The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE DNA DILEMMA:

WHY INDIAN LAWS ARE NOT READY FOR THE GENETIC AGE

~ Shrushti Dumbre

"In the digital age, a leaked password can be changed. A leaked genome cannot."

ABSTRACT

India is about to lose the only real protection its law gives to health and biometric information and almost no one has noticed. The old law, the ***Information Technology Act, 2000*** *and its 2011 Rules, treats medical and biometric data as "sensitive personal data" that deserves extra care, and a Bill drafted in 2019 would have gone further and named genetic data itself as protected. But the Parliament passed, the* ***Digital Personal Data Protection Act, 2023****, which threw that special category out. When its main provisions take effect on 13 May 2027, it repeals* ***Section 43A*** *of the older Act and puts nothing in its place. So, in two consecutive years India did two contradictory things: it built the tools to collect genetic material on a large scale, through the* ***Criminal Procedure (Identification) Act, 2022*** *and the* ***Genome India Project****, while tearing down the legal protection for it. Drawing on the long-running debate about "genetic exceptionalism", on how Europe, the United States and Britain handle the problem, and on the collapse and sale of the DNA-testing company 23andMe, this paper makes a simple argument: genetic data is genuinely different from ordinary personal data in three ways, Indian law no longer reflects that difference, and the chance to fix it runs out on that date. It ends with eight practical reforms, several of which need no change to the main law at all.*

KEYWORDS

Genetic privacy; genetic exceptionalism; Digital Personal Data Protection Act, 2023; sensitive personal data; ***Puttaswamy****;* ***Criminal Procedure (Identification) Act, 2022****; Genome India Project; genetic discrimination; informed consent; data protection.*

INTRODUCTION

Imagine you send a saliva sample to a lab and get back a report on your ancestry, your health risks and your traits. What happens to that information afterwards? Who owns it? How long is it kept, and can it be shared with researchers, with companies, or with the systems used to train artificial intelligence? And, most important for this paper: does Indian law give you any answer at all?

These questions sit at the heart of what we can call the DNA Dilemma: the growing gap between what genetic technology can now do and what the law is actually equipped to handle. That gap is not unique to India. What is unusual here is that it is not simply being left open instead it is being widened on purpose, by legislative design.

Indian law once accepted, if imperfectly, that health and biometric information deserved stronger protection than something like an email address.[1] The Bill drafted in 2019 went further still, naming genetic data outright as a protected category.[2] But the law Parliament actually passed in 2023 dropped the whole idea of protected categories.[3] And in the year before that, Parliament had already passed a law allowing the forced collection of "biological samples" from anyone arrested for any offence, to be kept for seventy-five years.[4] In the year after, the government quietly withdrew the one Bill that would have regulated DNA specifically.[5]

Put those pieces together and a pattern appears: A State that has built the power to collect

[1] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3 (India) (listing medical records and history and biometric information as sensitive personal data or information).

[2] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, cl. 3(36) (India). Available at: https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.

[3] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 2(t) (India) (defining "personal data" as "any data about an individual who is identifiable by or in relation to such data", with no graded category of sensitivity anywhere in the Act).

[4] The Criminal Procedure (Identification) Act, 2022, No. 11 of 2022 (India). Available at: https://prsindia.org/billtrack/the-criminal-procedure-identification-bill-2022.

[5] The DNA Technology (Use and Application) Regulation Bill, 2019 was withdrawn from the Lok Sabha on 24 July 2023. See PRS Legislative Research, The DNA Technology (Use and Application) Regulation Bill, 2019. Available at: https://prsindia.org/billtrack/the-dna-technology-use-and-application-regulation-bill-2019.

genetic material while removing the legal category that would have protected it. This paper sets out what has happened, why it matters, and what can still be done before 13 May 2027, the day the main provisions of the *2023 Act* take effect and the older protections are repealed.

RESEARCH DESIGN

Indian data protection law no longer treats genetic data any differently from other personal data, even though it once did, in part, and a Bill once proposed to do so openly. This paper asks a few connected questions. Is that position defensible? Is genetic data really different? How do the European Union, the United States and the United Kingdom deal with it? And what should India do, including steps that need no change to the main law? Its argument is that India's treatment of genetic data as ordinary is not an error but the result of deliberate decisions taken between 2022 and 2023, and that the danger will grow once the 2023 Act is fully in force. The method is doctrinal: it reads the statutes, rules and Bills, their legislative history and the relevant court decisions, alongside peer-reviewed work in law and bioethics, official publications, and reporting on real incidents. The three-country comparison is functional as each was chosen for a distinct technique.

LITERATURE REVIEW

Should genetic information be treated differently by the law? That question, the debate over "*genetic exceptionalism*", has occupied scholars for more than thirty years, and it is genuinely unsettled.

Early writing approached genetic information through medical confidentiality and bioethics, and **George J. Annas** was among the first to shape the conversation. He argued that ordinary confidentiality rules simply could not handle the problems genetic information created;[6] it needed its own law, not a patch on existing medical-privacy rules. Others disagreed. **Thomas Murray**, writing in 1997, asked whether genetic information is really different from other medical information and concluded that it is not different in kind.[7] Plenty of medical

[6] Annas, supra note 7. See also George J. Annas, Leonard H. Glantz & Patricia A. Roche, Drafting the Genetic Privacy Act: Science, Policy, and Practical Considerations, 23 J.L. Med. & Ethics 360 (1995). Available at: https://www.cambridge.org/core/journals/journal-of-law-medicine-and-ethics/article/abs/drafting-the-genetic-privacy-act-science-policy-and-practical-considerations/02DDE33C52DEC4100E654838D25BB03F.

[7] Thomas H. Murray, Genetic Exceptionalism and "Future Diaries": Is Genetic Information Different from Other Medical Information? in Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era 60 (Mark A. Rothstein ed., Yale Univ. Press 1997).

information is predictive, involves relatives and partners, and in something as ordinary as a written family history has always revealed things about people who never consented. **Murray** warned that carving out a genetics-only category draws the line in the wrong place, so the law ends up protecting the test rather than the information.

As genomic research moved into international databases and private labs, the question changed from whether genetic information deserves protection to how it can work at scale. **Bartha Maria Knoppers** argued that individual consent, on its own, was no longer enough in global genomic research, and called instead for governance built on transparency, accountability and public trust.[8]

Broad data protection laws above all the European Union's ***General Data Protection Regulation*** (**GDPR**) added another angle: scholars asked not whether genetic information deserves protection, but how that protection should be designed. **De Hert** and **Papakonstantinou** note that although the **GDPR** does put genetic data in a special category, hard problems remain such as later re-use of the data, commercial exploitation, and governance.[9] Placing information in a special category, in other words, is necessary but not sufficient.

1. WHERE THIS PAPER STANDS & THE GAP IT ADDRESSES

This paper accepts a qualified version of exceptionalism. **Murray** and **Rothstein** are right that genetic information is not different in kind from every other type of medical information, and that a badly drafted law can end up protecting a testing method rather than a category of information. But one feature, the fact that genetic data is shared across a family is a difference in kind, not just degree. Other medical information may touch relatives by accident; genetic information touches them by its very nature, and in ways that can be computed. The **Golden State Killer investigation** (discussed below) shows the point: there, one person's choice effectively gave away the privacy of others, enough to justify treating this kind of data differently.

The gap this paper fills is a national one. The debate just described is almost entirely

[8] Bartha Maria Knoppers & Ruth Chadwick, Human Genetic Research: Emerging Trends in Ethics, 6 Nature Reviews Genetics 75 (2005). Available at: https://www.nature.com/articles/nrg1505.

[9] Paul De Hert & Vagelis Papakonstantinou, The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? 32 Computer Law & Security Review 179 (2016). Available at: https://research.tilburguniversity.edu/en/publications/the-new-general-data-protection-regulation-still-a-sound-system-f/.

American and European, argued against laws that already exist. Indian writing on genetic privacy is thin, and most of it either predates the 2023 Act or discusses it only in general terms, without asking what it did to the "sensitive data" category. No one has yet properly examined how three things fit together: the *2023 Act*, the ***Criminal Procedure (Identification) Act, 2022***, and the withdrawal of the ***DNA Technology Bill*** or what the 13 May 2027 start date will mean. That is the gap this paper addresses.

2. WHAT MAKES GENETIC DATA DIFFERENT

Any claim that genetic data deserves special treatment has to start by showing that it really is special. This section sets out three features that separate DNA from ordinary personal information because the legal argument that follows depends entirely on them.

2.1 PERMANENT

A password can be changed, a credit card reissued, an address left behind. When information leaks, data protection law's usual fix is to replace the compromised item with a new one. There is no such fix for a genome. A person's DNA is set at conception and does not change; once it is out, it is out for good, and no law or technology can pull it back. That is why the familiar toolkit of breach notices and clean-ups, which assumes the damage can be stopped by acting quickly, simply does not fit genetic data.

2.2 PREDICTIVE

Most personal data describe what is true about you now, or what was true in the past. Genetic data also describes what might become true. It can flag a raised chance of conditions you do not have, may never develop, and may not even know about. This forward-looking quality is exactly what makes genomic medicine so valuable, it lets doctors anticipate disease risk and target treatment. But the same quality makes the data useful to anyone deciding whether you are a good bet: as an employee, a borrower, or an insurance customer. **George Annas** captured this back in 1993, calling DNA a coded "future diary" already written, but not yet read, even by the person it belongs to.[10]

2.3 RELATIONAL

This is the feature that sets genetic data most sharply apart, and the one that ordinary privacy law is least able to handle. We normally assume personal data belongs to the single person it describes. A genome does not work that way. Because DNA is inherited, your

[10] George J. Annas, Privacy Rules for DNA Databanks: Protecting Coded "Future Diaries", 270 JAMA 2346 (1993). Available at: https://pubmed.ncbi.nlm.nih.gov/8230598/.

genetic information automatically reveals information about your parents, your siblings, your children and even distant relatives; none of whom agreed to it, and some of whom may not even know. By a decision that, on paper, concerns only you, you can expose the genetic privacy of your whole family.

This is not hypothetical. In 2018, investigators in California identified a suspect in the Golden State Killer case by uploading a crime-scene DNA profile to GEDmatch, a free genealogy website, and then working outwards through the family trees of distant relatives who had uploaded their own DNA.[11] The suspect had never taken a genetic test. He was found through the DNA of people he had never met. Later research suggested that a database covering even a small slice of a population can make most of that population identifiable through distant-relative matches.[12] The consent of a few can expose the many. No other kind of personal data behaves like this.

Put the three together: genetic data is permanent where other data can be replaced, predictive where other data merely describes, and shared across a family where other data belongs to one person. A legal framework built on the assumption that data describes a single identifiable person, at a single moment, and can be secured or corrected after the fact, is simply not built for this.

3. THE INDIAN LEGAL FRAMEWORK: A REGRESSION IN FOUR STEPS

India is usually described as a country that has not yet caught up with genetic technology. In fact, its position has moved over about fifteen years from partial protection to none. And the final step has not even taken effect yet.

3.1 *PUTTASWAMY* & THE CONSTITUTIONAL FOUNDATION

In ***Justice K.S. Puttaswamy (Retd.) v. Union of India***, a nine-judge bench of the Supreme Court held, unanimously, that the right to privacy is built into the right to life and personal liberty under ***Article 21***, and into the other fundamental rights in ***Part III of the***

[11] Golden State Killer: DNA and GEDmatch profile led police to wrong man before suspect Joseph James DeAngelo, Washington Post (Apr. 27, 2018). Available at: https://www.washingtonpost.com/news/true-crime/wp/2018/04/27/golden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say/.

[12] See We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans, Science (Oct. 11, 2018), reporting research on long-range familial searching. Available at: https://www.science.org/content/article/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white.

Constitution.[13] The Court also recognised "*informational privacy*" a person's interest in controlling data about themselves. So ***Puttaswamy*** gives genetic information a constitutional foothold. What it does not give is a statute to enforce it, and a constitutional right with no statute behind it is a right you have to fight for one court petition at a time.

3.2 THE SENSITIVE DATA CATEGORY, 2011

Until the *2023 Act* starts, the law in force is ***Section 43A of the Information Technology Act, 2000***, and the rules made under it. *Rule 3* of those rules defines "*sensitive personal data or information*" to include medical records and history and biometric information.[14] Genetic data is not named, but genetic information from a medical test fits comfortably within that definition. The regime is weak and narrow as it binds only companies and no one would call it adequate. But it does stand for a principle: some information is more dangerous than the rest, and should be handled more carefully.

The ***Personal Data Protection Bill, 2019*** would have carried that principle forward and strengthened it. Its definition of sensitive personal data expressly included genetic data, alongside health, biometric, sex-life, caste, and religious or political data.[15] Had it become law, India would have had for the first time an explicit statement in statute that genetic data is different.

It did not become law. The Bill was replaced by what became the ***Digital Personal Data Protection Act, 2023***, which drops the idea of sensitive personal data entirely. It recognises just one category "*personal data*", defined as "*any data about an individual who is identifiable by or in relation to such data*".[16] There are no tiers. Genetic data is not mentioned anywhere in the Act. Under the *2023 Act*, your whole-genome sequence and your office phone extension sit in exactly the same legal box and carry exactly the same protections.

This is the pivot of the whole paper. India did not simply fail to protect genetic data. India had already written that protection, in plain words, in its own *2019 Bill* and then took it out. On this issue the *2023 Act* is not a half-finished version of the *2019 Bill*; it is a step backwards from it.

---

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India). Available at: https://indiankanoon.org/doc/91938676/.

[14] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3 (India).

[15] The Personal Data Protection Bill, 2019, cl. 3(36) (India). Available at: https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.

[16] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 2(t) (India).

3.3 THE REPEAL THAT HAS NOT HAPPENED YET

The effect of that deletion is still in the future, which is why it has drawn so little notice. ***Section 44(2) of the 2023 Act*** removes ***Section 43A of the Information Technology Act, 2000***.[17] When that takes effect, the *2011 Rules* made under *Section 43A* fall away with it and the sensitive personal data category simply ceases to exist.

Timing is everything here. The ***Digital Personal Data Protection Rules, 2025*** were notified on 13 November 2025 and bring the law in gradually. Its core obligations notice and consent, security safeguards, breach reporting, limits on how long data is kept and when it must be erased, and the rights of individuals take effect on 13 May 2027.[18] On that date, India's only existing category of stronger protection for health and biometric information is repealed and the law replacing it has no such category at all.

One qualification is needed. The idea of "*sensitivity*" does survive in the *2023 Act* but not as a right you can claim. *Section 10* lets the Central Government label an organisation a "*Significant Data Fiduciary*", based partly on the volume and sensitivity of the data it handles; such an organisation then carries extra duties, including a Data Protection Officer, independent audits, and periodic Data Protection Impact Assessments.[19] So sensitivity has been downgraded from a quality of the information, which the affected person could enforce, to a trigger for a government label, which only the regulator can enforce, and only if the government chooses to apply it. Whether genetic data gets special treatment is now a matter of government discretion, not a legal entitlement; a much weaker guarantee, and the opposite of what the *2019 Bill* offered.

3.4 THE COLLECTION MACHINERY

If the protective architecture has been pulled down, the collecting architecture has been built up. Three developments stand out.

First, the ***Criminal Procedure (Identification) Act, 2022*** replaced the old ***Identification of Prisoners Act, 1920***, which allowed only fingerprints and footprints. The *2022 Act* allows the collection of "*measurements*" a word it defines to include biological samples

[17] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 44(2) (India). See also Section 44 in The Digital Personal Data Protection Act, 2023, Indian Kanoon. Available at: https://indiankanoon.org/doc/140541614/.

[18] The Digital Personal Data Protection Rules, 2025, notified 13 November 2025; see Press Information Bureau, DPDP Rules, 2025 Notified. Available at: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf.

[19] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 10 (India).

and their analysis.[20] The Act does not define "*biological samples*", does not rule out DNA, and does not limit the analysis to simple identification. It applies to anyone convicted, arrested or detained, with no minimum seriousness so even a minor arrest is enough. Consent is not required; in fact, resisting or refusing collection is itself an offence. The records can be kept for seventy-five years and shared through the **National Crime Records Bureau**. The Act is currently being challenged before the Delhi High Court.[21]

Every abstract point from the section above has a concrete match in this one statute. Permanence: The Act keeps samples for seventy-five years; for most people caught by it, that means life. Consent: The Act does away with it. Relational reach: A database of the genetic profiles of arrested people is also, in effect, a partial database of their relatives, people who have not been arrested, are not suspected of anything, and have no rights under the Act. A forensic database does not politely stop at the edge of the group it was meant to cover.

Second, the ***DNA Technology (Use and Application) Regulation Bill, 2019*** which would have regulated DNA labs and data banks was withdrawn from the Lok Sabha on 24 July 2023.[22] It had drawn steady criticism, including that its consent provisions were too weak and that it risked enabling caste and community profiling. Those criticisms were fair. But the Bill was not dropped in favour of something better: reporting at the time suggested the government's view that its main provisions had already been enacted through the ***Criminal Procedure (Identification) Act, 2022***. If that is right, the result is stark, the parts that authorise collection were kept, and the part that would have regulated it was thrown away.

Third, the **Genome India Project** was launched by the Prime Minister on 9 January 2025, after sequencing the whole genomes of 10,000 Indians from a wide range of population groups. The dataset has already turned up about 27 million rare genetic variants roughly 7 million of which appear in no existing global database and it is stored at the **Indian**

[20] The Criminal Procedure (Identification) Act, 2022, No. 11 of 2022, § 2 (India). See PRS Legislative Research, The Criminal Procedure (Identification) Bill, 2022. Available at: https://prsindia.org/billtrack/the-criminal-procedure-identification-bill-2022.

[21] Bar & Bench, supra note 6.

[22] PRS Legislative Research, supra note 5.

Biological Data Centre in Faridabad.[23] This is a real scientific achievement; the point here is narrower. Who may access that data, including researchers outside India is governed by the **Framework for Exchange of Data** (**FeED**) protocols under the ***Biotech-PRIDE Guidelines***,[24] and by the ICMR's National Ethical Guidelines for Biomedical and Health Research Involving Human Participants, 2017.[25] They give no enforceable rights to the 10,000 people whose genomes they cover, and the bodies that issued them can change them without going back to Parliament. India's flagship genomic dataset rests on policy, not law.

4. THREE FAULT LINES

The consequences of all this are easiest to see through three specific problems.

4.1 CONSENT

Data protection law leans heavily on consent, and the *2023 Act* is no different. Genetic data strains that model in two directions.

The first strain is about the idea of consent itself. Consent only means something if the person giving it knows what they are agreeing to. With genetic data, they often cannot. What a genome might be used for in twenty years is unknowable at the moment the sample is given and the information revealed does not stop at the person giving consent. Someone can agree to a test and, in doing so, expose information about a sibling who was never asked. Whatever the sibling's position is, it is not consent.

The second strain is more direct, and specific to India. Under the ***Criminal Procedure (Identification) Act, 2022***, consent is not merely weakened or assumed, it is removed. For everyone within that Act's reach, the consent machinery of Indian data protection law simply does not apply. It is hard to call a system consent-based when the single largest genetic collection the State is allowed to run is, by law, non-consensual.

4.2 OWNERSHIP & COMMERCIALISATION

Once a sample has been collected and analysed, who controls the resulting information,

[23] Department of Biotechnology, Genome India Project makes genomic data of 10,000 Indians available for public access. Available at: https://dbtindia.gov.in/dbtinmedia/genome-india-project-makes-genomic-data-10000-indians-available-public-access.

[24] Press Information Bureau, India Takes a Giant Leap in Genomics: Launch of Indian Genomic Data Set & IBDC Portals to Empower Global Research. Available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2091577.

[25] Indian Council of Medical Research, National Ethical Guidelines for Biomedical and Health Research Involving Human Participants (2017). For a commentary, see Indian Journal of Medical Research. Available at: https://ijmr.org.in/national-ethical-guidelines-for-biomedical-health-research-involving-human-participants-2017-a-commentary/.

the person, the lab, or the healthcare provider? Indian law gives no clear answer, and that silence creates real uncertainty about commercial use and sharing.

That question stopped being theoretical in 2025. 23andMe, a consumer genetics company holding the genetic profiles of about 15 million customers filed for Chapter 11 bankruptcy in the United States. Its database was treated as an asset of the bankrupt estate and put up for sale under court supervision. Regeneron Pharmaceuticals was named the winning bidder at about US$256 million in May 2025;[26] when the bidding was reopened it declined to raise its offer, and the assets were finally bought in July 2025 by TTAM Research Institute, a non-profit set up by the company's founder. A group of state Attorneys General, led by New York, sued to stop the sale, arguing that millions of customers' genetic information could not be auctioned off without their knowledge or consent.[27]

The episode answers the ownership question in the least reassuring way possible. When a company holding a genetic database collapses, who controls the data is decided not by the people it describes, nor by a regulator, but by insolvency law and the interests of creditors. India has no rule for this: under the *2023 Act*, a genetic database held by an Indian company is just personal data like any other, and nothing stops it being transferred in a business sale or a bankruptcy.

4.3 GENETIC DISCRIMINATION

Genetic information can reveal a raised risk of future illness. Without specific safeguards, that information can shape decisions about employment, insurance and other opportunities. It is tempting to file this under "*future risks*". It is not one.

In October 2023, 23andMe revealed that attackers had reached data belonging to about 6.9 million users, using login details leaked from other services.[28] The striking thing about that breach was not its size but its precision. The attacker put together and offered for sale, lists sorted by ancestry: roughly one million users identified as Ashkenazi Jewish, and a separate list of about 350,000 identified as of Chinese descent.[29] A group of state Attorneys

[26] Regeneron Pharmaceuticals, Regeneron Enters into Asset Purchase Agreement to Acquire 23andMe for $256 Million (May 19, 2025). Available at: https://newsroom.regeneron.com/news-releases/news-release-details/regeneron-enters-asset-purchase-agreement-acquire-23andmer-256.

[27] Attorney General James Sues 23andMe to Protect New Yorkers' Genetic Data, N.Y. Att'y Gen. (2025). Available at: https://ag.ny.gov/press-release/2025/attorney-general-james-sues-23andme-protect-new-yorkers-genetic-data.

[28] See 23andMe data leak, and contemporaneous reporting. Available at: https://en.wikipedia.org/wiki/23andMe_data_leak.

[29] 23andMe faces lawsuit as hackers sell information on users with Jewish heritage, Times of Israel (Oct. 2023). Available at: https://www.timesofisrael.com/23andme-faces-lawsuit-as-hackers-sell-information-on-users-with-jewish-heritage/.

General later settled bankruptcy claims from that breach for US$18 million.[30]

This is what genetic discrimination actually looks like and it is worth being precise about why it matters here. The harm was not that individuals were denied insurance or loans. It was that a genetic database was turned, directly, into a targeting list for an ethnic group. As the epigraph says, a leaked password can be changed and a leaked genome cannot: the 6.9 million people affected cannot revoke their ancestry or make the list forget them. For a country with India's history of caste and community classification and a statute authorising the forced collection and lifetime storage of samples from arrested people, this is not an incident to file away as a foreign curiosity.

5. COMPARATIVE PERSPECTIVES

Several countries have accepted that genetic information needs stronger protection than ordinary personal data.

5.1 THE EUROPEAN UNION: CATEGORISATION

The **GDPR** defines genetic data as personal data about a person's inherited or acquired genetic characteristics that gives unique information about their physiology or health.[31] It then places genetic data among the "*special categories*" of personal data under *Article 9,* whose processing is banned unless a specific condition is met.[32] The technique is categorisation: the law marks out a class of information and attaches stronger duties to it automatically, with no government decision required. This is exactly the technique the *2019 Bill* would have adopted and *the 2023 Act* abandoned.

5.2 THE UNITED STATES: TARGETED PROHIBITION

With no broad federal data protection law to draw on, the United States tackled genetic information through a targeted anti-discrimination law instead. The ***Genetic Information Nondiscrimination Act of 2008*** (***GINA***) bans discrimination based on genetic information in health insurance and in employment, and stops employers from requesting or requiring genetic information except in a few narrow situations.[33]

---

[30] Attorney General Sunday Announces $18 Million National Settlement with 23andMe Over Genetic Data Breach, Pa. Off. Att'y Gen. Available at: https://www.attorneygeneral.gov/taking-action/ag-sunday-announces-18-million-national-settlement-with-23andme-over-genetic-data-breach/.

[31] Regulation (EU) 2016/679, art. 4(13) (General Data Protection Regulation). Available at: https://gdpr-info.eu/art-4-gdpr/.

[32] Regulation (EU) 2016/679, art. 9(1). Available at: https://gdpr-info.eu/art-9-gdpr/.

[33] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881; see U.S. Equal Employment Opportunity Commission, The Genetic Information Nondiscrimination Act of 2008. Available at: https://www.eeoc.gov/statutes/genetic-information-nondiscrimination-act-2008.

The telling feature of *GINA* is its limit. It does not cover life, disability or long-term-care insurance, where providers may lawfully ask for and act on genetic test results.[34] Those are precisely the markets where a raised risk of serious illness matters most financially. If India borrows GINA's model, it should not borrow GINA's narrow scope.

5.3 THE UNITED KINGDOM: VOLUNTARY CODE

The United Kingdom handles the insurance question by agreement rather than by statute. The ***Code on Genetic Testing and Insurance (2018)***, agreed between the government and the Association of British Insurers, replaced an earlier arrangement.[35] Under the *Code*, participating insurers will never require or pressure an applicant to take a predictive or diagnostic genetic test, and may ask for the result of only one predictive test for Huntington's disease and even then only for life insurance policies above £500,000.[36]

The UK model is worth studying for a reason that is easy to miss: even a non-statutory instrument can deliver protection that is narrow, concrete and durable. That is directly relevant to India, because the *Genome India Project* is currently governed by exactly that kind of instrument. But the comparison also exposes a crucial difference between a code that spells out what may not be done, and a framework that spells out how access is granted. The *UK Code* restrains the powerful party; India's **FeED** protocols smooth the sharing. The second should not be mistaken for the protection the first provides.

5.4 WHAT THE COMPARISON YEILDS

No model is perfect. But all three countries accept the premise that Indian law now rejects: that genetic information is a distinct category and needs distinct treatment. They differ on technique, and each technique has a clear weakness. India is not yet in a position to choose among them because it has not yet accepted the premise, they all rest on.

6. RECOMMENDATIONS

The recommendations below are ordered by what each one requires, starting with those that need no change to the main law at all. The order is deliberate. The usual objection to reform is that it needs parliamentary time that is never available. Several of these do not.

---

[34] See National Human Genome Research Institute, Genetic Discrimination, noting that GINA does not cover life, disability or long-term care insurance. Available at: https://www.genome.gov/about-genomics/policy-issues/Genetic-Discrimination.

[35] HM Government & Association of British Insurers, Code on Genetic Testing and Insurance (Oct. 2018). Available at: https://www.gov.uk/government/publications/code-on-genetic-testing-and-insurance.

[36] HM Government, Code on Genetic Testing and Insurance: 3-year review 2025. Available at: https://www.gov.uk/government/publications/code-on-genetic-testing-and-insurance-3-year-review-2025/code-on-genetic-testing-and-insurance-3-year-review-2025.

6.1 ACHIEVABLE WITHOUT AMENDING THE ACT

First, treat genetic processors as Significant Data Fiduciaries. *Section 10* already lets the Central Government give an organisation this label based on the volume and sensitivity of the data it handles and any organisation whose main business is genetic data clearly meets that test. The label would immediately bring the extra duties described earlier. This needs a government notification, not a new law, and can be done before the Act even starts.

Second, use the rule-making power. *Section 40* lets the Central Government make rules to carry out the Act's purposes. Rules setting stronger security safeguards, retention limits and erasure standards for genetic data made under this existing power would restore much of what the deletion of the sensitive-data category removed, without waiting for an amendment.

Third, put the *Genome India Project* on a proper legal footing or, failing that, strengthen the rules that currently govern it. The FeED protocols should be backed by an independent oversight body with the power to refuse access, a published register of who has been granted access, and a way for participants to withdraw.

6.2 REQUIRING THE AMENDMENT

Fourth, restore the category. The Act should be amended to add a definition of sensitive personal data that expressly includes genetic data, following the model of *clause 3(36)* of the *2019 Bill*. This is the central recommendation, and it is a modest one: it simply asks Parliament to enact what the government itself proposed in 2019. It should be done before 13 May 2027, so that repealing the *2011 Rules* does not leave a gap with no protection at all.

Fifth, pass a genetic non-discrimination law covering employment and all kinds of insurance. *GINA* supplies both the model and the warning. An Indian law should reach life, health, disability and long-term-care insurance, as well as employment, and should ban both using genetic information and requiring a person to be tested. Given India's history of caste and community classification, and the proven ability of genetic databases to be sorted by ancestry, the ban should expressly extend to discrimination based on genetic markers of community or descent.

Sixth, rein in the ***Criminal Procedure (Identification) Act, 2022***. At the very least: define "*biological samples*"; limit permitted analysis to identification and forbid drawing out predictive or physical-trait information; require a judge's authorisation before DNA is collected; restore a seriousness threshold, so that arrest for a minor offence does not trigger collection; cut the retention period sharply from seventy-five years; and require samples

and profiles to be destroyed when a person is acquitted, discharged, or released without charge.

Seventh, tackle the family problem. No country has solved this, and India will not solve it in a single law but two steps are within reach. Consent forms for genetic testing should have to state, in plain language, that the test will reveal information about biological relatives. And familial searching of any State-held genetic database identifying someone through a relative's genetic profile should need its own separate legal authorisation, rather than being treated as just part of holding the database. Searching a database for relatives is a different power from simply holding it.

Eighth, ban the transfer of genetic data as an insolvency asset. Where an organisation holding genetic data goes bankrupt or is sold, the genetic data should not be transferable without fresh consent from each individual and otherwise it must be erased. This is the direct lesson of 23andMe, it has no equivalent in Indian law, and it can be done either through rules under *Section 40* or by amending the insolvency framework.

6.3 THE ORGANISING PRINCIPLE

The *2019 Bill*'s approach and the approach behind this paper's fourth recommendation is to name genetic data as a protected category. But naming a category, on its own, repeats the weakness that **De Hert** and **Papakonstantinou** identified in the GDPR. So, the guiding principle should be the one **Knoppers** proposed: where consent cannot bear the weight placed on it, the answer is not to demand more consent, but to place duties on institutions. This paper's recommendations are built that way. The duties fall on those who hold genetic data, not on the people who provided it because those people are precisely the ones who cannot know what they are agreeing to.

CONCLUSION

As genomic technology becomes part of healthcare, research and criminal justice, India faces a choice. It can keep treating genetic information as just another form of personal data or it can recognise that a genome is not like other data, and legislate accordingly.

That choice is not open forever. On 13 May 2027 the main provisions of the *2023 Act* take effect and ***Section 43A of the Information Technology Act*** is repealed taking with it the *2011 Rules* and the only category of stronger protection Indian law currently gives to medical and biometric information. From that day, unless something is done, the most sensitive information a person has will be protected no better than their postal address while a criminal-procedure

law lets it be taken without consent and kept for seventy-five years.

The promise of genomics is extraordinary, and this paper has never suggested otherwise. The **Genome India Project** has produced a dataset of genuine scientific value, and the case for genomic research in a population as diverse as India's is compelling. But that promise depends on trust and trust is built by institutions and destroyed by incidents. Once several million people learn that a database gathered for research or policing has been sorted by community and offered for sale, getting people to join the next project becomes far harder. Protecting genetic data is therefore not an obstacle to genomic research in India; it is the precondition for it.

It is often said that DNA is the blueprint of human identity. The metaphor is worth resisting partly because a genome is less a fixed blueprint than a set of instructions whose results depend on circumstance, but mainly because the belief that a person can be read off their genome is what makes genetic discrimination possible in the first place. The reason to protect genetic data is not that it reveals who a person truly is. It is that others will act as though it does.

BIBLIOGRAPHY

Cases

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

Legislation and Subordinate Legislation: India

2. The Digital Personal Data Protection Act, 2023, No. 22 of 2023.
3. The Digital Personal Data Protection Rules, 2025 (notified 13 November 2025).
4. The Criminal Procedure (Identification) Act, 2022, No. 11 of 2022.
5. The Information Technology Act, 2000, No. 21 of 2000.
6. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
7. The Identification of Prisoners Act, 1920 (repealed).

Bills

1. The Personal Data Protection Bill, 2019, Bill No. 373 of 2019.
2. The DNA Technology (Use and Application) Regulation Bill, 2019 (withdrawn 24 July 2023).

Legislation: Foreign and Regional

1. Regulation (EU) 2016/679, General Data Protection Regulation, arts. 4(13), 9.
2. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (U.S.).

Books and Journal Articles

1. Annas, George J., Privacy Rules for DNA Databanks: Protecting Coded "Future Diaries", 270 JAMA 2346 (1993).
2. Annas, George J., Leonard H. Glantz & Patricia A. Roche, Drafting the Genetic Privacy Act: Science, Policy, and Practical Considerations, 23 J.L. Med. & Ethics 360 (1995).
3. De Hert, Paul & Vagelis Papakonstantinou, The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? 32 Computer Law & Security Review 179 (2016).
4. Knoppers, Bartha Maria & Ruth Chadwick, Human Genetic Research: Emerging Trends in Ethics, 6 Nature Reviews Genetics 75 (2005).
5. Murray, Thomas H., Genetic Exceptionalism and "Future Diaries": Is Genetic Information Different from Other Medical Information? in Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era 60 (Mark A. Rothstein ed., Yale Univ. Press 1997).
6. Rothstein, Mark A., Genetic Exceptionalism and Legislative Pragmatism, 35(4) Hastings Center Report 27 (2005).

Official Publications and Guidelines

1. Department of Biotechnology, Genome India Project makes genomic data of 10,000 Indians available for public access.
2. HM Government & Association of British Insurers, Code on Genetic Testing and Insurance (October 2018), and 3-year review (2025).
3. Indian Council of Medical Research, National Ethical Guidelines for Biomedical and Health Research Involving Human Participants (2017).
4. Press Information Bureau, DPDP Rules, 2025 Notified (November 2025).
5. Press Information Bureau, India Takes a Giant Leap in Genomics: Launch of Indian Genomic Data Set & IBDC Portals.
6. U.S. Equal Employment Opportunity Commission, The Genetic Information

Nondiscrimination Act of 2008.

7. National Human Genome Research Institute, Genetic Discrimination.

Other Sources

1. PRS Legislative Research, The Criminal Procedure (Identification) Bill, 2022; The DNA Technology (Use and Application) Regulation Bill, 2019; The Personal Data Protection Bill, 2019.
2. Attorney General James Sues 23andMe to Protect New Yorkers' Genetic Data, New York Attorney General (2025).
3. Attorney General Sunday Announces $18 Million National Settlement with 23andMe Over Genetic Data Breach, Pennsylvania Office of Attorney General.
4. Regeneron Pharmaceuticals, Regeneron Enters into Asset Purchase Agreement to Acquire 23andMe for $256 Million (19 May 2025).
5. Golden State Killer: DNA and GEDmatch profile led police to wrong man before suspect Joseph James DeAngelo, Washington Post (27 April 2018).
6. We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans, Science (11 October 2018).
7. 23andMe faces lawsuit as hackers sell information on users with Jewish heritage, Times of Israel (October 2023).
8. Delhi High Court seeks MHA's response to plea against law allowing police to collect DNA, biometrics of accused, Bar & Bench.