts that proposed distinct categories for sensitive personal data—including biometric, health, and genetic information—the DPDP Act adopts a **single-tier approach** to all personal data. While this simplifies compliance for many data processors, it raises significant concerns in domains where data sensitivity is inherently high, such as **genomic information**.

Genomic data, by virtue of its permanence, predictive capacity, and familial implications, challenges the DPDP Act's generalized framework. This section explores these challenges, highlighting the regulatory gaps and limitations in India's current legal regime.

3.1 Absence of "Sensitive Personal Data": Implications for Genomics

A fundamental feature of the DPDP Act is its deliberate **avoidance of a "sensitive personal data" classification**. In contrast, the **EU General Data Protection Regulation (GDPR)** identifies genetic, biometric, and health data as special categories requiring heightened protection. The lack of such classification in India has several consequences for genomic data:

- **Minimal consent obligations:** Genomic data is subject only to basic, one-time consent, akin to routine data like email addresses or contact numbers.

- **Reduced processor accountability:** Data processors handling genomic information are not bound by stricter duties such as privacy impact assessments, purpose limitation, or enhanced security measures.
- **Absence of storage and minimization rules:** The Act does not mandate genomic-specific storage limitations, deletion timelines, or data minimization principles.
- **Breach notification parity:** Breaches involving genomic data are treated no differently than breaches of ordinary personal data, despite the irreversible nature of genomic information.
- **Uniform penalties:** The law does not impose higher penalties for misuse of sensitive biological data, leaving victims of genomic breaches potentially underprotected.

This regulatory **vacuum exposes genomic data to heightened risks**, including unauthorized commercial exploitation, research misuse, and cross-border transfers without adequate safeguards.

3.2 Consent Requirements under DPDP and Their Limitations for Genomics

The DPDP Act emphasizes **free, specific, informed, and revocable consent**, accessible in plain language. While adequate for routine personal data, these requirements fall short when applied to genomic information.

3.2.1 Consent Cannot Predict Future Uses

Genomic data is **dynamic in its utility**. A single genome may be analyzed sequentially for multiple purposes:

- **Ancestry and genealogical studies**
- **Clinical and predictive health insights**
- **AI-driven behavioral, cognitive, or risk profiling**
- **Population-level research or public health databases**

A one-time consent cannot reasonably anticipate these evolving applications. Without continuous, purpose-specific consent, the individual loses meaningful control over downstream data use.

3.2.2 Consent Does Not Address Familial Rights

Genomic data is **inherently relational**. Consent granted by one individual may affect the privacy of:

- Parents and siblings
- Children and future descendants
- Extended relatives and genetic communities

The DPDP Act vests control solely in the individual, creating a **blind spot** where familial or community interests remain unprotected. In research or commercial contexts, this may result in inadvertent exposure of relatives' genetic predispositions without their knowledge or consent.

3.2.3 Revocation of Consent is Problematic

While the Act provides for revocable consent, genomic data presents unique challenges:

- **Irreversibility:** Scientists cannot "unsequence" a genome once processed.
- **AI entanglement:** Models trained on genomic data cannot easily eliminate individual genetic signatures.
- **Familial impact:** Even if an individual revokes consent, relatives share overlapping genetic markers that cannot be removed retroactively.

Thus, the revocation model envisaged by the DPDP Act **clashes with biological and technological realities**, undermining the intended protection.

3.3 Research Exemptions: A Gap for Biomedical and Genomic Research

The DPDP Act allows the government to notify exemptions for research purposes. However, its approach is **narrow and underdeveloped** concerning genomics:

- **Undefined criteria:** No standards specify which genomic research qualifies for exemption.
- **Ethical safeguards absent:** The law lacks requirements for institutional review boards, ethical committees, or consent oversight specific to genetic research.
- **No genomic oversight authority:** There is no dedicated regulatory body to monitor research involving highly sensitive genetic data.
- **Community consent ignored:** Studies on populations or tribal communities often involve shared genetic traits, yet the Act does not mandate community-level consultation or approval.
- **Anonymization challenges:** Genomic data is inherently re-identifiable, rendering anonymization unreliable as a privacy safeguard.

These gaps raise the risk of **ethical violations, misuse in commercial genomics, and unregulated population-level studies**.

3.4 Children's Genomic Data Under DPDP

Children represent a **particularly vulnerable population** in genomic research:

- Parental consent substitutes for the child's ability to consent.
- Children cannot meaningfully object to unforeseen future uses of their genetic data.
- Genetic data collected in childhood remains **permanent**, potentially affecting life-long privacy and autonomy.
- Predictive testing may violate the **child's right to an open future**, a principle recognized in bioethics and international human rights law.

The DPDP Act lacks specific guidance for **minors' genomic data**, leaving ethical and legal dilemmas unaddressed.

3.5 Cross-Border Transfers of Genomic Data

The Act permits data transfers to all jurisdictions **except those blacklisted by the government**, adopting a **"negative list" approach**. Compared to GDPR's **"adequacy" model**, which requires explicit evaluation of recipient countries' data protection levels, this framework is **weak and risky**:

- **Data exploitation risks:** Indian genomic data could be transferred to jurisdictions without stringent privacy protections.
- **Commercial misuse:** Global biotech companies may leverage population-scale genomic datasets for profit, often without meaningful benefit to data subjects.
- **Security threats:** Sensitive DNA data may reach countries with advanced bio-research or militarized genomics programs.

3.5.1 Bio-Sovereignty Concerns

Many countries, including **China, UAE, and Qatar**, treat genomic data as a **strategic national asset**, imposing strict localization and export controls. India currently lacks a **comprehensive framework to safeguard genomic sovereignty**, exposing its population and national research assets to potential exploitation. Protecting genomic data is not merely a privacy imperative; it is a matter of **national biosecurity and strategic scientific autonomy**.

The DPDP Act represents a landmark effort to codify personal data protection in India. However, its **single-tier approach and individual-centric consent model** are ill-suited for the **unique characteristics of genomic data**. The absence of:

- Recognition of genomic data as sensitive,
- Mechanisms for relational and ongoing consent,
- Ethical and research oversight,
- Safeguards for children, communities, and cross-border transfers

creates a **regulatory vacuum** that leaves Indian citizens and genomic assets vulnerable. To address these challenges, India requires **genomic-specific regulations**, aligned with international standards yet adapted to its socio-legal and bioethical context.

4. Global Standards Governing Genomic Data: A Comparative Overview

The governance of genomic data has evolved into a **multifaceted legal and ethical challenge** globally. Unlike conventional personal data, genomic information is **predictive, permanent, and relational**, raising complex questions of privacy, consent, discrimination, and biosecurity. Various jurisdictions and international frameworks have recognized these challenges, creating regulatory models that emphasize **heightened protection, explicit consent, ethical oversight, and cross-border safeguards**. This section examines the most influential standards and compares them to the DPDP Act, highlighting gaps and lessons for India.

4.1 European Union: GDPR and the Special Category Data Regime

The **General Data Protection Regulation (GDPR)**, enforced across the EU since 2018, provides one of the most comprehensive frameworks for genomic data protection. Under GDPR, **genetic data is classified as "special category personal data"** due to its sensitivity and potential for misuse.

4.1.1 Definition and Scope

GDPR defines genetic data as:

"Personal data relating to inherited or acquired genetic characteristics which give unique information about the physiology or the health of a natural person, and which result in particular from the analysis of a biological sample."

This definition is broad, covering:

- DNA and RNA sequences
- Epigenetic markers
- Whole-genome and exome data
- Genetic variants
- Polygenic risk scores

4.1.2 Key Protections for Genetic Data

Processing genetic data under GDPR requires:

1. **Explicit consent:** Individuals must provide informed, specific, and revocable consent. Blanket consent is insufficient.
2. **Purpose limitation:** Data can only be used for clearly defined purposes. Secondary uses require new consent or strong legal justification.
3. **Data minimization:** Only data necessary for the specified purpose may be collected.
4. **Enhanced safeguards:** Strong technical and organizational measures are required to protect sensitive genetic information.
5. **Restrictions on automated profiling:** Genetic data cannot be used for automated decision-making that produces legal or similarly significant effects without safeguards.

4.1.3 Research and Public Health Exceptions

GDPR permits limited exemptions for scientific research and public health purposes, provided:

- Ethical review is conducted
- Pseudonymization techniques are applied
- Oversight mechanisms are in place

By comparison, India's DPDP Act lacks these nuanced provisions for genomic research and public health applications.

4.2 Council of Europe: Oviedo Convention and Additional Protocols

The **Oviedo Convention (1997)** is the preeminent treaty on human rights and bioethics. While not yet ratified by India, it provides internationally recognized principles for genetic governance.

4.2.1 Key Principles

1. **Primacy of human dignity:** No individual should be treated merely as a source of data.
2. **Genetic testing for health purposes only:** Testing for non-medical purposes, such as predictive behavioural profiling, is prohibited.
3. **Prohibition of discrimination based on genetic traits:** States must prevent unfair treatment in employment, insurance, and access to services.
4. **Informed consent:** Genetic testing requires explicit, informed consent, including discussion of future uses and potential familial implications.

The Oviedo Convention underscores the **ethical dimensions of genomics**, which go beyond conventional data privacy and are largely absent in India's DPDP Act.

4.3 UNESCO Universal Declaration on the Human Genome and Human Rights

UNESCO's **Universal Declaration on the Human Genome and Human Rights (1997, revised 2003)** establishes that:

- The human genome is a **heritage of humanity** and must be protected.
- Genetic data requires **special ethical and legal safeguards**.
- States must prevent **genetic discrimination** and respect the rights of communities and indigenous populations.
- Consent must be informed, explicit, and contextual, accounting for potential societal consequences.

These principles provide a **rights-based ethical framework** for genomics, emphasizing human dignity and collective responsibility—a perspective not directly reflected in the DPDP Act.

4.4 OECD Guidelines on Human Biobanks and Genetic Research Databases

The **OECD Guidelines (2009)** provide detailed recommendations for the governance of genomic biobanks and research databases. Key elements include:

- **Transparency and accountability:** Clear rules about data collection, storage, and usage.
- **Ethical review:** Independent ethics committees must approve research involving genetic data.
- **Consent management:** Participants must be able to withdraw consent, with limitations communicated transparently.
- **Privacy by design:** Data must be protected using pseudonymization, encryption, and access controls.
- **Community and indigenous considerations:** Research impacting specific populations should involve community consultation and culturally sensitive protocols.

These guidelines recognize **both individual and collective dimensions** of genomic privacy, providing a model for India to consider.

4.5 United States: HIPAA, GINA, and Sectoral Protections

In the United States, genomic data protection is **fragmented and sector-specific**.

4.5.1 HIPAA (Health Insurance Portability and Accountability Act)

- Protects medical and health-related information, including genomic test results.
- Applies primarily to healthcare providers, insurers, and their business associates.
- Emphasizes **security safeguards, privacy notices, and breach notifications**.

4.5.2 GINA (Genetic Information Nondiscrimination Act, 2008)

- Prohibits genetic discrimination in health insurance and employment.
- Covers predictive genetic information, familial data, and manifested conditions.
- Does **not extend to life insurance, disability insurance, or long-term care coverage**, leaving regulatory gaps.

Despite these protections, the U.S. lacks a **comprehensive, cross-sectoral legal framework** equivalent to GDPR or a specialized genomic regulatory authority.

4.6 Asia-Pacific Models: China, Japan, and Australia

China

- Treats genomic data as a **strategic national asset**.
- Requires **localization** of genomic databases and strict government approval for cross-border transfer.
- Conducts extensive oversight on research, commercial use, and international collaborations.

Japan

- Implements detailed **guidelines for genomic privacy** in research and clinical contexts.
- Requires independent ethics committee review for all human genomic studies.
- Emphasizes **participant consent, data minimization, and security measures**.

Australia

- Incorporates genetic privacy protections into healthcare and research law.
- Requires transparency in biobank governance and participant consent.
- Encourages **community engagement** for research involving indigenous populations.

These models emphasize **state oversight, ethical review, and cultural sensitivity**, illustrating approaches India could adapt.

4.7 Key Lessons for India

Comparing these global frameworks with the DPDP Act reveals significant **gaps in India's regulatory approach**:

Feature	DPDP Act	Global Standards	Gap / Recommendation
Classification of genomic data	Not defined; single-tier model	GDPR: special category; UNESCO: protected	India should classify genomic data as a sensitive category
Consent	One-time, individual	Explicit, informed, tiered, relational	Need ongoing, context-specific, familial/community consent

Research oversight	Minimal; government exemptions	OECD, GDPR, Japan: ethics review, biobank governance	Establish a dedicated genomic oversight authority
Anti-discrimination	None	GINA, Oviedo, UNESCO	Introduce legal safeguards against genetic discrimination
Cross-border transfers	Negative list	GDPR adequacy, China localization	Implement adequacy assessment and bio-sovereignty standards
Community/indigenous protection	Not addressed	UNESCO, OECD, Australia	Include community consent and culturally sensitive protocols

Conclusion: Global standards emphasize **heightened protection, relational consent, ethical oversight, and anti-discrimination measures** for genomic data. In contrast, India's DPDP Act provides only **basic, individual-centric protections**, leaving citizens, communities, and national genomic assets exposed to significant ethical, legal, and security risks. A **contextual, genomic-specific regulatory framework** is therefore essential.

5. Challenges in Genomic Data Governance: Ethical, Legal, and Social Dimensions

Genomic data sits at the intersection of **biomedicine, technology, law, and society**, making its governance particularly complex. While technological advances have unlocked unprecedented opportunities in health, ancestry, and research, they have simultaneously raised **ethical, legal, and social concerns** that conventional data protection frameworks—including India's DPDP Act—struggle to address. This section examines the principal challenges facing genomic data governance.

5.1 Ethical Challenges

5.1.1 Informed Consent and Future Uses

Traditional consent models assume that individuals can make fully informed decisions about the use of their data. Genomic data, however, is inherently **forward-looking and evolving**. A genome sequenced today may be used tomorrow for:

- Predictive health analysis
- Behavioral and cognitive profiling using AI
- Population-scale research
- Personalized medicine trials

Ethical challenge: One-time consent is insufficient. Participants cannot foresee all potential applications, raising concerns about **autonomy and meaningful choice**. Global standards, such as GDPR and OECD Guidelines, advocate **tiered or dynamic consent** mechanisms, which India currently lacks.

5.1.2 Relational and Collective Ethics

Genomic data is **shared by nature**—it encodes information about relatives, descendants, and even ethnic groups. This creates **relational privacy concerns**:

- Testing one individual may inadvertently reveal disease risks for parents, siblings, or children.
- Certain genetic variants may stigmatize entire communities or ethnic populations.

Ethical challenge: Individual consent is **necessary but insufficient**. Collective and familial consent frameworks are critical to respecting both **individual rights and communal dignity**.

5.1.3 Children and the Right to an Open Future

Genomic testing in minors raises unique concerns:

- Parents consent on behalf of the child, who cannot meaningfully object.
- Predictive testing may expose children to **lifelong discrimination** or psychological distress.
- Information about adult-onset conditions may violate the child's **right to remain unaware until they reach maturity**.

The DPDP Act provides some protection for minors but **fails to address these genome-specific ethical dilemmas**.

5.2 Legal Challenges

5.2.1 Lack of Recognition of Genomic Data as Sensitive

As discussed, the DPDP Act **does not classify genomic data as sensitive**, resulting in:

- Minimal obligations for processors
- Equal treatment of genomic data and routine personal data like email addresses
- Limited recourse for victims of misuse

Global standards, including GDPR, GINA, and UNESCO declarations, explicitly recognize **genomic data as highly sensitive**, demanding heightened protections.

5.2.2 Inadequate Protections Against Discrimination

Genetic information can be misused in:

- **Insurance underwriting:** denying or increasing premiums based on risk predisposition
- **Employment:** screening candidates for susceptibility to diseases or behavioral traits
- **Education and services:** bias in access to opportunities

Without explicit anti-discrimination provisions, India's DPDP Act leaves gaps that could enable **genetic profiling and societal inequities**.

5.2.3 Enforcement and Redress

- Existing penalties under the DPDP Act are **uniform**, regardless of data sensitivity.
- The lack of **special oversight mechanisms** for genomic data reduces accountability.
- Cross-border enforcement is **problematic**, especially if genomic data is transferred to jurisdictions without strong privacy protections.

5.3 Technological Challenges

5.3.1 Re-identification Risks

Even anonymized genomic datasets are **highly re-identifiable**. Studies have demonstrated that an individual's DNA can be linked to their identity using minimal auxiliary information (e.g., age, sex, location). This undermines standard **anonymization techniques** used in research and commercial datasets.

5.3.2 AI and Predictive Profiling

Artificial intelligence enables predictive analytics on genomic data, including:

- Disease susceptibility
- Behavioral tendencies
- Drug response profiling

Risk: AI models trained on genomic datasets can inadvertently encode biases or be misused for **population-level surveillance, eugenics, or targeted commercial strategies**. Without safeguards, predictive models may compromise privacy and fairness.

5.3.3 Data Storage and Security

Genomic data is **large and complex**, requiring robust storage solutions. Challenges include:

- Ensuring secure long-term storage
- Preventing unauthorized access or breaches
- Balancing cloud storage efficiency with national biosecurity considerations

India's DPDP Act **does not specify heightened obligations for genomic data storage or encryption**, creating vulnerabilities.

5.4 Social and Cultural Challenges

5.4.1 Stigmatization and Discrimination

Genomic findings can create social stigma at both **individual and community levels**:

- Communities may be labeled as genetically predisposed to certain diseases.
- Cultural practices or taboos may intersect with genetic findings, creating ethical dilemmas.
- Misinterpretation of genetic data can exacerbate social inequalities.

5.4.2 Public Trust and Participation

For genomic research and precision medicine initiatives to succeed, **public trust** is essential. Governance gaps, inadequate consent models, and the potential for misuse can **erode confidence**, reducing participation in research and public health programs.

5.4.3 Equity and Access

Advanced genomic testing is expensive and often limited to urban or high-income populations. Without equitable policies, **genomic medicine may widen health disparities**, leaving marginalized communities underserved.

5.5 Biosecurity and National Concerns

Genomic data is increasingly recognized as a **strategic national asset**:

- Unrestricted cross-border transfers may expose population-level genomic information to foreign governments or commercial entities.
- Genomic data could be exploited for **bioweapon development or targeted biological interventions**.
- India currently lacks a **bio-sovereignty framework**, unlike countries such as China, Qatar, or UAE.

Implication: Genomic governance is not merely a privacy issue; it intersects with **national security, ethical governance, and scientific sovereignty**.

5.6 Integrating Ethical, Legal, and Social Governance

The challenges outlined above demonstrate that **genomic data cannot be governed through conventional, individual-centric data protection laws alone**. Effective governance requires an **integrated framework** combining:

- **Ethical safeguards:** tiered consent, relational privacy, community engagement
- **Legal protections:** sensitive data classification, anti-discrimination provisions, penalties proportional to harm
- **Technological measures:** encryption, secure storage, AI auditing, re-identification prevention
- **Social policies:** equity in access, cultural sensitivity, public engagement
- **National security protocols:** bio-sovereignty standards, export controls, and cross-border adequacy assessments

Globally, these principles are embedded in GDPR, OECD Guidelines, UNESCO declarations, and specialized national regulations. India's DPDP Act, by contrast, addresses only **the individual consent dimension**, leaving the broader ethical, legal, technological, and social ecosystem largely unregulated.
Genomic data governance presents **complex, multi-layered challenges** that span ethical, legal, social, and technological domains. The unique characteristics of genomes—immutability, rationality, predictive power, and permanence—demand **context-sensitive regulations and governance frameworks**. India's current DPDP Act represents a foundational step in data protection but **falls short of global best practices**, particularly in genomic data governance. Addressing these gaps is critical for **protecting individual and collective rights, ensuring ethical research, and safeguarding national biosecurity**.

6. Policy Recommendations and Path Forward: Strengthening Genomic Data Governance in India

The analysis of the DPDP Act and global standards highlights a critical gap in India's **genomic data governance framework**. While the DPDP Act marks a significant step in personal data protection, its **single-tier, individual-centric approach** is insufficient for the unique characteristics of genomic information. To safeguard privacy, ethical research, social equity, and national biosecurity, India must adopt **genome-specific policies**, informed by global best practices and adapted to its socio-cultural and legal context. This section outlines key policy recommendations.

6.1 Recognize Genomic Data as a Special Category

India must **explicitly classify genomic data as "sensitive personal data"** under the DPDP Act or through supplementary legislation. Features of this classification should include:

- **Heightened protection standards:** Obligations for security, storage, and breach notification.
- **Consent requirements:** Tiered, informed, and dynamic consent reflecting evolving uses.
- **Family and community considerations:** Consent frameworks acknowledging relational privacy.
- **Penalties for misuse:** Enhanced consequences for violations of genomic data privacy or discriminatory use.

This approach aligns with **GDPR's special category data model**, UNESCO ethical frameworks, and OECD biobank guidelines.

6.2 Develop Tiered and Relational Consent Mechanisms

Given the **predictive and relational nature of genomes**, India should implement **tiered consent protocols**:

- **Tiered consent:** Allow participants to consent separately for ancestry, clinical research, AI profiling, and public health studies.
- **Dynamic consent:** Enable ongoing updates and revocation of consent, with mechanisms to track and manage data use over time.
- **Relational consent:** Account for familial and community impacts, particularly for research affecting multiple generations or tribal populations.

This ensures **meaningful autonomy, ethical transparency, and respect for collective rights**.

6.3 Strengthen Research Oversight and Ethics Review

Research involving genomic data requires **robust regulatory oversight**. Recommended measures include:

- **Dedicated Genomic Data Authority:** An independent body overseeing genomic data collection, storage, research use, and international collaboration.

- **Mandatory ethics review:** All genomic research should be approved by institutional or national ethics committees, with community consultation where applicable.
- **Data minimization and pseudonymization:** Researchers must collect only essential data and apply technical safeguards to reduce re-identification risk.
- **Community engagement protocols:** Particularly for tribal or indigenous populations, community consent should complement individual consent.

These measures are modeled on **OECD Guidelines, Japan's genomic research frameworks, and Australian Indigenous research protocols**.

6.4 Protect Children and Vulnerable Populations

Children's genomic data requires **specialized safeguards**:

- **Delayed access to adult-onset information:** Predictive results for adult-onset conditions should be withheld until the child reaches maturity.
- **Parental oversight with ethical checks:** Parents may consent for research, but ethics committees should ensure long-term interests of the child are protected.
- **Periodic reassessment:** Consent and use should be revisited as the child matures and can make autonomous decisions.

These steps respect the **child's right to an open future**, a principle endorsed by UNESCO and bioethics scholarship.

6.5 Introduce Anti-Discrimination and Legal Protections

To prevent misuse of genomic data, India should implement **explicit legal safeguards**:

- **Genetic non-discrimination laws:** Protect against employment, insurance, education, and service discrimination based on genetic information.
- **Legal recourse for misuse:** Individuals or communities must have access to complaint mechanisms and compensation for privacy violations.
- **Penalties proportionate to harm:** Violations involving genomic data should incur **higher fines or criminal liability**, reflecting the permanence and sensitivity of the information.

These measures mirror the **U.S. GINA framework, GDPR anti-discrimination principles, and UNESCO guidelines**.

6.6 Secure Storage and Technological Safeguards

The DPDP Act should mandate **genomic-specific technical safeguards**:

- **Encrypted and secure storage:** Both at rest and in transit.
- **Restricted access controls:** Role-based or purpose-based access, with audit trails.
- **Re-identification risk mitigation:** Algorithms and AI models should be audited to prevent inadvertent disclosure or profiling.
- **Secure cross-border transfer protocols:** Data should only leave India for countries with **adequate privacy and security protections**.

Technological standards should **anticipate AI-driven analytics, cloud storage vulnerabilities, and population-scale data management**.

6.7 Strengthen Bio-Sovereignty and Cross-Border Governance

Genomic data is increasingly recognized as a **national strategic resource**. India should:

- **Implement adequacy-based cross-border transfer rules:** Similar to GDPR, only allowing transfers to countries with equivalent protections.

- **Localize critical genomic databases:** Especially for population health, AI research, or sensitive commercial applications.
- **Establish a national genomic policy:** Align research, commercial, and public health use with biosecurity and national interests.

These measures safeguard **scientific autonomy, national security, and population-level privacy**.

6.8 Promote Public Engagement and Equity

For genomic governance to succeed, **public trust and inclusivity** are essential:

- **Transparency initiatives:** Inform citizens about data collection, storage, and use.
- **Equitable access:** Ensure genomic testing, personalized medicine, and research participation are not limited to urban or high-income populations.
- **Community consultation:** Particularly for indigenous or marginalized groups, incorporate cultural and ethical considerations in data collection.
- **Educational campaigns:** Raise awareness of genomic privacy, consent, and potential risks.

Public engagement ensures **ethical legitimacy, increased participation, and social acceptance**.

6.9 Harmonize India's Policies with Global Standards

India can adopt **a hybrid model**:

- **Legal and ethical alignment:** Recognize genomic data as sensitive, require tiered and relational consent, and establish anti-discrimination safeguards.
- **Technological safeguards:** Incorporate security, anonymization, and AI auditing standards from GDPR and OECD guidelines.
- **Ethical governance:** Institutionalize oversight and community consultation, modeled on Japan, Australia, and UNESCO frameworks.
- **Bio-sovereignty measures:** Localize databases, regulate cross-border transfers, and treat genomic data as a strategic asset.

This approach balances **innovation, research utility, ethical protection, and national security**, creating a **comprehensive genomic data governance ecosystem**.

Genomic data governance in India is at a crossroads. The DPDP Act provides a foundational **legal framework for personal data protection**, but its **one-size-fits-all approach is inadequate** for the unique ethical, legal, technological, and societal challenges posed by genomic data. By adopting **genomic-specific classifications, tiered consent mechanisms, ethical oversight, anti-discrimination protections, and bio-sovereignty policies**, India can:

- Protect **individual, familial, and community privacy**
- Enable **responsible research and innovation**
- Ensure **national security and population-level safeguards**
- Align domestic policy with **international best practices**

Such reforms would not only **future-proof India's genomic ecosystem** but also position the country as a **global leader in ethical, equitable, and secure genomic research**.

Conclusion

Genomic data governance is a **complex, multi-dimensional challenge** that encompasses ethical, legal, technological, social, and national security dimensions. India's DPDP Act, while a foundational step in personal data protection, **falls short in addressing the unique characteristics of genomic information**. By adopting **sensitive data classification, tiered consent, ethical oversight, anti-discrimination**

safeguards, and bio-sovereignty measures, India can protect individual, familial, and community rights, enable responsible research, and safeguard national interests. Aligning domestic frameworks with global best practices while respecting **India's socio-cultural context** is essential for the **ethical, equitable, and secure governance of genomic data**, positioning the nation as a global leader in genomic research and policy.

References

1. Brassington, I. (2023). *The private life of the genome: Genetic information and the right to privacy*. Routledge. https://www.routledge.com/The-Private-Life-of-the-Genome-Genetic-Information-and-the-Right-to-Privacy/Brassington/p/book/9781032320434
2. Hallinan, D. (2021). *Protecting genetic privacy in biobanking through data protection law*. Oxford University Press. https://academic.oup.com/book/39484
3. Laurie, G. (2002). *Genetic privacy: A challenge to medico-legal norms*. Cambridge University Press. https://philpapers.org/rec/LAUGPA-3
4. Mascalzoni, D. (Ed.). (2015). *Ethics, law and governance of biobanking: National, European and international approaches*. Springer. https://link.springer.com/book/10.1007/978-94-017-9573-9
5. Tyagi, A. K. (Ed.). (2023). *Privacy preservation of genomic and medical data*. Wiley-VCH. https://www.wiley-vch.de/en/areas-interest/computing-computer sciences/privacy-preservation-of-genomic-and-medical-data-978-1-394-21262-0
6. Krimsky, S., & Simoncelli, T. (2012). *Genetic justice: DNA data banks, criminal investigations, and civil liberties*. Columbia University Press. https://cup.columbia.edu/book/genetic-justice/9780231145206
7. Rawal, L., & Ali, S. (Eds.). (2017). *Genome analysis and human health*. Springer. https://link.springer.com/book/10.1007/978-981-10-4298-0
8. Human Genome Organisation (HUGO). (2015). *Ethical, legal and social issues in human genomics*. Springer.
9. UNESCO. (2003). *International declaration on human genetic data*. United Nations Educational, Scientific and Cultural Organization. https://www.unesco.org/en/ethics-science-technology/human-genetic-data
10. Knoppers, B. M. (2014). *Genomics and society: Ethical, legal and social perspectives*. Springer.
11. Geller, G., & Rothstein, M. A. (Eds.). (2012). *Genomic and precision medicine: Ethical, legal, and social implications*. Academic Press.
12. Parker, L., & Lucassen, A. (2004). *Genetics and ethics in the clinic: Genetic counselling, consent and privacy*. Routledge.
13. Haga, S. B., & O'Daniel, J. M. (Eds.). (2016). *Genomic medicine and the law: Regulating the genomic revolution*. Springer.
14. Samuel, G., & Farsides, B. (2009). *The social and ethical issues of genetic testing*. Cambridge University Press.
15. Dheensa, S., Fenwick, A., & Lucassen, A. (2016). *Genetic responsibility: Ethics, law and familial communication*. Routledge.