INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL EVIDENCE PRIVACY: THE ROLE OF DNA PROFILING, DATA STORAGE AND CHAIN OF CUSTODY IN MODERN INVESTIGATIONS

AUTHORED BY - AYUSH VISHWAKARMA

ABSTRACT

Digital evidence is particularly significant in today's criminal proceedings, which are a blend of science and law. DNA analysis is one of the most significant instruments since it helps extremely properly identify people. But DNA and other digital information are only useful if they're stored and used in a secure way. Storing data correctly helps protect sensitive information from being accessed, used, or changed by anyone who is not authorized to access, use, or alter it. Equally crucial is the "chain of custody," the whole record of how evidence is collected, transported, and introduced in court. An effective chain of custody increases people's confidence in the evidence and decreases their doubts about whether the evidence is true. DNA profiling, secure data storage, and strict chain of custody mechanisms all combine to bolster investigations, ensure fair trials, and keep a lid on things.

KEYWORDS- DNA Profiling, Digital Evidence, Data Storage, Chain of Custody and Privacy

INTRODUCTION

In the digital era today, criminal investigations are increasingly depending on high-tech equipment to create, keep, and review private data. Out of these, DNA testing has become one of the greatest ways to identify suspects, because it can link people to crime scenes with great accuracy. DNA data is incredibly personal, and it will live forever, unlike other sorts of proof. That makes me very concerned about privatization and profitization. In the context of an investigation, digital evidence must be used in a scientifically valid manner and be subject to robust legal guarantees of people's rights. In the current legal systems, the use of digital information by courts and police is becoming increasingly common; thus, there is a big challenge of how to solve crimes fast while also respecting people's privacy.

The integrity of digital evidence depends upon the chain of custody and secure mechanisms for data storage. Data storage protects private data from persons who should not be able to see,

ISSN: 2582-6433

change, or lose it. This preserves evidence for the investigation. However, chain of custody is a record of all the procedures involved in collecting, processing, and presenting evidence in a court of law. Anything that breaks this link makes the proof less dependable and less likely to be accepted. The reliability of investigations is a combination of DNA profiling, secure data storage, and chain of custody methods. They not only help the prosecution's case but also stop the incorrect people being convicted, keeping the courts fair. Thus, the parts' functions indicate how the privacy of digital proof is evolving and how science, technology, and law must work together to preserve the law in the present world.

CONCEPT OF DNA PROFILING

DNA profiling is a scientific technique employed to identify a person by their unique DNA. It is also known as genetic fingerprinting. DNA profiling is the most accurate way of identifying a person. This is because everyone has their own unique DNA code save for identical twins. Organic samples like blood, saliva, hair, or skin cells are gathered and then compared to parts of DNA that are very different from one person to another. These variants, known as short tandem repeats (STRs), are analyzed for identity determination, biological relationship establishment, or to link individuals to crime scenes.

DNA fingerprinting was a novel notion that revolutionized forensic science in the late 20th century. DNA profiling was a revolutionary concept, and it changed the world of forensic research in the late twentieth century. It was a good tool for police to solve crimes, to clear innocent individuals, and to present good proof in court. DNA profiling is different from other sorts of evidence, such as eye-witness statements or fingerprints, in that it is biologically certain. So, there is less margin for error. But there are also various ethics and privacy issues. DNA contains sensitive information about your health, ancestry, and genetic traits. If not properly used or controlled, it could be used against the rights of individuals. DNA profiling is scientific, moral, and legal. "Strong protections around data storage, chain of custody, and judicial oversight need to be in place." These are the scenarios where science, law, and privacy intersect in DNA profiling. And it is also the future for justice systems everywhere.

SCOPE OF DNA PROFILING

1. Criminal Investigations and Forensic Identification

Today DNA profiling is the most essential portion of investigation science. It provides the police with the most accurate approach to link suspects to crime areas when investigating

ISSN: 2582-6433

crimes. If you collect samples of blood, saliva or hair from the crime scene and compare them to a suspect's DNA profile, you can be certain that they are involved. This is more scientifically certain, and hence it does not depend upon conjecture or eyewitness experiences, which are not always accurate. DNA profiling can be effective when information held for years is still informative. It plays an important role in criminal justice, helping to bring more cases to justice, deter crime, and increase confidence in the investigation process.

2. Exoneration of the Innocent

One of the greatest benefits of DNA profiling has been the exoneration of those falsely convicted of crimes. DNA evidence has led to the overturn of many cases across countries where the accused has been shown to have had no involvement. This demonstrates the potential of DNA profiling in the prevention of miscarriages of justice. The provision of unassailable scientific proof ensures that innocent persons are not convicted of crimes they did not commit. For instance, the Innocence Project in the United States has cleared hundreds of people using DNA testing. Thus, DNA profiling is a weapon not only of conviction, but it also protects the basic idea of justice that no innocent man should suffer.

3. Paternity and Family Disputes

DNA profiling also has a very important role in criminal law and civil law. For example, it is used in paternity, property, and custody of children matters. DNA evidence is used in court to prove beyond any question that two people are related by blood. DNA testing can help resolve the parentage problem and save costly and time-consuming judicial battles. It can also help in the hunt for legitimate heirs in case of inheritance disputes. It also covers cases where DNA profiling may be used to establish biological ties or to resolve concerns of identification following an adoption. DNA profiling provides scientists with actual proof, removing doubt and making family law more just.

4. Disaster Victim Identification

In cases of large-scale disasters such as earthquakes, tsunamis, plane crashes, or conflicts, identification of casualties poses a difficult task. DNA profiling is a proven method to connect remains to family members and provide closure to grieving families. DNA from teeth or bones can establish identity, even when remains are extensively damaged or unrecognizable. DNA profiling is regularly used by international organizations and governments during humanitarian operations to assist in the correct identification of victims. Hence, its position in crisis

ISSN: 2582-6433

management is particularly critical as it combines science with compassion, helping societies to overcome catastrophes.

5. Medical and Genetic Research

DNA profiling is not only utilized for forensic purposes but also has a significant function in medical and genetic research. Scientists employ DNA profiling for the study of genetic abnormalities, inherited diseases, and community genetics. This helps to provide tailored care, where a person's therapy is based on their genes. But there are privacy concerns about the scope: the genomic data can reveal sensitive information about health risks and hereditary features. There is a great deal of promise for it to enhance health care, but there have to be strict regulations to avoid misuse. DNA profiling thus crosses the boundary between law, science, and medicine and has uses outside investigations.

6. Immigration and Citizenship Cases

The use of DNA profiling in immigration and citizenship disputes is increasing day by day. DNA testing is scientific proof when people lie about biological relationships to gain admission or citizenship. It is also utilized in rules around cross-border adoptions to make sure children are placed with the right guardians. It makes immigration operations more efficient but also raises ethical concerns about consent and privacy. DNA profiling in immigration has two faces. It offers legal clarity but must be used with care to respect the rights of persons.

7. Military and National Security Applications

DNA profiling is used by the military and national security organizations to identify soldiers and keep databases safe and to find missing personnel. Testing DNA can help identify dead in war zones and make sure they are buried correctly. It also helps to keep the country safer by preventing identity theft and better border control. But this is a tricky issue because massive DNA databases that governments have can be used for surveillance and other unpleasant stuff. C. Military Uses of DNA Analysis In military applications of DNA analysis, the balance between security needs and the right to privacy must be resolved.

8. Ethical and Privacy Challenges

DNA profiling has certain utilitarian applications, but its real value is in the moral problems it raises. DNA holds a wealth of personal information that could be exposed if not treated with care. Problems include genetic discrimination and illegal access and misuse by government or

ISSN: 2582-6433

corporations. Consent is a moral issue. Should people be compelled to provide DNA evidence for investigations like this? The problems need strong legal frameworks for DNA profiling, including data privacy regulations and judicial control, to ensure that it is a weapon of justice and not an infringement of fundamental rights.

9. International Legal Standards

In different nations there are different regulations governing DNA testing. Genetic data is more protected under the EU regulation General Data Protection Regulation (GDPR). India has regulations on the use of DNA. These are the Evidence Act and the proposed DNA Technology Regulation Bill, 2019. In the US, the Constitution prohibits citizens from being searched without a valid reason. That is why international rules govern how much DNA testing is done and how evidence is collected, stored, and presented in court. Comparing the models reveals common ideas and unique difficulties, emphasizing how vital DNA privacy is worldwide.

10. Future Prospects in AI and Big Data

"DNA analysis will be useful in the future when combined with AI and big data analytics." AI can also help with DNA studies, looking for complex patterns and speeding up identification. But this also raises new issues such as predictive policing and genetic monitoring, where DNA information can be used to forecast people's behavior or health conditions. These technologies have the potential to make things faster and easier, but they could also be an infringement of people's rights and privacy. And there will need to be a balance struck between new ideas and guidelines for the future of DNA profiling. This is to ensure that scientific advancement does not harm morals.

PRIVACY CONCERNS IN GENETIC DATA COLLECTION

The collecting of genetic data, in particular in the form of DNA profiles, has become a mainstay of modern forensic, medical, and administrative practice. Its power to give accurate identification and to uncover biological links is priceless. But the torrent of genetic information raises serious privacy issues. Unlike other identifiers, DNA contains sensitive information relating to health predispositions and ancestry and blood links and is therefore especially vulnerable to exploitation.

The security of data is a crucial issue. There are DNA databases kept by the government, hospitals, and private businesses and means to get into them. Unlike passwords or ID numbers,

ISSN: 2582-6433

genetic information can't be changed once it's been stolen. People take a risk with their lives when they gain access to this type of material without authorization. You might observe them or use them. This permanence highlights the necessity of strong encryption, stringent access controls, and unambiguous accountability guidelines.

Genetic bias is another significant topic. Employers, insurers, or governments could misuse the genetic information to decide who qualifies, what insurance to cover, or who to recruit. For example, they may be excluded from insurance or charged more if a DNA test shows a risk of certain diseases. These sorts of things are unjust and unequal and turn genetic privacy into a civil rights issue.

Getting consent and freedom for collecting genetic data is considerably difficult. When DNA is shipped off, people don't have much control over what happens to it. In criminal investigations, samples may be taken from suspects or family members under duress, raising ethical issues with non-voluntary involvement. Data can also be shared between jurisdictions without the knowledge or consent of the individuals whose DNA is stored. This breeds distrust in institutions. The scenario becomes more stressful when family members are located. Additionally, DNA profiling may unintentionally reveal parental identities or put family members at the center of criminal investigations. While this method aids in the capture of criminals, it also meddles in private family affairs and raises concerns about our right to privacy in general.

Lastly, these worries are made worse by the sharing of data from other nations. Laws vary greatly between nations. Strict privacy rights are required by the General Data Protection Regulation (GDPR) and similar laws around the world, while some regions might not have such laws. Therefore, persons may be at danger of exploitation due to lax regulations when genetic information is exchanged across borders. In conclusion, there are numerous advantages to acquiring genetic data, but there are also numerous privacy issues. Stronger legal and moral standards are required in view of the issues of illegal access, discrimination, lack of authorization, interference by family members, and disparate foreign safeguards. Data security is only one aspect of genetic privacy. It also entails protecting people's liberties and rights as well as their trust in the law and science.

ISSN: 2582-6433

LEGAL FRAMEWORK GOVERNING DNA EVIDENCE

1. Admissibility under the Indian Evidence Act

The Indian Evidence Act of 1872[1] provides the many sorts of expert evidence that can be given in the court. Section 45 empowers judges to have regard to expert evidence in scientific areas such as DNA fingerprinting. In the beginning, especially with respect to paternity disputes, Indian courts were cautious. Section 112 made a child born during marriage valid. In Gautam Kundu v. State of West Bengal[2], the Supreme Court has said that privacy and dignity are very important and DNA tests cannot be done without consent. However, in Nandlal Wasudeo Badwaik v. State of Maharashtra[3], the Court observed that the only method to confirm the paternity was through DNA evidence. They changed the law, against what should have happened even. What this history shows is the evolution of the idea of admissibility in the struggle between scientific certainty and legal presumption.

2. Criminal Procedure Code and Forensic Sampling

According to the Code of Criminal Procedure, 1973[4], the police may gather biological samples during the course of investigations. The major constitutional question is whether the requirement of providing DNA would be against Article 20(3), which says that no person shall be compelled to produce evidence against himself. In Selvi v. State of Karnataka[5] (2010), the court had clarified that testimonial obligation does not encompass DNA or any physical evidence. So, if you take the necessary measures, you can take a DNA sample. It reconciles the use of DNA for investigations with the constitutional rights of individuals. It permits judges to rely on DNA evidence without breaching basic rights.

3. Reliability and Expert Testimony

DNA evidence must be supported by expert testimony to be proven reliable. The courts think about the functioning of a lab, the chance of contamination, and the way to interpret statistics. Before DNA, the Court drew a distinction between physical evidence and testimonial pressure (State of Bombay v. Kathi Kalu Oghad)[6]. This case was a precursor to later decisions on DNA. The Madras High Court in Kattavellai, Devakar v. State of Tamil Nadu (2025)[7], underlined the

[1] Indian Evidence Act, 1872, Act No. 1 of 1872, India
[2] Gautam Kundu v. State of West Bengal, AIR 1993 SC 2295
[3] Nandlal Wasudeo Badwaik v. State of Maharashtra, (2014) 2 SCC 576
[4] Code of Criminal Procedure, 1973, Act No. 2 of 1974, India
[5] Selvi v. State of Karnataka, (2010) 7 SCC 263
[6] State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808
[7] Kattavellai @ Devakar v. State of Tamil Nadu, 2025 INSC 845 (SC)

ISSN: 2582-6433

importance of the chain of ownership and the dependability of the expert. This shows how the courts view the scientific credibility of DNA evidence very highly, protecting the process.

4. Constitutional Right to Privacy

DNA testing threatens the right to privacy protected under "Article 21 of the Indian Constitution"[8]. The Supreme Court in Sharda v. Dharmpal (2003)[9] has also held that the medical testing of DNA tests was admissible if they were reasonable. Then came the important verdict in K.S. Puttaswamy v. Union of India (2017)[10] that changed the rules of the game for DNA evidence by holding privacy to be a fundamental right. Courts now ensure that the collection of DNA is done legally, fairly, and with respect for an individual's right to privacy but also remains relevant to investigations.

5. DNA Technology Regulation Bill, 2019 (India)

India has passed the DNA Technology (Use and Application) Regulation Bill to regulate DNA labs, oversee databanks, and protect the privacy of people. The bill would require consent, lab approval, and consequences for abuse of the system. Though not an act, it is a sign that India is seeking to adopt the best practices across the world. Its passage would clarify the legislation on admission, consent, and protections. This will guarantee that DNA evidence is scientifically and legally sound.

6. International Standards: GDPR (EU)

Genetic information is categorized as "special category data" under the European Union's General Data Protection Regulation (GDPR) and requires specific consent and additional protections. Article 9 prohibits the processing of genetic data, unless it is authorized by law or consent. In S & Marper v. UK (2008)[11], the European Court of Human Rights held that the blanket retention of DNA profiles of innocent persons constituted a violation of Article 8 (Right to Privacy). The case has modified the law in the UK, and so the retention is subject to more stringent time limits. As such, the GDPR provides a universal standard for the protection of genetic privacy.

[8] Constitution of India, art. 21
[9] Sharda v. Dharmpal, (2003) 4 SCC 493
[10] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
[11] S. and Marper v. United Kingdom, [2008] ECHR 1581, Applications nos. 30562/04 and 30566/04

ISSN: 2582-6433

7. UK National DNA Database and Safeguards

There are some huge DNA libraries. One is in the UK. The concept of retaining profiles of persons who were declared not guilty was initially criticized, but the Protection of Freedoms Act was amended in 2012 to only keep profiles of people who were found guilty. In the 2006 case R v. Bates the courts accepted DNA evidence but noted that it should only be retained if necessary. The UK system also highlights how laws safeguard evolution to ensure human rights are protected while still arresting criminals. This prevents the use of DNA databases for mass surveillance.

8. US Legal Framework – Reliability and Daubert Standard

In the US, DNA evidence must meet the scientific standards established by the case Daubert v. Merrell Dow Pharmaceuticals (1993). The courts are looking at matters like peer review and methodologies and mistake rates." People v. Wesley (1988, New York)[12] was the first case to admit DNA evidence, setting precedent. Federal law allows the FBI to continue to access the national DNA database, CODIS. US courts have insisted on scientific rigor, and only DNA evidence from methods that have been vetted and validated will be included.

9. Chain of Custody and Procedural Integrity

Courts everywhere emphasize chain of custody. Any breach vitiates admission. The need for adequate documentation came up in the case of Thogorani alias K. Damayanti v. State of Orissa (2004)[13] in India. US courts also need proof of custody before DNA evidence may be admitted. Judicial emphasis on sealing, labeling, and transport integrity maintains evidence integrity and ensures dependability. Chain of custody is therefore the cornerstone of procedural integrity in DNA evidence.

10. Future Challenges – AI, Big Data, and Genetic Surveillance

Emerging technologies such as AI-enabled DNA analysis provide new legal questions. Predictive police and genetic genealogy (U.S. Golden State Killer case, 2018) are contributing to the investigation of crimes but threaten personal privacy. First, it is the courts' concern whether these uses are consistent with fundamental rights. It is difficult to strike the correct balance between rights and innovative ideas. "In the future we should regulate AI and big data so that genetic monitoring doesn't happen and scientists can continue to grow."

[12] People v. Wesley, 533 N.Y.S.2d 643 (App. Div. 1988)
[13] Thogorani alias K. Damayanti v. State of Orissa, 2004 Cri LJ 4003 (Ori HC)

ISSN: 2582-6433

DATA STORAGE MECHANISMS FOR DIGITAL EVIDENCE

Digital evidence that must be stored to ensure integrity, privacy, and convenience of access includes DNA profiles, electronic records, and forensic data. The principal technique to safeguard information from being used or changed by anyone who is not allowed to do so is to keep it in secure digital locations that use encryption, access controls, and audit trails. Evidence is generally held in central systems operated by the police or by licensed forensic laboratories. Repositories of this sort use several methods of data storage, such as numerous copies on cloud computers, to ensure that data is not lost in the event of hardware failure or a cyberattack. Chain of custody mechanisms are used in storage systems to ensure that any access, transfer, or modifications are logged and traceable. Another thing hashing does is it creates digital marks of data. These can be used by investigators to see if evidence has been modified. Digital evidence needs to be stored securely, and courts are increasingly asking for evidence of these measures before they would allow the evidence to be utilized.

Barring technical measures, data storage systems should conform with the legal and ethical frameworks for privacy protection. Highly sensitive evidence like DNA profiles or biometric data is treated as highly personal data and must comply with data protection legislation such as India's proposed Digital Personal Data Protection Act, 2023; the EU's GDPR; and sector-specific forensic standards. These rules have limited retention durations, purpose-specific use, and strong consent requirements. Role-based access control is currently in place in modern storage systems, so only authorized individuals can see or handle evidence. They are also looking into the use of blockchain technology to create tamper-proof records of evidence handling that can help increase confidence in the judicial process. Simultaneously, international collaboration implies the need for harmonized standards, as it may be necessary to exchange evidence across countries. Therefore, the existing techniques of storage are not only technical solutions but are part of the wider legal ecosystem that attempts to balance the necessity for inquiry and respect for individual rights. Data storage systems use encryption, redundancy, blockchain, and compliance with privacy law to make digital evidence reliable, admissible, and respectful of human dignity.

CYBERSECURITY CHALLENGES IN EVIDENCE PRESERVATION

1. Risk of Unauthorized Access

One of the primary issues in preserving the digital evidence is the risk of unauthorized access to the evidence. These data (e.g., DNA profile, fingerprint, digital forensics) are typically

ISSN: 2582-6433

preserved in evidence repositories. These systems could be exposed to hackers or other individuals who shouldn't be there if not adequately secured. Proof can be copied, altered, or leaked by those who should not be able to, making it less dependable. If the court is not satisfied with the truth of the information, the court may refuse it. To avoid this, companies should use strict monitoring systems, access controls, and encryption. The difficulty is that you have to make it easy for investigators to use but also prevent it from being exploited.

2. Data Breaches and Leakage

Data leaks are another huge worry. Cyberattacks potentially provide a treasure trove of forensic data for crime networks or the public. But digital evidence may be copied and sent right away, making breaches far more damaging. But once evidence is out there, you can't take it back. And abusing evidence could undermine continuing investigations. Breaches cause people to lose faith in the judicial system because they are scared their personal information may be shared. Government entities need to put in place breach response protocols, encryption, and intrusion detection tools. As hackers get smarter and smarter all the time, it's impossible to block them completely. It definitely shows how important it is to keep upgrading and paying attention.

3. Tampering and Manipulation Risks

Digital evidence can be manipulated. Even small things, like modifying timestamps or information, might raise questions about reliability. Unlike tangible evidence, digital files can be changed with no evident traces. This is why cybersecurity protections are critical. Methods such as hashing, audit trails, and digital signatures are used to show that evidence has not been changed. The difficulty is to make sure that these measures are used consistently throughout the handling of evidence. If tampering is found, courts may toss out the evidence, torpedoing charges. If it is to keep its evidentiary value, the trick is to make it tamper-proof.

4. Weak Authentication Systems

The first line of defense against those who shouldn't be here are authentication techniques. Evidence repositories are vulnerable to hacking due to weak passwords, outdated methods of logging in, and no multifactor protection. Cyber criminals often use these vulnerabilities to get access. Courts require agencies to demonstrate that the evidence could only have been accessed by authorized personnel. "People are less convinced about preservation, and there are questions of integrity when there is weak authentication." Modern systems require biometric verification,

ISSN: 2582-6433

multi-factor security, and role-based access controls. The tricky thing is implementing these processes without slowing down investigations.

5. Cloud Storage Vulnerabilities

Due to their efficiency and scalability, digital data are increasingly stored in cloud systems. But there are also hazards with cloud storage, such as data ownership, outside attacks, and data theft. If the servers are in other countries, the cloud data may be subject to the legislation of other nations. There are privacy and legal issues here. The government wanted to check that the cloud service providers it was using to protect data were following the law and strong encryption requirements. The trick is to mix the ease of cloud storage with the need for solid legal and security protections.

6. Insider Threats

Insider threat is dangerous since it comes from someone who has legitimate access to the system. Evidence may be used by employees, investigators, or technicians for personal advantage, subversion, or misconduct. External controls are harder to spot and less effective in preventing insider exploitation. Audit trails, monitoring systems, and tight role-based access can reduce the threat of insiders. But these procedures need to be evaluated frequently, and there needs to be cultural understanding within the firm. Insider threats show that cybersecurity is a human concern, not only a technological one; from an ethical point of view, training and accountability are crucial aspects.

7. Cross-Border Data Sharing Issues

Digital proof must always be sent from one country to another, but it is especially important when crimes happen across lines. On the other hand, every country has its own laws and safety guidelines concerning hacking. They share evidence of the abuse, but because the regulations aren't as stringent in other nations. This makes it harder to ensure that proof is admitted and people’s privacy is protected. Agencies depend on treaties, agreements, and agreed-upon standards to guarantee that if evidence is to be transferred, it can be secured. It's hard to find a good balance between working with other countries and protecting national freedom and power. "Sharing across borders without strong safeguards could hurt investigations and people's rights."

ISSN: 2582-6433

8. Retention and Deletion Challenges

It is very important to keep and delete proof correctly. Private rights can be violated by keeping proof longer than needed. It could hurt cases if it were erased too soon. Rules for data keeping in cybersecurity systems must meet government standards. Accidental or illegal deleting should not be able to happen with automated deletion tools. It's difficult to find a suitable middle ground between the interests of privacy and research." Agencies must certify that evidence was preserved for the relevant time period and was not removed without permission. So regulations concerning deleting and retaining are very important for cybersecurity as well as for legal admissibility.

9. Emerging Threats from AI and Malware

New problems: Artificial intelligence and super-complex viruses. Digital evidence can be altered to disguise AI-generated phony files as real. Malware can also get into forensic databases and alter or delete evidence. These risks are ever-changing, and standard defenses don't work. The authorities need to utilize the most recent cybersecurity techniques to combat these dangers, such as AI-enabled monitoring systems. The truth is, cybercriminals are growing smarter and smarter in how they do things. However, as new threats emerge, cybersecurity must also evolve to ensure proof integrity.

10. Balancing Privacy and Security

Maintaining the security of information in cybersecurity can be difficult because of the requirement to balance privacy rights and investigations. There are just too many ways that too much surveillance or hanging on to information for no good reason might violate individual rights. And if the protections are not robust enough, evidence can be destroyed. The courts highlight proportionality: the evidence must be safeguarded without infringing on people's privacy. "Agencies need to write rules that protect people but also respect their rights. As technology changes, the right mix matters. Privacy and safety are not mutually exclusive; both are essential for trustworthy legal systems.

COMPARATIVE ANALYSIS: GLOBAL APPROACHES TO DNA PRIVACY

1. European Union – GDPR and Human Rights Approach

The European Union regards genetic data as the most sensitive data under the General Data Protection Regulation (GDPR). DNA data is classified as "special category data" and

ISSN: 2582-6433

processing is only permitted with explicit agreement or a strong legal basis. The GDPR underlines the need of necessity, proportionality and purpose limitation. This would ensure that DNA information is not permanently stored and only collected for legitimate purposes such as criminal investigations or medical research. It is also protected by the right to privacy, since the European Court of Human Rights ruled that it is against the right to privacy to hold DNA data of innocent individuals for too long. The European Union is built on the premise that everyone has rights and these rights include the respect and the freedom of each person. It provides a universal standard for protecting DNA privacy in a world where technology is getting better and better. It combines strong legislative protections with strict court control.

2. United States – Balancing Law Enforcement and Privacy

The U.S. has created a two-pronged approach to DNA privacy. DNA evidence, on the other hand, is commonly employed in criminal investigations and is supported by national databases such as CODIS (Combined DNA Index System). Law enforcement officials say DNA is helping them solve crimes and clear innocent people. On the other hand, privacy concerns are protected by constitutional protections, most notably the Fourth Amendment against unreasonable searches. Courts have wrestled with whether mandatory DNA collection violates privacy rights, typically allowing its collection from convicted offenders but on a more restrictive basis for those in custody. The U.S. model combines the strength of the DNA tool for public safety with constitutional safeguards. But other approaches, such as genetic genealogy, have raised new privacy concerns because they include the use of consumer databases of DNA for investigations.

3. United Kingdom – National DNA Database and Reform

The UK has one of the world's largest DNA databases and was the first to face criticism for keeping profiles of people who were never charged or were acquitted. But concerns about mass monitoring and privacy abuses led to modifications under the Protection of Freedoms Act that tried to limit retention to convicted offenders and to set clear limitations on retention periods. The UK approach is an illustration of how human rights considerations influence legal systems. DNA is still a powerful weapon for law enforcement, but privacy safeguards have been put in place to avoid its exploitation. The British approach increases friction between effectiveness of criminal detection and respect for individual rights. This indicates that big scale databases can work but need to be complemented by rigorous retention policies and independent control to retain public trust.

ISSN: 2582-6433

4. India – Emerging Frameworks and Privacy Challenges

India is currently in the nascent stage of discussing DNA privacy. DNA evidence is allowed under the Indian Evidence Act in the realm of expert testimony, but the DNA databases are not regulated by any specific law. The proposed DNA Technology (Use and Application) Regulation Bill aims to set standards for laboratories, databanks and permission procedures. Indeed, the Supreme Court's acknowledgment of privacy as a basic right in 2017 has fueled further discussions on genetic data. India must contend with issues including balancing the needs of investigation with privacy, consent and misuse in the face of fast technology innovation. There is no fully legislated framework thus practices differ and this raises questions about consistent safeguards. The Indian experience highlights the challenge of implementing effective privacy protections in a system where technology is ahead of legal legislation.

5. Global Trends – Harmonization and Future Challenges

DNA privacy rules are rights-based in Europe, balanced in the USA, pragmatic in the UK and developing in India. The underlying denominator is that DNA data is uniquely sensitive and needs extra security beyond other digital evidence. In the investigation of a crime, cooperation between countries is essential. This illustrates the need of standardization. Problems of the future — increase of artificial intelligence, analysis of massive data and genetic genealogy. They expand the utility of DNA, but also have privacy problems. The global debate is increasingly about proportionality: how to have the benefits of DNA profiling without it being used for surveillance, discrimination or abuse. Comparative studies reveal that the idea is universal, despite the diversity of frameworks: DNA privacy must be respected for justice and human dignity.

FUTURE CHALLENGES: AI, BIG DATA, AND GENETIC SURVEILLANCE

1. Artificial Intelligence in DNA Analysis

Machine learning (ML) is increasingly being applied in forensic science, especially in DNA analysis. AI systems can rapidly evaluate vast quantities of genomic data and detect complex patterns that human experts might overlook. This will accelerate investigations and make the results more accurate. "But the challenge is to be open and responsible." AI algorithms are often "black boxes" because it is difficult to explain how they reach their choices. In a legal context, courts want clarity and reliability; therefore, AI outcomes that are not explainable may

ISSN: 2582-6433

have reduced chances to be accepted. Algorithms relying on incomplete or biased datasets can likewise be a source of prejudice. “AI is going to play a bigger role in DNA testing, and there are going to have to be guidelines for auditing it, interpreting it, and monitoring it.” The use of AI could be disastrous for privacy and for justice if these restrictions are not in place.

2. Big Data Integration and Privacy Risks

Big data has transformed the way we store and evaluate genetic information. DNA profiles are being connected with increasing frequency to other sorts of data, including medical data, biometric identifiers, and data from social media sites. This enables high-tech inquiries but also amplifies the hazards to privacy. DNA coupled to other data can mean private information about a person’s health, background, or behavior becomes public. The question is how do you stop it from being abused, particularly by firms or governments who might use DNA information for surveillance or discriminatory treatment of certain populations? Consent is also an issue for big data platforms since consumers don’t know how their DNA will be connected with other DNA. DNA only to be used for legal purposes Need for legal guidelines to restrict how data is merged. The next problem is to achieve the correct balance between the right to privacy and the use of big data for investigations.

3. Genetic Surveillance and Civil Liberties

Using DNA data to keep an eye on large groups of people is called genetic monitoring. And with the progress of technology, massive genetic data banks may now be stored, perhaps for whole populations. It could stop crime and make the country safer, but it presents a lot of civil rights problems. Genetic tracking might produce a future in which everyone is under constant surveillance and their biological identity is forever registered. It takes away people’s freedom and allows for genetic discrimination. The challenge is to get the balance right between the need to stop abuse and the requirement to investigate adequately. “Governments must set clear limits on surveillance, and DNA data should be kept only for the necessary time and not used for other purposes,” he said. The future of genetic surveillance will show how well community safety and individual freedom are balanced. It is also one of the biggest threats to the privacy of digital proof right now.

4. Cross-Border Data Sharing and Global Regulation

DNA data often travels with researchers when they undertake experiments in more than one area. AI and big data techniques can send genetic information from one country to another in an

ISSN: 2582-6433

instant. Privacy laws and protections vary in each country. Some regions have severe restrictions about safety, like the European Union. In some locations the rules aren't too strict. It is more difficult to ensure that privacy standards are constantly considered. "When you share across borders, you expose people to abuse under foreign law, and that undermines trust in the justice system. The problem for the future is to develop international rules that safeguard DNA privacy while also allowing people to work together to catch criminals. There will be a need to establish international accords and treaties, but it is hard to persuade people to agree on anything when their legal systems are so varied. With the rising use of genetic monitoring around the world, it is more important than ever to develop agreement on basic criteria. "Sharing of DNA information between countries could make people lose control of it if the information is not harmonized.

5. Ethical and Societal Implications of Genetic Technologies

But the future of DNA profiling is fraught with serious ethical dilemmas as well as technical and legal challenges. Big data and artificial intelligence systems can predict the genetic predispositions that impact decisions on healthcare, work, or insurance. This is a danger of genetic discrimination. Your talent is irrelevant to your DNA, and people are handled by their DNA, not their ability. If people fear that their genetic information can be abused, this may erode the trust of society in justice institutions. So, the use of DNA technology must be regulated by ethical rules to safeguard dignity and autonomy. The people need to be educated and provide their agreement, as they need to know how their DNA is collected, kept, and used. The challenge is to develop a culture of responsibility, where technology serves justice but does not take liberties. As genetic surveillance becomes more sophisticated, problems of identification, privacy, and fairness will have to be addressed by society. Future legislation will be based on ethics.

CONCLUSION

Today digital evidence is a significant part of investigations. The most critical features of good forensic work are DNA profiling, safe data storage and the chain of ownership. These technologies improve the precision and quickness of the justice done yet the privacy considerations are very significant. DNA information is particularly private because it can disclose not only your name but health and family information. If this information is misused then the rights of people are in serious jeopardy. So, to have accurate and usable data, tight custody procedures and adequate storage methods are necessary. Meanwhile, the globe is

ISSN: 2582-6433

embroiled in a discussion about privacy, advances in AI and Big Data and the increasing use of genetic surveillance. All of these require more legal and moral protection. Digital evidence will be used in future to find a balance between fast investigations and respect for people's rights. Digital proof can be utilized for justice without taking away essential rights when there is a strong framework linking science, law and privacy.

REFERENCES

ACTS

The Indian Evidence Act of 1872

The Code of Criminal Procedure, 1973 The Constitution of India

WEBSITES

https://www.unodc.org/cld/zh/education/tertiary/cybercrime/module-4/key-issues/digital-evidence.html

https://blog.ipleaders.in/all-about-digital-evidence/

https://www.hpnlu.ac.in/PDF/569acd51-8859-496e-97a5-07c60415be7e.pdf