Legal Aspects of Challenges and Privacy Concerns in Establishing and Maintaining a Forensic DNA Database in Sri Lanka

S.M. Rathnayake[1#], Y.M. Mayadunne[1] and K.O. Liyanage[1]

[1]*Faculty of Law, General Sir John Kotelawala Defence University, Rathmalana, Sri Lanka*

[#]38-llb-0088@kdu.ac.lk

Abstract– *This research has been conducted to identify the legal aspects of challenges and privacy concerns in establishing and maintaining a forensic DNA database in Sri Lanka. Establishing a forensic DNA database in Sri Lanka raises legal, financial, and practical issues. This research observes the laws and regulations in an international context and identifies the lack of legislation in the country that concerns the legal aspects of establishing a forensic DNA database. A qualitative research methodology is adopted to collect primary and secondary data. Lack of a specified DNA identification act, legality of the DNA concerning privacy and human rights, issues in accessing, protecting, and securing DNA information, and retention and deletion of DNA information were identified as the main legal issues in establishing a national forensic DNA database. Sri Lanka must strike a compromise between the need for effective law enforcement and the preservation of private information in the establishment of a forensic DNA database.*

Keywords - DNA, Legal, Forensic

INTRODUCTION

Deoxyribonucleic acid (DNA) is identified as the source of each individual's genetic makeup. Each person's DNA is unique, except for identical twins. DNA does not change over time, other than in cases of mutation. The uniqueness of DNA has led to the identification of humans in various instances. DNA molecular structure was first discovered in 1950 by Francis Crick and James Watson. DNA is used to create databases such as population, national, and forensic databases. The function of a forensic DNA database is to store individuals' DNA profiles, which enables the comparison of DNA samples collected from the crime scene. As a subfield of digital forensic science, this electronically stored data system is used in reconstructing clues, detecting crimes, and completing case cracking.

As a considerable range of opportunities has been opened up in criminal investigations, the scope of DNA analysis evidence found at the scene of crime (i.e., blood, hair, saliva, sperm, etc.), which creates the forensic DNA database, allows to locate the perpetrator of the particular crime. DNA typing and profiling were initiated by the laboratories of the United Kingdom, Canada, and the United States of America in the mid-1980s. Professor Alec Jeffrey invented modern DNA typing, which was first used in the Colin Pitchfork case in 1985 in the UK. The case has demonstrated how a small DNA sample is used to find the perpetrator among a large population. US commercial laboratories and the Federal Bureau of Investigation (FBI) started using DNA technology in the late 1980s. According to Interpol, 70 countries have been reported as having forensic DNA databases, and 87 countries have been reported as using DNA profiling in criminal cases in the modern context.

*Sajeewa Alias Ukkuwa and Others v. The Attorney General (*Hokandara case) is considered the first case in Sri Lanka to accept DNA evidence.

However, by the Supreme Court's decision, in this case, the conviction had been solely based on circumstantial evidence and other scientific evidence, such as chiral fingerprinting, rather than DNA evidence. Nevertheless, DNA evidence has been used in other criminal cases since 2004. Currently, there are private labs such as Genetech that offer DNA testing in Sri Lanka However, Sri Lanka lacks a national forensic DNA database. As the rate of crime gradually increases, the requirement for a forensic DNA database is essential in Sri Lanka. Establishing a national forensic database in Sri Lanka has legal, financial, and practical challenges and privacy concerns. This article will discuss the legal aspects of the challenges and privacy concerns associated with establishing and maintaining a national forensic database

METHODOLOGY

This research is conducted to understand the current legal challenges in Sri Lanka to establish and maintain a forensic DNA database. The study as inductive research observes the current legal framework of Sri Lanka alongside with the legal practices of other nations with a

forensic DNA database. Data collection for this study was done through several qualitative methods. The research includes primary data as well as secondary data. Primary data was collected through virtual interviews with Former government analyst Mrs.Sakunthala Tennakoon and Narcotic Director, SSP S.D. Wijesekara. As current practices relating to DNA data handling in Sri Lanka are not documented, the most suitable method of collecting data is by interviewing professionals who are working in the field of DNA data handling. Secondary data collection was done on an Internet basis and through library research. The majority of the acts, journal articles, and other reports were gathered through Internet research.

Data analysis is done on the basis of the discussions and the prevailing law in Sri Lanka. The prevalent situation had been analyzed based on the Criminal Procedure Code No. 15 of 1979 (CPC) of Sri Lanka and other recent enactments relating to privacy and the protection of data. DNA identification acts of several countries had been mainly referred to compare the legislations of countries and to highlight the lack of legislation in Sri Lanka relating to the management of forensic data. While existing research promotes the need for a forensic DNA database in Sri Lanka, they have not addressed the legal challenges which arise when establishing a forensic DNA database. This research addresses the gap by proposing solutions to overcome the challenges and privacy concerns by referring to the laws of other states.

DISCUSSION

The prevailing law in Sri Lanka authorizes many institutions to collect DNA data. According to Section 116(3) of the CPC of Sri Lanka, magistrates have the power to refer any document or weapon to a government analyst, government examiner, or registrar of fingerprints and get a report. Section 123 authorizes the police to collect DNA samples from suspected persons. Section 122 of the Criminal Procedure Code (CPC) relates to the medical examination by a medical practitioner.

Presently, in Sri Lanka, private companies and government analysts keep records of DNA samples in their private data collections. This raises the question of whether these private data collections should be regarded as official databases. Although globally there are no established criteria for an official DNA database, there are some common standards that are used by law enforcement agencies and other organizations that collect and store DNA data. The common criteria and standards include a reliable monitoring and alerting system, support for backup and restore, reasonable upgrades, an active support community, ease of performance tuning, and ease of troubleshooting.

A. Lack of a specific DNA identification act The initial issue identified during the research is the lack of a specified act relating to DNA identification information in Sri Lanka. The majority of the foreign countries that manage forensic DNA databases have enacted DNA identification acts or similar enactments to regulate the laws relating to the use of DNA information. This can be recognized in the DNA Identification Act of 1994 in the USA, the DNA Identification Act of 1998 in Canada, and the DNA Identification Act No. 9944 of 2010 in South Korea.

B. Legality of DNA concerning privacy and human rights For the purpose of collecting, analyzing, and keeping DNA samples and profiles, many legal systems demand informed consent. This makes sure that people are aware of the benefits, ramifications, and possible concerns related to the inclusion of their genetic information in a DNA database. The use of DNA databases is frequently subject to legal limitations. Usually, only approved purposes, such as locating the missing and conducting criminal investigations, are allowed to utilize DNA data. (Clayton et al.,2019) Limiting the available purposes protects genetic data from possible abuse or unlawful access. Established in 1994, the United States DNA Identification Act was integrated into criminal investigations and regulated the collection, testing, and use of DNA samples and profiles. Fighting crime is critical, but courts have debated whether storing DNA samples from people with no prior criminal records violates the Fourth Amendment to the US Constitution, which protects against arbitrary searches and seizures. Accordingly, the EU decided to adopt the General Data Protection Regulation (GDPR), which specifically outlines recommended procedures and requirements for data protection. In line with the provisions of the GDPR, personal data, including genetic information, in the UK is subject to a set of guidelines set out in the Protection of Freedoms Act (2012) and the Data Protection Act (2018).

Guidelines for genetic information and personal data vary from case to case. Canada's DNA Identification Act, the Personal Information Protection and Electronic Documents Act (PIPEDA), and Australia's Crimes Act 1914 provide legislation for DNA databases used in criminal investigations, including consent and privacy regulations, data retention, and security standards. In general, private entities and government agencies must follow regulations to manage and use genetic information. Along these lines, Sri Lanka strongly feels the need for a comprehensive forensic database.

Sri Lanka should also consider privacy factors when establishing a forensic DNA database. Article 12 of the United Nations Declaration of Human Rights (UDHR) declares the right to privacy. It guarantees that people have

the right to keep their genetic information private and safe from unlawful access or exploitation. (Shalev,2002) Also, collecting and maintaining DNA samples concerns the right to dignity and the right to physical integrity. For the establishment of a forensic DNA database in Sri Lanka, there should be a robust privacy safeguard to protect people's rights and interests. At present, the act (*Personal Data Protection Act No. 09 of 2022*) of Sri Lanka provides provisions relating to privacy concerns to a certain extent, but it does not cover privacy in relation to forensic DNA.

C. Access to the forensic DNA database

A legal issue arises regarding access to the forensic DNA database. In the international context, according to the general laws of states, law enforcement agencies, forensic laboratories, criminal justice professionals, authorized personnel for quality control, and other authorized government agencies get access to the forensic DNA database of the state. Section 6(5) of the Canadian act (Data Identification Act of 1998) provides authorized users, and Section 7 of the act provides instances of accessing information. The act *(Use and Protection of DNA Identification Information Act No. 9944 of 2010)* has authorized the establishment of a DNA index, and the Act (*Justice for All Act of 2004*) has expanded the scope of the DNA Identification Act in the USA.

According to Sections 414–417 of the CPC, government analysts and government radiologists provide the evidence for criminal trials, and practically, private companies' DNA evidence is accepted in trials. Sri Lankan authorities lack access to the DNA files of government analyst departments and private companies. Sri Lanka should consider the governmental procedures and implement how access to the database should function in relation to implementing and maintaining a forensic DNA database in Sri Lanka.

D. Cross-border DNA data sharing

Cross-border forensic DNA data sharing concerns with privacy and human rights as mentioned above, other than that there are many issues arising practically in cross border Forensic data sharing such as exacerbation of data protection issues, loss of intelligence due to incomplete county connections, the potential use of false positives in legal actions etc. (Sallavacy, 2015) Differing standards at the national level make for inequality of data and fundamental rights protection when the information is exchanged across borders. The European Union (European Union Law Enforcement Corporation), the Five Eyes Alliance, Schengen area countries, and the United States engage in cross-border data sharing for the purpose of crime-fighting. Sri Lanka meets the issue of regulating cross-border forensic data sharing by maintaining the forensic DNA database. Sri Lanka lacks an enactment to regulate cross- border data sharing.

In an international context, the DNA Identification Act of 1994 and the DNA Fingerprint Act of 2005 of the USA regulate and authorize international law agencies to share DNA data. In the UK, the act (*Crime and Security Act 2010*) provides the legal framework for exchanging DNA data and fingerprints with other countries (*Section 19- Materials Related to the International Criminal Court Act 2001*). The act (*Crimes Act of 1914*) in Australia empowers the sharing of forensic information, including DNA, with other countries. All these enactments allow cross-border data sharing in specific situations, such as preventing crimes and assisting in investigations of offenses.

E. Protection and Security

A legal issue arises regarding the protection and security of data. It concerns different procedures and actions relating to forensic DNA. Security issues arise when various parties access the data. Access should be limited. Section 8(1) of the Canadian act (*DNA Identification Act of 1998*) prohibits unauthorized access to the forensic DNA database. It also provides for the removal of access in specific incidents to protect data. Sri Lanka should implement security procedures in accessing the DNA databases because it affects the privacy and other rights of the people

In Sri Lanka, DNA utilization shall be limited only to the purpose for which it was acquired. Article 15 of the DNA Identification Act of Korea prohibits the use of data for any purpose other than the performance of duties. Moreover, Article 42 of the GDPR presents the certification mechanism for the purpose of demonstrating compliance with this regulation of processing operations by controllers and processors. Therefore, establishing data protection certification mechanisms reduces the risks relating to protection and security. Sri Lanka should refer to foreign DNA identification acts and implement regulations for the purpose of protecting forensic data. Furthermore, the mechanisms must certify managerial, technical, and operational security. The Identification Act (*The DNA Regulation (application and Use) Bill 2019*) requires IS/ISO/IEC 27001 on information technology, security techniques, and protection, and they must do so in accordance with international standards in the Indian DNA and information management systems. It would be ideal if Sri Lanka implemented similar mechanisms for the protection and security of forensic DNA data.

F. Retention of data

Only those suspected or found guilty of more serious crimes, such as rape and murder, are often the subjects of DNA profiling in many nations. However, in some nations, even in cases where DNA evidence plays no part, DNA is taken when a person is detained on suspicion of committing relatively minor crimes. In a case of reinvestigation due to a suspect not being found immediately or a possibility of miscarriage of justice during the case, biological samples collected at the scene of the crime are necessary for reanalysis at a later date. According to Council of Europe Recommendation No. R (92)1, samples and other body tissues, or the information derived from suspects, may be stored for longer periods of time either upon request from the person concerned or when a sample is discovered at the scene of an offense and cannot be linked to a specific person. In the UK, police cautions (warnings given by the police on the admission of a person's guilt without the need for a trial) also count as convictions and result in the retention of a person's DNA profile until after death (the deletion date is set at age 100), unless the offender was a minor at the time of the offense. Nevertheless, according to UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files), the period of time personal data is kept must not exceed the necessary time for the extracted purpose.

G. Deletion of data

According to Article 13 of the Act (*Use and Protection of DNA Identification Information Act No. 9944 of 2010*), of South Korea, DNA Data can be deleted or erased in several instances such as when the prisoner's dismissal of a public prosecution decision is finalized in a retrial, the DNA identification data that was gathered and stored in the database should be deleted at the prisoner's request, when the detained suspect is proven “not guilty” of the crime DNA data can be deleted at the request of the subject, when a prisoner or a suspects’ request of revocation of the decision to collect DNA samples are agreed by the courts DNA identification information must be erased, In instances where it is no longer necessary to preserve and manage DNA identification information collected DNA data can be erased, or Under Article 13(4), DNA data can also be erased at the request of a relative after the death of a suspect or prisoner, except for repeated offenders and sex crimes under Article

5. In Council of Europe Recommendation No. R (92)1 Regarding the use of DNA analysis within the criminal justice system, measures should be taken to delete data that is no longer necessary for the purpose. However, if the subject has been found guilty of grave offenses against life, integrity, or security of others, the results of the DNA analysis and the information so derived may be kept. In these circumstances, domestic law should establish strict storage time limits.

As per Article 17 of the GDPR, under the Right to Erasure and Right to Be Forgotten, an individual has the obligation to erase personal data that are no longer necessary in relation to the purposes for which they were collected or otherwise processed. Article 32 of the GDPR also mentions, in particular, the risks posed by processing, such as those from accidental or unlawful destruction, loss, or alteration of personal data transmitted, stored, or otherwise processed.

Strong privacy protections and legal issues must be put in place in order to develop a forensic DNA database in Sri Lanka. The creation and upkeep of the database should be done within a clear legal framework that addresses privacy issues, spells out the uses that can be made of DNA data, establishes strict access controls, places restrictions on data sharing, and gives people the right to access, correct, and delete their data. Gaining the public's trust in the forensic DNA database requires accountability and transparency systems. Regular audits, independent monitoring organizations, and reporting procedures can guarantee adherence to privacy laws and offer channels for recourse in the event that they are broken.

CONCLUSION

There is a requirement for a database, which is limited and developed to some extent by various constitutions and other provisions, according to other models and sources globally. It shows progress in overcoming the problems of collecting forensic data. This privacy concern also lends further validity to the formality of having an informal database. These protections should include informed consent for DNA collection, purpose limitation and data minimization, stringent data security measures, and procedures for data preservation and disposal in accordance with the law. In order to avoid the problems of access to forensic databases, cross- border sharing, protection and security, and retention and deletion of data, Sri Lanka strongly needed to create a DNA database and prepare it in time. Even within the Constitution of Sri Lanka, the space for the use of genetic data while protecting privacy data is the most important point of such a database because this is important even for other legal systems in Sri Lanka. The creation of a forensic DNA database in Sri Lanka must strike a balance between the necessity for efficient law enforcement and the protection of personal information.

REFERENCES

Crime and Security Act 2010.

Criminal Procedure Code No. 15 of 1979.

Use and Protection of DNA Identification Information Act No. 9944 of 2010.

DNA Identification Act of 1994.

DNA Identification Act of 1998.

Ellen Wright Clayton and others, The law of genetic privacy: applications, implications, and limitations, Journal of Law and the Biosciences, Volume 6, Issue 1, October 2019, Pages 1–36, https://doi.org/10.1093/jlb/lsz007.

Establishing best practice for forensic DNA databases,2017, <http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/BestPractice_Report_plus_cover_final.pdf>.

Fernando, R., (2011). A National DNA Database for Sri Lanka. *Sri Lanka Journal of Forensic Medicine, Science & Law* [online]. **1**(1), 10. [Viewed 6 August 2023]. Available from: doi: 10.4038/sljfmsl.v1i1.2710

Guillen M, 'Ethical-legal problems of DNA databases in criminal investigation' (2000) 26(4) Journal of Medical Ethics 266

<http://dx.doi.org/10.1136/jme.26.4.266> accessed 13 June 2023.

Interpol, Global DNA profiling Survey results, 2019,

<https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAIQw7AJahcKEwjwrMbvlMD_AhUAAAAAHQAAAAAQAw&url=https%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F15469%2Ffile%2FINTERPOL%2520Global%2520DNA%2520Profiling%2520Survey%2520Results%25202019.pdf&psig=AOvVaw1B9naClGrqVUC9eVFlXjSJ&ust=1686742801611440>.

Justice for All Act of 2004.

Kaye, D.H. and Imwinkelried, E.J. (2001). Forensic DNA Typing, Selected Legal Issues: A Report to the Working Group on Legal Issues, National Commission on the Future of DNA Evidence.

SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.2050706.

Parven, K. (n.d.). forensic use of dna information v human rights and privacy challenges. [online] available at: http://classic.austlii.edu.au/au/journals/UWSLawRw/2013/5.pdf.

Personal data protection act No. 09 of 2022.

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).

Puri, A. (2001). An international DNA database: balancing hope, privacy, and scientific error. 24(2), pp.341–80.

Roisin A Costello, Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?, Human Rights Law Review, Volume 22, Issue 1, March 2022, ngab031, https://doi.org/10.1093/hrlr/ngab031.

Sajeewa Alias Ukkuwa and others v. The Attorney General (2004), 2 Sri LR 263.

Sallavaci, O. (2015). Cross-border exchange of forensic DNA and human rights protection. Forensic Science International: Genetics Supplement Series, 5, pp.e86–e88. doi:https://doi.org/10.1016/j.fsigss.2015.09.035.

Shalev, Carmel. (2002). Human Cloning and Human Rights: A Commentary. Health and Human Rights. 6. 10.2307/4065317.

South Korea: DNA Database System Established to Effectively Prosecute Violent Criminals, <https://www.loc.gov/item/global-legal-monitor/2010-08-31/south-korea-dna-database-system-established-to-effectively-prosecute-violent-criminals/>.

The Crimes Act of 1914.

The DNA Regulation (application and use) Bill, 2019.

Toom, V., Granja, R. and Ludwig, A. (2019). The Prüm Decisions as an Aspirational regime: Reviewing a Decade of Cross-Border Exchange and Comparison of Forensic DNA Data. Forensic Science International: Genetics, 41, pp.50–57. doi:https://doi.org/10.1016/j.fsigen.2019.03.023.

ACKNOWLEDGEMENT

We wish to thank Mrs. Sakunthala Tennakoon for providing information about the current procedures relating to forensic DNA in Sri Lanka and the involvement of the government analyst department and private institutions. We also wish to thank Mr. S.D. Wijesekara for providing information about DNA collection and the involvement of the Sri Lanka police in the procedures relating to forensic DNA in Sri Lanka during the research.

AUTHORS BIOGRAPHIES

Mr. S.M. Rathnayake, the author, is a third year law student at General Sir John Kotelawela Defence University. This is his first experience in research publication. Law related to Forensic medicine, Family Law and IT Law are his particular research interests.

Ms. Y.M. Mayadunne, the author, is a third year law student at General Sir John Kotelawela Defence University. This is her first experience with research publications. IT Law, Law related to Forensic medicine, and Criminal law are her particular research interests.

Mr. K.O. Liyanage, the author, is a third year law student at General Sir John Kotelawela Defence University. This is his first experience in research publication. Law related to Forensic medicine, Criminal law and Legal methods are his particular research interests.