GENETIC JUSTICE OR GENETIC SURVEILLANCE? A LEGAL INQUIRY INTO EXPANDING DNA DATABASES IN CRIMINAL INVESTIGATIONS

Ochaya Richard Martin[1], B COM LLB (hons), Department of Law, Marwadi University.

ABSTRACT

The increasing use of DNA databases in criminal investigations represents a significant technological leap in the administration of justice. These databases offer the promise of solving complex crimes, absolving the innocent, and improving the speed and accuracy of criminal identification. However, this forensic innovation also presents a paradox: the same tools that serve justice can easily slide into instruments of mass surveillance and rights violations if left unchecked. This article explores the legal, ethical, and policy dimensions of expanding DNA databases through a critical lens.

At the heart of this inquiry lies a pressing legal dilemma: do state-maintained DNA databases advance the goals of justice, or do they risk infringing upon individual privacy, bodily autonomy, and constitutional protections against arbitrary state action? By employing a combination of legal doctrinal analysis, comparative policy evaluation (focusing on India, the United States, and the United Kingdom), and key judicial decisions, this article unpacks the implications of unregulated or poorly regulated genetic data collection and retention practices.

Through an examination of the Indian DNA Technology (Use and Application) Regulation Bill, 2019 and relevant global jurisprudence, the article argues for a balanced approach—one that ensures forensic utility while upholding fundamental rights. It concludes by offering reformative recommendations aimed at establishing robust legal safeguards, procedural accountability, and ethical oversight in the collection, use, and storage of genetic information.

Keywords: DNA profiling, Genetic surveillance, Privacy rights, Forensic databases, Criminal investigations.

[1] B COM. LLB (hons), Department of Law, Marwadi University.

INTRODUCTION

DNA profiling has revolutionized criminal investigations in recent decades, providing forensic science with a level of accuracy that was previously unthinkable. How evidence is gathered, suspects are identified, and justice is administered has been completely transformed by the capacity to identify people almost with certainty based on their genetic composition. DNA evidence has solved long-standing cold cases, cleared wrongfully convicted individuals, and brought closure to crimes that would otherwise go unsolved. With the exception of identical twins, every person has a unique DNA profile that can be derived from minute biological traces like saliva, blood, hair, or skin cells. This is what gives it its power.[2]

Governments all around the world have created extensive DNA databases in order to utilize this forensic capability. These repositories hold the genetic data of people, including suspects, arrested people, convicted criminals, and occasionally even volunteers. The Combined DNA Index System (CODIS) has emerged as a key instrument in both federal and state investigations in the United States.[3] The National DNA Database (NDNAD) of the United Kingdom is one of the largest DNA databases in the world. Formalizing the collection, use, and storage of DNA profiles for both criminal and civil purposes is the goal of India's proposed DNA Technology (Use and Application) Regulation Bill, 2019.

However, the rapid extension of state-run DNA databases has brought up an important and pressing question: Are these genetic repositories becoming tools of genetic surveillance or are they a means of enforcing the law? DNA evidence presents significant threats to bodily autonomy, individual privacy, and the possibility of misuse in unregulated or authoritarian environments, even while it can be a formidable ally in the search for the truth. There are serious ethical and constitutional issues with the indefinite storage of DNA samples, the inclusion of people who have never been found guilty of a crime, and the absence of consent and supervision procedures.[4]

---

[2] *See generally* National Research Council, The Evaluation of Forensic DNA Evidence (1996); Erin Murphy, Inside the Cell: The Dark Side of Forensic DNA (2015).
[3] Federal Bureau of Investigation, *CODIS and NDIS Fact Sheet*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet.
[4] Human Rights Watch, *"Why Did You Leave Me There?" Abuses Against Children in Ugandan Police Cells* (Sept. 2014), at 49–51 (on database abuse risks); S. Krishnaswamy, Genetic Surveillance and Indian Democracy, 10 *Indian J. Const. L.* 1, 17–20 (2017).

In India, the situation is particularly complex. While the 2019 DNA Bill attempts to establish legal infrastructure for the use of DNA technology, it has been criticized for inadequate safeguards, vague consent provisions, and the potential to infringe upon the right to privacy as recognized in the landmark *Justice K.S. Puttaswamy v. Union of India*[5] decision. The absence of a comprehensive data protection law only heightens the stakes, making it imperative to scrutinize the balance between forensic utility and individual rights.[6]

This article seeks to undertake a **critical legal inquiry** into the rise of DNA databases in criminal investigations, with a focus on their legal, ethical, and policy implications. It begins with a brief overview of the scientific techniques underpinning DNA profiling and the architecture of national databases. It then analyzes the existing legal frameworks in the United States, the United Kingdom, and India, identifying areas of convergence and divergence in their approaches to privacy, consent, and regulation. The next section addresses the constitutional and ethical concerns surrounding the use and expansion of DNA databases, including potential violations of the right to privacy, the risk of mass surveillance, and the disproportionate impact on marginalized communities.

The article concludes with a set of policy recommendations aimed at ensuring that DNA databases serve the cause of justice without compromising civil liberties. It advocates for clear legislative safeguards, independent oversight bodies, and adherence to proportionality principles to prevent the misuse of genetic data in the name of law enforcement.

SCIENTIFIC AND TECHNOLOGICAL FOUNDATIONS

DNA profiling, also known as DNA fingerprinting, is a forensic method that identifies individuals based on variations in their genetic code. The fundamental principle is that although nearly 99.9% of the human genome is identical across individuals, certain regions—especially non-coding sequences—contain enough variability to distinguish one person from another. These regions serve as the basis for forensic DNA profiling.

The most widely used technique in modern criminal investigations is **Short Tandem Repeat (STR) analysis**. STRs are short sequences of DNA (typically 2–6 base pairs) that repeat in

[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[6] Ujwala Uppaluri, Re-imagining the DNA Technology Bill in the Post-Puttaswamy Era, *Economic & Political Weekly*, Vol. 55, No. 6 (Feb. 2020), at 14–17.

specific locations on the genome. The number of repeat units at a given locus can vary from person to person, creating a genetic profile that is statistically unique. STR analysis is highly reliable, even when conducted on small or degraded DNA samples, and is the basis for most national DNA databases, including CODIS in the United States.

In some cases, forensic experts use **Y-STR analysis**, which focuses on markers on the Y chromosome. Because the Y chromosome is passed unchanged from father to son, Y-STR testing is particularly valuable in cases involving male DNA (e.g., sexual assault with mixed samples) or when trying to trace paternal lineage. However, it is less discriminating than autosomal STRs because all male relatives in a paternal line will share identical Y-STR profiles.

Another emerging method is **Single Nucleotide Polymorphism (SNP) analysis**, which examines single-base changes at specific locations in the genome. Although SNPs are less informative on a per-locus basis, they are more stable and useful for analyzing highly degraded or old samples, and can provide ancestral or phenotypic information. SNP analysis underpins the newer field of **investigative genetic genealogy**, which has recently been used to identify suspects in cold cases by matching crime scene DNA to distant relatives in publicly accessible genealogical databases.

DNA databases are structured to store digital DNA profiles derived from such analyses, typically in the form of numeric codes representing alleles at various STR loci. These databases do not store entire genomes or raw DNA sequences. The **Combined DNA Index System (CODIS)** in the U.S., for instance, stores profiles generated from 20 core STR loci, and allows law enforcement agencies to search for matches between crime scene evidence and known individuals.

Entries into national DNA databases can vary widely across jurisdictions. In many countries, profiles of **convicted offenders** form the core of the database. However, several jurisdictions also collect and retain DNA from **arrestees**, even before a conviction is secured.

In some instances, DNA is collected from **suspects**, **volunteers**, or even **victims**, raising questions about consent and the scope of data retention. For example, the UK's now-modified policy once allowed indefinite retention of profiles from individuals who were never charged or convicted, which was declared a violation of the right to privacy by the European Court of

Human Rights in *S. & Marper v. United Kingdom*.[7]

A particularly contentious and growing trend is the use of **familial DNA searches**. These searches involve scanning a DNA database for profiles that are not exact matches but may belong to biological relatives of the person who left DNA at a crime scene. While this technique has aided in solving otherwise intractable cases, it has also sparked debate over the privacy rights of individuals who have never themselves provided a DNA sample, but become subjects of police interest by virtue of genetic proximity.

In summary, the advancement of forensic DNA technologies and their integration into criminal databases have significantly enhanced investigative capabilities. However, the same scientific tools that promote justice also raise profound concerns about privacy, consent, and the potential overreach of the state's forensic powers—issues which must be addressed through law and policy.

LEGAL AND POLICY FRAMEWORK.

In many jurisdictions, the quick incorporation of DNA profiling into criminal investigations has brought up difficult legal and policy issues. Although the technology has great potential to improve the administration of justice, regulations governing it varied greatly, reflecting varying views on civil liberties, privacy, and government monitoring. After giving a comparative summary of international regulatory regimes, this part delves deeply into India's changing legal system.

A. Global Overview

1. United States: CODIS and Federal/State DNA Collection Policies

The United States operates one of the most robust forensic DNA infrastructures in the world, cantered around the **Combined DNA Index System (CODIS)**. Administered by the FBI, CODIS allows for the comparison of DNA profiles collected at crime scenes with those in local, state, and federal databases. [8] DNA profiles are generated using 20 core STR loci, and

[7] Erin Murphy, *Familial DNA Searches: Legal and Ethical Implications*, 40 *Stan. L. Rev.* 29, 31–38 (2010).
[8] FBI, *CODIS and NDIS Fact Sheet*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet.

participants include all 50 states, the District of Columbia, and federal agencies.

Federal and state laws allow for DNA collection from **convicted offenders**, and many jurisdictions extend this to **arrestees**, even before trial or conviction. The Supreme Court upheld such practices in *Maryland v. King*[9], declaring that DNA swabs taken during booking procedures were constitutional and akin to fingerprinting. However, critics argue this blurs the line between identification and investigation, raising concerns about privacy and the presumption of innocence.

Oversight mechanisms and data retention policies vary across states. Some jurisdictions permit expungement of profiles upon acquittal or dropped charges, but the burden often lies on the individual to initiate the process, creating structural inequities.

2. UK; The Proportionality Doctrine and NDNAD

One of the first and still one of the biggest DNA databases in the world is the National DNA Database (NDNAD) in the United Kingdom. At first, the NDNAD was broad and encompassing, keeping profiles of everyone who was arrested, regardless of whether they were charged or convicted. [10] In the historic case of S. & Marper v. United Kingdom, the European Court of Human Rights ruled that the indefinite storage of DNA from people who have not been found guilty goes against their right to privacy as guaranteed by Article 8 of the European Convention on Human Rights. [11]

Following this ruling, the UK adopted a more **proportional and balanced framework**. The Protection of Freedoms Act, 2012 introduced time limits for retention, distinctions between adults and juveniles, and independent oversight by the Biometrics Commissioner. The UK model thus reflects a deliberate calibration between the utility of DNA evidence and individual civil liberties, underpinned by the proportionality doctrine—a key principle of human rights law.

3. European Union: Forensic Data Governance and GDPR

DNA profiling is governed by the General Data Protection Regulation (GDPR) and criminal

[9] *Maryland v. King*, 569 U.S. 435, 465 (2013).
[10] Nuffield Council on Bioethics, *The Forensic Use of Bioinformation: Ethical Issues* 28–36 (2007).
[11] *S. & Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, 48 Eur. Ct. H.R. 50 (2008).

procedure rules in the European Union. By enforcing requirements for data minimization, purpose limitation, and explicit consent, GDPR indirectly influences law enforcement practices even though its primary focus is on commercial and civilian data use.[12]

Forensic DNA data is treated as **"special category" personal data** under Article 9 of the GDPR, requiring higher thresholds of justification for collection and retention. Member states must ensure that biometric data used for criminal identification is accompanied by clear legislative authorization and subject to judicial oversight.

Additionally, the **Prüm Framework** allows for cross-border DNA data sharing among EU member states, raising concerns about harmonization of standards and inter-jurisdictional accountability.[13]

B. Indian Context

1. The DNA Technology (Use and Application) Regulation Bill, 2019

India's attempt to institutionalize forensic DNA regulation is embodied in the DNA Technology (Use and Application) Regulation Bill, 2019.[14]The Bill seeks to establish a National DNA Data Bank and a DNA Regulatory Board, and permits the use of DNA profiling in both criminal and civil matters. It proposes categorization of DNA profiles into distinct indices: crime scene, suspects, offenders, missing persons, and unknown deceased persons.

Despite its objectives of aiding justice, the Bill has drawn criticism for vague consent provisions, lack of judicial oversight, and potential for function creep—the repurposing of data for unauthorized surveillance or profiling.[15] There are no clear safeguards for expungement, nor are there specific standards for data retention and destruction.

2. Legal Loopholes in Consent, Privacy, and Oversight.

The lack of a thorough data protection law in India is a serious issue. The DNA Bill runs the risk of turning into a stand-alone surveillance framework in the absence of a comprehensive

[12] GDPR, Regulation (EU) 2016/679, art. 5.
[13] Council Decision 2008/615/JHA, 2008 O.J. (L 210) 1 (EU) [Prüm Decision].
[14] DNA Technology (Use and Application) Regulation Bill, 2019, Bill No. 73 of 2019, available at https://prsindia.org/billtrack/the-dna-technology-use-and-application-regulation-bill-2019.
[15] Vidushi Marda, The DNA Bill and the Potential for State Surveillance, *The Wire* (Sept. 2019), https://thewire.in/tech/dna-bill-surveillance.

privacy law. Additionally, it is unclear under what circumstances, with what procedural safeguards, and who may be forced to provide a DNA sample. Furthermore, because it has executive-nominated members and no judicial review process for profile insertion, retention, or deletion, the proposed DNA Regulatory Board lacks complete independence. Additionally, noticeably absent are grievance redress procedures and public awareness mechanisms.

3. Right to Privacy and Puttaswamy Judgment.

The Supreme Court's decision in *Justice K.S. Puttaswamy v. Union of India* recognized the **right to privacy as a fundamental right under Article 21 of the Constitution**[16], and laid out the test of **legality, necessity, and proportionality** for any restriction. The DNA Bill arguably fails to satisfy these standards due to its **overbroad scope**, **inadequate safeguards**, and **insufficient justification** for retention of sensitive biometric data.

Puttaswamy mandates that any intrusion into bodily integrity or informational privacy must be backed by a legitimate state aim and least-restrictive means—a threshold that India's DNA regulatory framework is yet to meet.

4. Existing Legal Provisions: CrPC and Indian Evidence Act

Indian criminal procedure already provides for the collection of bodily samples, including blood and hair, under Sections 53 and 54 of the Criminal Procedure Code (CrPC).[17]However, the legal status of DNA evidence remains underdeveloped. The Indian Evidence Act, 1872 does not contain specific provisions on the admissibility of DNA evidence, relying instead on judicial discretion under Section 45 (expert opinion).

Courts have generally accepted DNA as reliable, but concerns about sample contamination, chain of custody, and lack of accreditation for forensic labs persist.[18] Without clear procedural rules and statutory protections, the integrity of DNA evidence remains vulnerable.

[16] India constitution 1950.
[17] Code of Criminal Procedure, 1973
[18] *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India) (addressing involuntary narco-analysis and implications for bodily autonomy).

ETHICAL AND CONSTITUTIONAL CONCERNS

While DNA profiling holds immense promise for advancing justice, it simultaneously raises pressing ethical and constitutional issues. The integration of DNA databases into law enforcement frameworks often occurs without adequate scrutiny of how these technologies may infringe upon civil liberties, particularly **the right to privacy, bodily autonomy**, and **freedom from discrimination**. This section explores three core concerns: the erosion of privacy rights, the looming threat of mass surveillance, and the disproportionate impact on already marginalized communities.

A. Right to Privacy and Bodily Autonomy

1. Consent for DNA collection: voluntary versus coercive

The necessity (or lack thereof) of voluntary and informed consent is a fundamental ethical concern in DNA collection. DNA samples are frequently taken from people without their express agreement in numerous jurisdictions, especially when arrestees or other "of interest" are involved. [19] Coercive collection methods run the risk of eroding public confidence in law enforcement in addition to raising questions regarding bodily autonomy, a right acknowledged in Selvi v. State of Karnataka[20].

In India, the **DNA Technology (Use and Application) Regulation Bill, 2019** provides insufficient safeguards around consent. It allows for DNA collection from “suspects,” “victims,” and “persons associated with a crime scene,” with little clarity on when consent is truly voluntary versus legally compelled. The potential for abuse is especially high where individuals may not fully understand the legal consequences of compliance or refusal.

2. Inclusion of Innocents and Arrestees

Another key concern is the inclusion of individuals who have not been convicted of any offense-such as arrestees or mere suspects, into permanent DNA databases. The practice risks violating the presumption of innocence and stigmatizing individuals who may never face formal charges. In *S. & Marper v. United Kingdom*, the European Court of Human Rights

[19] Natalie Ram, Genetic Privacy After Carpenter, 105 *Va. L. Rev.* 1357, 1373–76 (2019).
[20] *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India).

condemned the blanket retention of DNA from unconvicted individuals as a breach of privacy.[21]

In Maryland v. King, the U.S. Supreme Court affirmed the use of DNA swabbing on arrestees, presenting it as a valid method of identification. [22]Scholars contend, however, that this broadens the surveillance network without accompanying accountability, particularly in light of the difficulties associated with expungement. There is a gap in legal protections in India because the proposed legislation does not specify how DNA profiles will be deleted after a person is found not guilty or released from custody.

3. Potential for Misuse and Profiling

With minimal oversight, DNA databases are vulnerable to **function creep**—the unauthorized use of data for purposes beyond the original intent, such as profiling individuals based on caste, religion, or political beliefs. The centralization of sensitive biometric data without clear statutory limits may enable **targeted surveillance or discriminatory law enforcement**.[23]

The absence of binding legal standards for the **collection, storage, and destruction** of DNA data magnifies the potential for misuse. India's lack of a comprehensive data protection law, even after the *Puttaswamy* judgment, creates a constitutional lacuna in the regulation of sensitive personal data.

B. RISK OF MASS SURVEILLANCE

1-Genetic Panopticon and the Aadhaar Analogy

DNA databases, particularly those that hold profiles of suspects, arrestees, and non-criminals, produce what academics refer to as a "genetic panopticon."[24]Much like Jeremy Bentham's architectural metaphor, such systems enable perpetual state observation of individuals without their knowledge. This risk is amplified when linked with other biometric identification schemes such as India's **Aadhaar system**, which already raises serious privacy concerns due to

[21] *S. & Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, 48 Eur. Ct. H.R. 50 (2008).
[22] *Maryland v. King*, 569 U.S. 435, 465 (2013).
[23] Vidushi Marda, The DNA Bill and the Potential for State Surveillance, *The Wire* (Sept. 2019), https://thewire.in/tech/dna-bill-surveillance.
[24] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 31 *Harv. J.L. & Tech.* 563, 598 (2018).

centralized storage and weak accountability mechanisms.

The Aadhaar case (*Puttaswamy II*) upheld the constitutionality of mandatory biometric enrolment but emphasized the need for proportionality and purpose limitation. Extending this rationale to DNA collection, any state-led genetic identification program must adhere to strict legal boundaries to prevent misuse[25].

2. Investigative Genetic Genealogy: The Golden State Killer Case

The advent of **investigative genetic genealogy (IGG)** presents new frontiers—and new ethical dilemmas. In the United States, the **Golden State Killer** was identified by uploading crime scene DNA to a public genealogy website, where a partial match led investigators to distant relatives.[26] While the case was hailed as a breakthrough, it relied on data shared voluntarily by individuals for recreational purposes, not law enforcement.

There are worries that law enforcement is circumventing conventional privacy safeguards by taking advantage of gaps in commercial terms of service by using third-party, open-access databases like GEDmatch. [27] Without stringent data usage regulations, identical techniques might be applied in India, transforming DNA matching into an unregulated monitoring tool.

C. RACIAL AND SOCIO-ECONOMIC DISPARITIES

1. Overrepresentation of Marginalized Communities

Empirical evidence from multiple jurisdictions suggests that DNA databases disproportionately reflect the genetic data of **marginalized communities**—particularly those subjected to higher rates of policing and arrest. In the UK, a 2018 report revealed that Black individuals were significantly overrepresented in the NDNAD. In the U.S., CODIS mirrors similar disparities due to racially biased policing practices.

This overrepresentation creates a **feedback loop**: increased policing leads to increased DNA collection, which in turn increases surveillance in already overpoliced communities. Such

[25] *K.S. Puttaswamy (Aadhaar-5J) v. Union of India*, (2019) 1 SCC 1 (India).
[26] Heather Murphy, *How the Golden State Killer Was Caught: A Step-by-Step Guide*, *N.Y. Times* (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/us/golden-state-killer.html.
[27] Natalie Ram & Christi Guerrini, *Genealogy Databases and the Future of Criminal Investigation*, 363 *Science* 880 (2019).

dynamics reinforce systemic inequities under the guise of scientific objectivity.

2. Amplification of Racial Bias through Forensic Tools

Far from being neutral, forensic tools can **amplify existing racial biases** in criminal justice systems. As scholar Erin Murphy notes, DNA evidence may carry an "aura of infallibility," masking its role in **reinforcing discriminatory enforcement patterns**. If investigatory focus is disproportionately applied to certain communities, false positives and wrongful accusations become more likely.

In India, where caste and class hierarchies often influence law enforcement priorities, similar risks abound. The deployment of DNA databases without anti-discrimination safeguards could further entrench these divisions.

CASE LAW AND JURISPRUDENTIAL TRENDS

Courts worldwide are increasingly battling the conflict between the goals of crime control and fundamental rights as the legal ramifications of DNA profiling become more complicated. The changing body of jurisprudence reflects efforts to strike a balance between the rights of individuals to privacy, dignity, and a fair trial and the state's interests in law enforcement. In addition to offering a comparative study of judicial techniques based on necessity and proportionality, this part examines landmark rulings from the Indian, European, and US courts.

A-INTERNATIONAL JURISPRUDENCE

1. Maryland v. King (United States)

In *Maryland v. King*, the U.S. Supreme Court upheld the constitutionality of collecting DNA samples from individuals arrested for serious offenses, even before conviction.[28] Writing for the majority, Justice Kennedy argued that DNA collection was akin to fingerprinting, a routine identification method, and served legitimate state interests.

However, the dissent, led by Justice Scalia, warned of a **slippery slope** into a surveillance state: "Because of today's decision, your DNA can be taken and entered into a national database — not because you are convicted, but merely because you are arrested." the decision thus

[28] *Maryland v. King*, 569 U.S. 435 (2013).

underscores a critical judicial divide: whether DNA collection is a benign identification technique or a profound intrusion on bodily integrity and privacy.

2. S. & Marper v. United Kingdom (European Court of Human Rights)

In contrast to *Maryland*, the European Court of Human Rights in *S. & Marper v. UK* held that the **indefinite retention** of DNA profiles from individuals not convicted of a crime violated Article 8 of the **European Convention on Human Rights**, which guarantees the right to respect for private life.[29]

The court emphasized that retaining biometric data from unconvicted individuals **lacked proportionality**, especially in the absence of mechanisms for review or deletion. It reasoned that the retention "casts the shadow of suspicion" over innocent persons, damaging their dignity and presumption of innocence. This decision prompted the UK to reform its **National DNA Database (NDNAD)** laws to introduce time limits and stricter criteria for retention.[30]

B. INDIAN LEGAL FRAMEWORK AND JUDICIAL REASONING.

1**. Admissibility and Evidentiary Value.**

Section 45 of the Indian Evidence Act, 1872, treats DNA evidence as a type of expert witness , and Indian courts have gradually begun to accept it in criminal prosecutions.
In State of Himachal Pradesh v. Rajiv Jassi, the Supreme Court upheld the idea that, as long a s the integrity of the collection and testing procedures is preserved, DNA data can serve as a powerful corroborating tool.[31]

Similarly, in *Selvi v. State of Karnataka*, while ruling against narco-analysis and polygraph tests on grounds of involuntary self-incrimination, the Court distinguished DNA collection as constitutionally permissible if obtained through consensual and non-invasive means.[32]The Court did, however, caution that procedures must uphold human dignity and bodily integrity, recognizing the right to privacy as implicit in Article 21 of the Constitution.

[29] *S. & Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, 48 Eur. Ct. H.R. 50 (2008).
[30] Protection of Freedoms Act 2012, c. 9 (U.K.).
[31] *State of Himachal Pradesh v. Rajiv Jassi*, (2016) 12 SCC 682 (India).
[32] *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India).

2. Lack of Procedural Safeguards

Despite increasing reliance on DNA evidence, Indian courts have yet to develop a comprehensive **judicial framework** addressing procedural safeguards, especially in the context of mass database creation under the **DNA Technology (Use and Application) Regulation Bill, 2019**. Questions concerning **retention**, **consent**, and **access control** remain judicially underdeveloped. Without binding precedent or legislative clarity, there is a risk of inconsistent practices across states and investigative agencies.

C. COMPARATIVE INSIGHTS: PROPORTIONALITY AND NECESSITY

1. Proportionality Doctrine in the EU and India

The **doctrine of proportionality** has been a cornerstone of European jurisprudence. As seen in *S. & Marper*, the ECHR insists that any interference with fundamental rights must be **necessary in a democratic society** and tailored to the legitimate aim pursued. This principle has inspired reforms in jurisdictions like Germany and the Netherlands, where DNA retention is limited by severity of offense, time-bound protocols, and judicial oversight.

India's Supreme Court, especially in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, has echoed these principles. The Court adopted a **four-pronged test**: legality, necessity, proportionality, and procedural safeguards. Applying this standard to DNA databases, any legislative or administrative action must be demonstrably the **least restrictive means** to achieve a legitimate law enforcement objective.

However, the **DNA Bill, 2019** does not meet these standards in its current form. It permits wide-ranging collection and storage of profiles without strong mechanisms for independent oversight or data minimization. The failure to incorporate proportionality into the statutory design makes it susceptible to constitutional challenge.

2. Consent and Voluntariness: Global Norms

The concept of consent is still up for debate in different countries. The EU's General Data Protection Regulation (GDPR) sets a high standard, categorizing genetic data as sensitive personal data that needs heightened protection, even though U.S. and UK regulations

frequently allow gathering from arrestees without authorization.[33]

A consistent threshold for consent in forensic DNA collection has not yet been adopted by Indian courts. Informed, explicit, and revocable consent would be necessary for a rights-protective strategy, particularly for non-criminal entry like volunteers or missing persons. There are serious moral and constitutional issues with the lack of such norms.

POLICY RECOMMENDATIONS AND REFORM

Although DNA databases are useful for investigations, their growth requires a corresponding development of legal protections to protect constitutional rights. Such technologies run the potential of turning into tools of surveillance rather than of justice in the absence of a strong regulatory framework. In order to guarantee the moral, reasonable, and rights-compliant application of DNA profiling technologies, this section describes important reforms in the areas of legislation, procedure, and public involvement.

A. LEGISLATIVE SAFEGUARDS AND OVERSIGHT AUTHORITY

The DNA Technology (Use and Application) Regulation Bill, 2019, although a step toward institutionalizing forensic DNA use, lacks substantive rights-based protections. To align with constitutional standards and global best practices, the following legislative reforms are essential:

1. Independent Oversight Body

An **autonomous and statutorily constituted oversight authority** must be established to regulate all aspects of DNA database operations—collection, storage, access, usage, and deletion. This body should comprise legal experts, human rights advocates, forensic scientists, and representatives from marginalized communities to ensure pluralistic governance.

The oversight authority should be vested with powers to:

- Conduct periodic audits of database use.

[33] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons (GDPR), art. 9.

- Approve inclusion of new entries, especially volunteers or arrestees.
- Hear and resolve grievances, including wrongful inclusion and data breaches.
- Order deletions of DNA profiles based on acquittals, exonerations, or successful privacy appeals.

This mirrors institutions like the **UK's Biometrics and Surveillance Camera Commissioner** and can enhance transparency, accountability, and public trust.

2. Clear Retention and Deletion Protocols

The law must clearly distinguish retention periods for:

- **Convicted individuals** (limited to serious offences with renewal provisions).
- **Arrestees** (profiles to be deleted unless charge results in conviction).
- **Volunteers and family members** (strict time limits and revocable consent).
- **Unidentified persons and deceased** (restricted to humanitarian purposes).

Automatic deletion mechanisms and user-notified expiration periods should be mandatory, in keeping with **data minimization principles** under international data protection norms such as the **GDPR**.

3. Explicit Consent Framework

The current framework presumes consent in most forensic contexts, blurring the line between voluntary cooperation and coercion. Future legislation must define and enforce a **tiered consent model** that differentiates between:

- **Voluntary consent**: Informed, written, and revocable.
- **Judicially authorized collection**: Based on reasonable suspicion and necessity.
- **Emergency situations**: Limited to narrowly tailored, time-sensitive investigations with post hoc review.

This ensures that **bodily autonomy**, a core tenet of the *Puttaswamy* privacy doctrine, is respected in practice.

B. Transparency, Accountability, and Access Control

Strong access controls must be codified to prevent unauthorized use of genetic information. Only **trained forensic personnel and investigators** with case-specific warrants should be permitted access to DNA databases. The use of such data must be **logged and subject to audit trails**.

Additionally, strict penalties, including imprisonment and fines. Should be imposed for:

- Unauthorized access or misuse.
- Cross-linking DNA data for non-forensic purposes (e.g., civil profiling).
- Failing to delete profiles as mandated.

These measures will discourage misuse and establish a deterrent framework for potential data breaches.

C. Public Awareness and Participation

A critical reform often overlooked is **public education and engagement**. DNA databases affect not only suspects and convicts but also volunteers, victims, and entire communities through **familial searches**. Therefore, transparency and civic participation must be central to the regulatory ecosystem.

Key initiatives should include:

- **Public awareness campaigns** to inform citizens of their rights and risks related to DNA profiling.
- **Informed consent templates** in multiple languages, easily understandable formats, and accessible online.
- **Right to be informed** of profile inclusion and right to seek deletion.

- **Citizen advisory boards** to review database policies and recommend improvements.

Greater literacy and agency can transform individuals from passive data subjects into informed rights holders.

D. Judicial Review and Civil Remedies

The legal framework should incorporate **judicial review mechanisms** to challenge inclusion or misuse of genetic data. Affected persons must have a **statutory right to approach High Courts** or a designated tribunal for:

- Deletion of data.
- Compensation for wrongful inclusion or misuse.
- Rectification of records and forensic errors.

Codifying these remedies reinforces **due process guarantees** and discourages arbitrary state action.

CONCLUSION

The rise of DNA profiling and national genetic databases marks a profound shift in modern criminal investigations. As a scientific tool, DNA evidence has the potential to revolutionize law enforcement, solving cold cases, identifying repeat offenders, and even exonerating the innocent. However, this forensic power cannot be divorced from the broader constitutional and ethical framework within which it operates. At its core, the question remains: Can the use of DNA databases truly serve the ends of justice if it compromises fundamental rights in the process?

This article has examined the dual nature of expanding DNA infrastructures, capable of both advancing justice and enabling surveillance. From the United States' CODIS to the UK's NDNAD, and India's proposed DNA Regulation Bill, legal regimes have struggled to draw boundaries that respect individual privacy, bodily autonomy, and due process. The absence of adequate consent mechanisms, independent oversight, and clear retention policies risks transforming tools of identification into instruments of unchecked state power.

Particularly in democracies, the use of such intrusive technology demands more than procedural compliance, it requires **democratic legitimacy**. Citizens must have confidence that their genetic information will not be weaponized against them or retained indefinitely without cause. Without transparency, accountability, and public engagement, even well-intentioned laws can erode the very freedoms they purport to protect.

Therefore, any attempt to institutionalize DNA profiling must be accompanied by strong legal safeguards: consent protocols, deletion rights, independent review bodies, and civil remedies for misuse. As affirmed by *Puttaswamy v. Union of India*, privacy is not a privilege, but a constitutional guarantee that must extend to our biological data as well.

REFERENCES / BIBLIOGRAPHY

STATUTES AND LEGAL INSTRUMENTS

1. The DNA Technology (Use and Application) Regulation Bill, 2019, Bill No. 52 of 2019 (India).

2. DNA Identification Act of 1994, 42 U.S.C. § 14132 (USA).

3. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU).

4. Code of Criminal Procedure, 1973, No. 2, Acts of Parliament, 1974 (India).

5. Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).

CASE LAW

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

2. *Maryland v. King*, 569 U.S. 435 (2013) (USA).

3. *S. & Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, 2008 ECHR 1581 (European Ct. H.R.).

GOVERNMENT & INSTITUTIONAL REPORTS

1. Human Rights Watch, *India: Draft DNA Bill Raises Serious Privacy Concerns* (2019), https://www.hrw.org/news/2019/07/01/india-draft-dna-bill-raises-serious-privacy-concerns.

2. NITI Aayog, *Responsible AI: Strategy for India* (2021), https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.

3. Central Bureau of Investigation (CBI), *Forensic Manual on DNA Profiling in Criminal Investigations* (2018) [on file with author].

4. Narcotics Control Bureau (NCB), *Standard Operating Procedures for DNA Evidence*

(2020).

SCHOLARLY JOURNALS AND ARTICLES

1. Natalie Ram, *Genetic Privacy After Carpenter*, 105 Va. L. Rev. 1357 (2019).

2. Saptarshi Mandal, *Surveilling the Body: DNA Profiling and the Law in India*, 14 Indian J.L. & Tech. 1 (2018).

3. Elizabeth E. Joh, *The Myth of Genetic Privacy*, 92 N.C. L. Rev. 1521 (2014).

4. Simone Biles & Ravi Venkataraman, *DNA Databases and the Criminal Justice System: Policy Challenges and Legal Gaps in India*, 89 Brook. L. Rev. 407 (2023).

5. Megan Graham, *Familial Searches and Forensic DNA: Ethical and Legal Considerations*, 32 Harv. J.L. & Tech. 197 (2019).