UDK 343.14:57.088.7(497.5)
342.722:341.645(4-67EU)
Original scientific paper

CORRECTING MISCARRIAGES OF JUSTICE IN CROATIA: ACCESSION AND TIME-LIMITED RETENTION OF DNA PROFILES IN THE JURISPRUDENCE OF THE EUROPEAN COURT OF HUMAN RIGHTS*

Damir Primorac, PhD, Full Professor
Attorney at Law and Full-time Professor at the Faculty of Law University of Mostar and Associate Professor at the University Department of Forensic Sciences at the University of Split, Domjanićeva 25, Zagreb, Croatia
damir.primorac@primorac-partners.com

Andrej Božinovski, LLM, Assistant
Faculty of Law in Zagreb, Croatia
Gundulićeva 10, Zagreb, Croatia
abozinovski1@pravo.hr

ABSTRACT

The emergence of Innocence Projects in Croatia in 2015 sparked an interest in the fate of wrongfully convicted individuals and the potential of post-conviction DNA examination. In 2020, the experimental Innocence Project was established at the Faculty of Law in Zagreb, funded by the Croatian Science Foundation to raise public awareness of miscarriages of justice, advocate for legal changes to make it easier for defendants to reopen their cases, and provide legal representation for those believed to be wrongfully convicted. This article delves into the use and handling of DNA information by law enforcement agencies and its treatment within the jurisprudence of the European Court of Human Rights and in the Croatian national criminal legislation. However, concerns have been raised regarding the retention, use, and time-limited frameworks of DNA data in law enforcement databases, particularly concerning the presumption of innocence for individuals who have not been convicted of a crime. The European Court of Human Rights adopted the "Marper" test to address this issue and to ensure that all DNA data is expunged from

* The research for this publication has been conducted within the framework of the Research Project titled "Innocent Project Croatia" (CROINOP), funded by the Croatian Science Foundation (IP-2019-2104-9893), and Career development project for young researchers - training of new PhDs (DOK-2021-2102-5858), also funded by the Croatian Science Foundation. See: https://croinop.pravo.unizg.hr/.

law enforcement databases when it is not relevant to criminal investigations. This test balances the government's interests in crime prevention and criminal investigation against individual citizens' privacy interests, making it essential in addressing wrongful convictions. Using the theoretical, comparative, case study, and dogmatic method The article examines the legal standards of the Council of Europe and the European Union, the jurisprudence of the European Court of Human Rights, as well as Croatian positive legal standards on the retention and use of DNA data and applicable databases. Finally, the article suggests potential legislative reforms in Croatia to improve the utilization, storage, and ramification of DNA data and the use of forensic DNA databases to address miscarriages of justice, particularly in "cold cases".

Keywords: *DNA, Innocence Projects, Marper Test, Wrongful Convictions*

1. INTRODUCTION

The interest in Innocence Projects started in Croatia in 2015, mainly as a result of academic discussions and conferences about the fate of wrongfully convicted people and the possibilities of post-conviction DNA examination. It culminated in 2020 when for the first time the experimental Innocence Project was established, implemented by the Faculty of Law in Zagreb, and financed by the Croatian Science Foundation. The main purpose of the Croatian Innocence Project is to raise public awareness of miscarriages of justice, campaign for legal changes which ought to lower the threshold for defendants to have their cases re-opened, and provide legal representation for those who are believed to have been wrongfully convicted.[1] This article will shed light on the use of DNA information by law enforcement agencies for crime prevention purposes that has undoubtedly aided in criminal investigations and contributed to the apprehension of perpetrators. The retention, use, and time-limited frameworks of DNA data in law enforcement databases raise concerns regarding the presumption of innocence for individuals who have not been convicted of a crime. When DNA information is collected, retained, and utilized for individuals who have been acquitted, had charges dropped, been arrested for non-violent or non-sexual crimes, or completed their sentence, the presumption of innocence is diminished. In several cases from the jurisprudence of the European Court of Human Rights, it is visible that national laws on expungement often lack clarity or are inadequate, leading to improper use of DNA information.[2] In order to address this issue and prevent the erosion of the presumption of innocence the European Court of Human Rights adopted

[1] See Bozhinovski, A.. *Addressing Wrongful Convictions in Croatia through Revision of the Novum Criterion: Identifying Best Practices and Standards;* Mali, J (eds.), Human Rights in Contemporary Society – Challenges From an International Perspective, Vol. 1 2023, pp. 57-77.

[2] Expungement of DNA data is different in every country and refers to the process of erasing or removing certain records or information from official databases or records. In the context of DNA information, expungement involves the removal of DNA data from law enforcement databases for individuals who have not been convicted of a crime. Expungement is recognized as a legal mechanism to protect

a test – the *Marper* test that would require law enforcement agencies to expunge DNA data from their databases based on the individuals' statuses as arrestees, non-convicts, convicts, or ex-convicts, and taking into account the severity of the alleged offense that justified the extraction of DNA. The essence of the *Marper* test is the balance the interests of the government in crime prevention and criminal investigation against the privacy interests of individual citizens which further ensures that all DNA data is expunged from law enforcement databases in cases where it is not relevant to criminal investigations. This makes the Marper test essential for addressing wrongful convictions. In this article, the first part will examine the binding legal documents promulgated by the Council of Europe and the European Union in the context of retention, storage, and ramification of DNA data pre- and post-conviction. In the second part, the standards of the European Court of Human Rights and the Court of Justice of the European Union will be examined in the context of time-limited retention of DNA data and forensic DNA databases utilizing the *rationale* of the court in recent judgments. The third part will be presented the positive Croatian legal standards in the Law on Criminal Procedure for the retention and use of DNA data and applicable databases. The conclusion part of the article will give an insight into possible implications in the Croatian national legislation in terms of reforms that are needed concerning the utilization, storage, and ramification of DNA data and the use of forensic DNA databases to address the so-called "cold case" correcting miscarriages of justice.

2. LEGAL STANDARDS OF THE COUNCIL OF EUROPE AND THE EUROPEAN UNION FOR THE TREATMENT OF DNA MATERIALS IN THE CRIMINAL JUSTICE SYSTEMS

The scientific and technological development in genetics and molecular biology piques the interest of the states in the application of such methods in forensics and the criminal justice system in general. According to Primorac and Moses in its simplest form, a DNA profile consists of numerical figures that represent the variations of alleles found in each locus, like bar codes. However, cellular samples can provide a lot more information, including health and genetic information that may have deeper privacy implications, such as ethnic and familial tracing and predisposition to genetic diseases.[3] In its practice, the Court has acknowledged this wealth of information and has extended the same protection to both cellular samples and DNA profiles. Despite this, limiting sample collection to DNA pro-

the privacy and rights of individuals who have not been found guilty of a crime and to prevent the misuse of their DNA information.

[3] See Primorac, D. and Schanfield, M, *Forensic DNA applications: An interdisciplinary perspective.* CRC Press, 2023., p. 54-59.

files provides adequate privacy protection given their limited use for identification purposes.[4] Legal safeguards can be implemented by requiring the destruction of cellular samples and DNA extracts after the production of DNA profiles to limit interference to numerical figures representing a person's DNA profile. When handling this information, the relevant laws adhere to the legality test, established by the Court in the *Marper* case that determines the scope and the nature. The test has two main requirements: 1. The interference of the measure should have some basis in the domestic law or a member state; and 2. The law must be clear, foreseeable, and adequately accessible. This is the primary test on which all future cases are adjudged upon.[5] Deviation from this criterion will result in a breach of Article 8 of the European Convention of Human Rights The relevant legislation governing the principles of retention, storage, and utilization of DNA data in Europe is promulgated by the Council of Europe and the European Union. The mutual trait of these legislations is the treatment of DNA data as a special, sensitive type of data that belongs in the group of special categories of personal data.

2.1. Council of Europe

The Council of Europe's Convention for the Protection of Individuals concerning the Automatic Processing of Individual Data, known as ETS No. 108, is a treaty adopted in 1981 that aims to safeguard individuals' fundamental rights and freedoms in the context of automated processing of their data.[6] It sets forth principles and guidelines for data collection, storage, and use, including requirements for data quality, security, and individual rights. Most importantly this convention serves as an important international instrument for protecting privacy and data protection rights in the context of automated data processing. Article 6 of this Convention stipulates that the DNA data may be categorized as a special category of data and that the DNA profiles can be categorized either as genetic data or biometric data attributed uniquely to one person, and the processing of such data is not prohibited if the state law contains the appropriate safeguards. In the *Marper decision, the Gaughran v. the United Kingdom, Petrovic v. Serbia and in Trajkovski and Chipovski* the court cited this convention in terms of the standard *Quality of law.* However, there is nothing in this convention that prohibits the creation of universal DNA databases. In 2018, the

---

4 See Derenčinović, D.; Roksandić Vidlička, S.; Dragičević Prtenjača, M., *'Innocence Projects' and Subsequent DNA Testing in Croatia: a Possible Reality or an Unattainable Desire?.* Zbornik Pravnog fakulteta u Zagrebu, Vol. 67, No. 3-4, 2017, pp. 373–404.

5 See *infra* note. 23. *S. and Marper v the United Kingdom,* no. 30562/04 and no. 30566/04., par. 77.

6 See The Council of Europe's Convention for the Protection of Individuals Regarding the Automatic Processing of Individual Data and Protocols, ETS. No. 108 +, available at: [https://www.coe.int/en/web/data-protection/convention108-and-protocol].

Council of Europe promulgated Convention ETS No. 108 + to enhance the framework on personal data protection. Convention 108+ builds upon Convention 108 by addressing contemporary issues in data protection.[7] It expands the scope of protection to include manual data processing alongside automatic processing, adapting to new technologies. It aligns its provisions with the GDPR, ensuring compatibility and facilitating the transfer of personal data between member states. Convention 108+ strengthens individual rights, emphasizing transparency, accountability, and the right to access, rectify, and erase personal data. It introduces provisions for independent supervisory authorities and international cooperation among data protection authorities.[8] Additionally, it includes mechanisms for monitoring compliance and establishes a monitoring body to assess implementation and provide guidance. Concerning the harmonization with the GDPR, Convention 108+ enables seamless data transfer between the Council of Europe (CoE) member states and the European Union (EU) by adopting similar concepts, definitions, and principles. By incorporating the robust data protection standards of the GDPR, Convention 108+ enhances the level of privacy and security for individuals' personal data. It facilitates international data transfers by adhering to the GDPR's stringent requirements for transfers outside the EU. Additionally, the harmonization strengthens the influence of Convention 108+ on global data protection regulations, as the GDPR has become a global benchmark. Overall, the harmonization with the GDPR elevates data protection within the CoE and fosters consistency and effectiveness in the treatment of personal data.

Another legal instrument promulgated by the Council of Europe is Recommendation No. R(92)1 on the use of DNA analysis in criminal investigations adopted in 1992. The Recommendations provide guidance on the use of DNA analysis in criminal investigations and underscore the primacy of the respect for human rights, including the right to privacy, in the context of DNA analysis by law enforcement authorities. It emphasizes the necessity of the promulgation of clear and transparent legal frameworks and procedures governing the collection, storage, and utilization of DNA samples and profiles.[9] The importance of quality control

---

7 See The Council of Europe's Convention 108 + Convention for the protection of individuals with regard to the processing of personal data, available at: [https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf].

8 General Data Protection Regulation, Official Journal of the European Union, No. L119/1, available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679].

9 See Council of Europe Committee of Ministers. Recommendation No. R (92) 1 of the Committee of Ministers to Member States on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system. Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies. Available at: [https://rm.coe.int/09000016804e54f7].

and data protection measures is also emphasized. Furthermore, the Recommendation promotes cross-border cooperation among member states in DNA data exchanges while stressing the need for robust safeguards to prevent potential misuse or abuse of DNA information. In the context of the criminal procedure, this Recommendation emphasizes the principle of equality of arms, stipulating that the DNA materials must be accessible to both parties, the prosecution as well as to the defense. In the legal text, this recommendation refers to the European Convention of Human Rights and the Convention for the Protection of Individuals about the Automated Processing of Individual Data. In the context of defining DNA data or DNA analysis, this recommendation defines DNA analysis as *"Any procedure that can be applied in the analysis of DNA – the basic genetic material of the human being and all other beings"*; DNA sample is defined as *"Any material stemming from the organic origin which can be used for the DNA analysis"*; and also defines a DNA dossier as *"every structured collection of DNA results regardless in which form they are kept, including print and electronic databases can be categorized as a DNA dossier*. The validity of this recommendation has been confirmed in *Marper* and in *Gaughran* where in both cases, it is evident that the provisions outlined do not prescribe the establishment of universal databases. However, they do prescribe certain safeguards that must be in place to ensure compliance. These safeguards encompass restricting the use of the databases exclusively to the investigation and prosecution of criminal offenses, adherence to domestic law in sample collection procedures, and the deletion of data once their purpose has been fulfilled, as articulated in Provision 8. Moreover, if the databases are employed for research and statistical purposes, it is mandated that the identity of the data sources remain unascertainable, as stipulated in Provision 3.[10]

Recommendation Nm. (87) 15 of the Council of Europe regulates the use of personal data in the police sector. issued in 1987, is a guideline that guides member states regarding the utilization of personal data in the police sector. The recommendation underscores the significance of safeguarding the rights and freedoms of individuals while ensuring the effectiveness of law enforcement efforts.[11] It highlights the need for comprehensive legislation on data protection in the police sector,

---

[10] See Krstulović Dragičević, A. and Sokanović, L., *Načelo zakonitosti pred izazovima europskog kaznenog prava,* Zbornik radova s medunarodnog savjetovanja „Europeizacija kaznenog prava i zaštita ljudskih prava u kaznenom postupku i postupku izvršenja kaznenopravnih sankcpija", Vol. 1, 2017 Split, pp. 25-30.

[11] See Council of Europe, Committee of Ministers. Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector. Adopted by the Committee of Ministers on 17 September 1987 at the 410th Meeting of the Ministers' Deputies. Available at:
[https://rm.coe.int/168062dfd4]. See also: Alleyne, L,. *Interpol handbook on DNA data exchange and practice – Recommendations From the Interpol DNA Monitoring Expert Group.,* Vol. 2, 2009.

encompassing lawful processing of personal data, data quality and accuracy, data security, and individual rights such as access, rectification, and erasure of data. The recommendation also underscores the importance of supervisory mechanisms for ensuring compliance with data protection principles and the need for international cooperation in the exchange of personal data for law enforcement purposes. The Recommendation stipulates that retention of DNA data must be limited to what is necessary for the prevention of real danger or the suppression of a specific criminal offense; when storing the DNA data, the storage must be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks, and deletion of the data once it stops being used for the intended purposes by the police. Also one of the main principles of this Recommendation is the principle of *Equality of Arms* that stipulates DNA analyses should be equally available as evidentiary material to the defense and the prosecutor.[12] Furthermore, the standardization of DNA methods is set as a basic rule at the national and international levels, which inevitably assumes interlaboratory cooperation to unify analytical and control procedures. Although intellectual property rights are tied to certain DNA methods analyses, in this sphere it is strictly required that this is not the case. DNA analysis can be performed in a laboratory or institution from another country and it will be valid in the state where the case is handled if it is an institution that fulfills all criteria defined in this Recommendation. Cross-border communication and exchange of information must be in accordance with international standards and documents for the exchange of information in criminal cases and data protection.

2.2. European Union

The European Union has taken specific steps to regulate the legal aspects of DNA analysis in criminal investigations. In 1997 and 2009, the European Council adopted the Resolution on the Exchange of DNA Results Analysis[13], which emphasizes the significance of exchanging DNA analysis results for successful criminal investigations. Based on the principle of mutual trust the exchange of such information must be limited to the non-coding part of the DNA molecule to prevent the disclosure of sensitive personal data. DNA investigation involves technical, legal, political, and ethical considerations that require attention in future cooperation efforts. The Resolution refers to various European documents such as conventions and recommendations that highlight the use and protection of personal data. Standardizing DNA markers is crucial to ensure that the results of DNA analyses

[12] See Tseloni, A.; Pease, K., *DNA retention after arrest: Balancing privacy interests and public protection*, European Journal of Criminology, Vol. 8, No. 1, 2010, pp. 36–38.

[13] See Council of the European Union. "Council Resolution of 9 June 1997 on the Exchange of DNA Analysis Results." Official Journal of the European Communities L193 (1997).

exchanged between countries are usable.[14] Furthermore, according to the Stockholm Programme and the application of the principle of mutual trust, establishing well-functioning databases is necessary.[15] The Resolution also addresses issues such as creating national databases of DNA data, standardizing DNA technology, providing legal guarantees, and exchanging DNA analysis results at the European level. Furthermore, with efficient cross-border cooperation, legal guarantees, and standardization, the resolution can help prevent errors and misunderstandings that could lead to wrongful convictions or acquittals, and identify perpetrators who might otherwise go undetected.

In 2001, the European Union (EU) Council introduced a Resolution on exchanging DNA analysis results, which was later replaced by a similar act in 2009.[16] The Preamble of the Resolution refers to previous Council of Europe and EU acts, as well as the European Network of Forensic Institutes' efforts to standardize DNA markers and technology. It defines terms such as "DNA marker" and "DNA analysis result," and emphasizes limiting the exchange of DNA results to chromosomal zones without genetic expression, thus avoiding the disclosure of sensitive personal data. The Resolution's Annex[17] provides a list of markers that are considered safe for exchange, but countries must discontinue the use of any markers if new scientific developments allow information on hereditary characteristics to be obtained from them. In 2005, the Prum Convention was introduced to promote cross-border cooperation in the fight against terrorism, cross-border crime, and illegal migration. The decisions that were, adopted in 2008, further address the issue of exchanging DNA profiles, limited to the non-coding part of the DNA molecule, per the EEC and Interpol's ISSOL.[18] DNA data is classified as special categories of personal data and is considered the most sensitive. The Convention

---

14 See Primorac, D.; Primorac, D.; Butorac, S. S., & Adamović, M. *Analiza DNA u sudskoj medicini i njezina primjena u hrvatskome kaznenopravnom sustavu.* Hrvatski ljetopis za kazneno pravo i praksu, Vol. 16, 2009, pp. 3-16.

15 The Stockholm Programme, OJ C 115, 4.5.2010, available at: [https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF].

16 See Council of the European Union. "Council Resolution of 30 November 2009 on the exchange of DNA analysis results (2009/C 296/01)." Official Journal of the European Union, Vol. 52, No. C 296, 1 Dec. 2009.

17 *Ibid.,* p. 5.

18 INTERPOL International Standard Set of Loci (ISSOL) is a set of 10 genetic markers, also known as loci, used for DNA profiling. These markers are commonly used in forensic DNA analysis to compare DNA samples from different sources and determine whether they match. The ISSOL is used by forensic laboratories around the world as a standard for DNA profiling and ensures that results obtained in different labs can be compared and shared with confidence. The markers in the ISSOL were selected based on their high degree of polymorphism, which means that they are highly variable between individuals, making them useful for identifying unique genetic profiles.

aimed to facilitate information exchange, including DNA-related data, to enhance cooperation among these countries. Over time, other EU member states joined the treaty, and in 2007, the Council of the European Union approved many of its provisions as Council Decisions that became part of the EU's acquis communautaire, such as Council Decision 2008/615/JHA[19], the first EU instrument that foresees direct access to the national databases of other countries, requires EU member states to establish national databases and provides rules for competent authorities of other EU member states to search in national DNA, dactyloscopy, and vehicle registration databases. However, It is crucial to distinguish between direct access to a DNA database and direct access to all the data stored in a DNA database. For example, Member State A can search for a DNA profile in Member State B's DNA database and receives either a positive or negative reply regarding the existence of a relevant DNA profile and reference data (the non-coding part of DNA and a reference number). The searching Member State only receives reference data that can be called 'anonymous,' but there is no direct access to data related to the matched DNA profile. To obtain personal data from the DNA database, it must send an additional request to Member State B.[20] Under Council, Decision 2010/616/JHA[21], designated contact points were designated that are usually either forensic science services or law enforcement units responsible for information exchange that can perform searches in the national DNA databases of other countries. Article 4 of the decision allows for the comparison of unidentified DNA profiles from one EU member state with all other EU member states before bilateral consent. The establishment of 'hit' and 'post-hit' stages allows member states to maintain absolute control over the data associated with DNA profiles.

The General Data Protection Regulation (GDPR) was promulgated by the EU in 2016, and it is an extensive data protection regulation that governs the processing of personal data, including biometric and DNA data, and aims to protect individuals' privacy and ensure responsible handling of their data.[22] Under the GDPR, biometric data refers to personal data derived from the physical, physiological, or

---

19 See Council Decision 2008/615/JHA, 23 June 2008, Official Journal of the European Union, L 210/1.

20 See Soleto Muñoz, H. and Fiodorova, A*, DNA and law enforcement in the European Union: tools and human rights protection,* Utrecht Law Review, Vol. 10, 2014 pp. 149-162.

21 Council of the European Union, "Council Decision of 26 July 2010 on the Conclusion of the Agreement Between the European Union and Iceland and Norway on the Application of Certain Provisions of Council Decision 2008/615/JHA on the Stepping up of Cross-border Cooperation, Particularly in Combating Terrorism and Cross-border Crime and Council Decision 2008/616/JHA on the Implementation of Decision 2008/615/JHA on the Stepping up of Cross-border Cooperation, Particularly in Combating Terrorism and Cross-border Crime, and the Annex Thereto." Official Journal of the European Union, Vol. L195, 28 July 2010, pp. 1-16.

22 General Data Protection Regulation, Official Journal of the European Union, No. L119/1, available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679].

behavioral characteristics of an individual that allows for unique identification. This includes DNA data, which is distinctive to each person and can be used for identification purposes. To process biometric and DNA data lawfully, organizations must have a legal basis, such as obtaining explicit consent from individuals or relying on other legal grounds like compliance with legal obligations or the protection of vital interests. The GDPR recognizes that biometric and DNA data is sensitive and, therefore, imposes stricter requirements for its processing. Organizations must implement appropriate security measures to safeguard this data from unauthorized access, loss, or destruction. Individuals have specific rights regarding their biometric and DNA data. These rights include the ability to access, rectify, or erase their data, restrict its processing, and object to certain types of processing. They also have the right to data portability, allowing them to obtain and use their biometric and DNA data for their own purposes. When processing biometric or DNA data presents high risks to individuals' rights and freedoms, organizations are required to conduct a Data Protection Impact Assessment (DPIA). This assessment helps identify and address potential risks associated with the processing of sensitive data. The GDPR also regulates the transfer of biometric and DNA data to countries outside the EU, ensuring that adequate safeguards are in place to protect the data during such transfers.[23] Currently, the GDPR emphasizes the need for explicit consent, enhanced security measures, and individual rights protection. Compliance with the GDPR is essential for organizations handling biometric and DNA data to uphold privacy rights and maintain data security.

As seen above in all legislative documents the quality of law can be evaluated based on its accessibility, clarity, and foreseeability for the persons concerned. Accessibility refers to the availability of the law to citizens, which is usually achieved through publication in a manner specified by national practice. The same dissemination system can be used for universal databases. Clarity of the law relates to the discretion exercised by public authorities in implementing it. There should be a reasonable degree of clarity in the scope and manner of this discretion to provide minimum protection to people, which can be measured through legal safeguards. This ensures predictability in the implementation of the law for everyone involved. The element of foreseeability is closely linked to clarity, where laws must be clear and specific to ensure the predictability of their effects. In *Petrovic v. Serbia*, the Court held that legal provisions should be foreseeable as to their effects, which was not the case in the law allowing for DNA sample collection. Legal protection must therefore be guaranteed to ensure that laws are not applied arbitrarily by law enforcement agencies. These elements are crucial for evaluating the quality of the law and ensuring its effective implementation.

[23] *Ibid.*

3. COLLECTION, RAMIFICATION, AND STORAGE OF DNA MATERIALS IN THE JURISPRUDENCE OF THE EUROPEAN COURT OF HUMAN RIGHTS AND THE COURT OF JUSTICE OF THE EUROPEAN UNION

The use of DNA technology in criminal investigations has raised numerous concerns regarding privacy and human rights. As noted above The European Court of Human Rights (ECtHR) has addressed these concerns in several cases, including the landmark case of *S. and Marper v. United Kingdom*. Starting from this case, The ECtHR has consistently held that the collection, retention, and use of DNA samples and profiles is a serious interference with an individual's right to respect for private life. The Court has also emphasized the importance of ensuring that any such interference is proportionate and necessary and has established a three-pronged test to evaluate the legality, legitimate purpose, and proportionality of DNA collection and retention practices. This section of the article will examine the Court jurisprudence in the cases of S. and *Marper v. the United Kingdom*[24], *Aycauger v. France*[25], *Gaughran v. the United Kingdom*[26], *and Trajkovski and Chipovski v. North Macedonia*[27] in terms of the three-pronged test. Each of the cases promulgated by the court refers to the handling of DNA data in different stages of the criminal procedure. The cases of *Aycauger v. France* and *Petrovic v. Serbia* refer to the pre-trial of the procedure, where accused persons have been sanctioned after denial to undergo biological testing for the purpose of inclusion in the national database. The *Marper* case is important from the aspect of unlimited retention of DNA materials in cases where the accused is not found guilty (pre-sentencing), and *Gaughran v. the United Kingdom and Trajkovski and Chipovski v. North Macedonia* are cases that refer to unlimited retention of DNA materials after the defendants have been found guilty and sentenced.

Starting with *S. and Marper v. the United Kingdom,* in 2008, the Grand Chamber of the European Court of Human Rights (ECtHR) issued a landmark judgment. The case centered on the retention of DNA profiles by police authorities in the UK, specifically the retention of the DNA profiles of individuals who had been arrested but not convicted of any crime. The first applicant in the case was an 11-year-old boy who had been arrested on suspicion of attempted robbery in 2001, and whose

---

24 See Judgment *S. and Marper v United Kingdom* (2008), application no. 30562/04 and no. 30566/04, 4 December 2008, paras 1-25.

25 See Judgment *Aycaguer v France* (2017), application no. 8806/12, 22. June 2017, paras. 15-25.

26 See Judgment *Gaughran v the United Kingdom* (2020), application no. 45245/15, 13 February 2020, paras. 13-18.

27 See Judgment *Trajkovski and Chipovski v North Macedonia* (2021), application no. 53205/13 and no. 63320/13, 13/02/2020, paras. 1-25.

fingerprints and DNA samples were taken by the police.[28] The second applicant had been arrested and charged with ill-treatment of his partner in 2001, and his DNA sample and fingerprints were taken by the police after the proceedings against him were suspended. Both applicants requested that the seized biological material be destroyed, but their requests were refused by the police. The national courts upheld the police's decision, arguing that the retained biological material was of great importance for preventing crime and enabling effective criminal prosecution. However, the ECtHR found that the authority of competent authorities regarding the retention of DNA samples as particularly sensitive personal data was blanket and non-selective. Furthermore, the Court emphasized that the unlimited use of modern technology within the framework of the criminal justice system without weighing the public interest with the interest of protecting individuals could lead to an unacceptable weakening of the protection mechanism under Article 8 of the Convention that regulates the right to privacy.[29]

The Court argued that the almost unlimited encroachment on privacy was particularly unacceptable for individuals given a large amount of information or data contained in the genetic material. Moreover, the retention of personal data of minors who are not legally competent and convicted in criminal proceedings may call into question the reintegration of this vulnerable group in society, which is contrary to the standards of protection of the best interests of children according to international law.[30] The judgment of the Court and the arguments highlighted in it led very quickly to a change of position in the practice of the national judiciary. The Supreme Court, referring to most of the Court's arguments from the S. and Marper judgment, ruled that DNA profiles that were entered into the database after arresting persons, and after they were released from accusations, must be destroyed. What is interesting is that the process of execution of the judgment led to the preparation of the new Law on the Protection of Freedoms[31], which provided for a series of legal reforms following the standards of the Court expressed in the "Marper" case. However, this law applied only in England and Wales, and not Northern Ireland, and has amended the Law on Police and Criminal Evidence. One of the essential changes brought by the new law was the destruction of DNA samples immediately after taking the DNA profile or within six months at the latest months from taking DNA samples.[32] Furthermore, DNA profiles of minors and adult persons arrested for minor criminal offenses are deleted after the

---

28 See *Supra* note 22, p. 23 - 26.

29 *Ibid.,* p. 34.

30 *Ibid.,* p. 102-106.

31 See Law on Protection of Freedoms Act, 2012, UK Government, available at [https://www.gov.uk/government/publications/protection-of-freedoms-bill].

32 See Romeo Casabona, C. M., *La insostenible situación del derecho penal.,* Granada: Comares, 2000, p. 35-43.

suspension decision is made of the procedure, the decision not to file an indictment or to issue an acquittal. It also introduced a three-year limitation on the retention of DNA profiles of persons who have been arrested for a serious crime criminal offense, but who have not been convicted.[33] The law introduced periodic checks of the validity of the reasons for further retention of personal data, and the possibility of rebutting the retention decision and the realization of their deletion or destruction of data. Furthermore, the amendments to the law established the position of the Biometric Retention Office, whose primary function is to oversee the procedure for collecting, ramifications, and storage of biometric data.

The *Aycaguer v. France* case involved a convicted individual who participated in a protest in 2008 and threatened to attack members of public authorities and then attacked them with an umbrella. The applicant was sentenced to a two-month suspended prison sentence for this offense. The prosecutor requested the applicant to provide a biological sample (DNA) as per Article 706-55 of the French Criminal Procedure Act, which lists criminal offenses for which biological samples are taken and stored in the national digital DNA database (FNAEG). The threat, for which the applicant was convicted, is one such offense. However, the applicant refused to provide the DNA sample and was subsequently detained and fined in 2009.[34] The Court of Cassation, including the higher courts, confirmed the decision of the lower courts in 2011 and concluded that it was per Article 8 of the Convention. However, the Court found that the punishment of the applicant was disproportionate and unnecessary interference in an individual's private life, stating that the legitimate establishment of databases for criminal proceedings should be proportionate and justified by the circumstances of each case. The Court also concluded that due to the absence of relevant secondary legislation, the retention of the DNA profile for the maximum duration of 40 years de facto became the standard, which is not per the principle of proportionality.[35] The Court also objected to the procedure for deleting DNA profiles from the database, which is only possible for suspects and not for convicts, contrary to the principles of protection incorporated in Article 8 of the Convention. The state exceeded the margin of judgment in a way that was not necessary for a democratic society due to the apparent absence of mechanisms for fair weighing of public and private interest.[36]

---

33 See Kaye, D.H., *Maryland v. King: Per se unreasonableness, the Golden Rule, and the future of DNA databases*. Harv. L. Rev. F., 127, 2013 p. 39. See also: Tuazon, O.M., *Universal forensic DNA databases: acceptable or illegal under the European Court of Human Rights regime*? Journal of Law and the Biosciences, Vol. 8, No. 1, 2021 pp. 18-21.

34 *Ibid.*, p. 18-24.

35 *Ibid.,* para. 32.

36 See Becker, S.W.; Derenčinović, D.; Primorac, D., *DNA as Evidence in the Courtroom*; Primorac, D. and Schanfield, M., (eds.) *Forensic DNA Applications: An Interdisciplinary Perspective*, 2023, p. 433.

The Aycaguer case highlights the need for proportionality and justification when establishing DNA databases for criminal proceedings and for proper legislation to govern the retention and deletion of DNA profiles.

Gaughran v. the United Kingdom is a consequence of the legal reforms in the English and the Irish judiciary, after the *Marper case*, which did not include Northern Ireland. This case saw the arrest of the applicant in Northern Ireland due to driving a personal vehicle while intoxicated, which is considered a criminal offense punishable by imprisonment. Biometric data, including a DNA sample, was excluded from the applicant after they confessed to the commission of the offense. Despite being fined and banned from driving, the applicant asked the police to destroy or return the exempted biometric data, which was refused with the explanation that their retention was in accordance with national legislation. The applicant's DNA sample was destroyed in 2015, but all other biometric data, including the DNA profile, was retained indefinitely. The national courts found that the retention of the personal data of an adult for a criminal offense punishable by imprisonment was justified, and therefore the applicant's case was unsuccessful.[37] However, a dissenting opinion stated that national legal solutions for retaining DNA profiles should have been more nuanced with the possibility of deleting profiles from the database and that the High Court and the majority decision of the Supreme Court did not sufficiently take into account the principle of proportionality. The applicant argued that their right to privacy was violated disproportionately, and referred to Recommendation No. R(87) 15 Committee of Ministers, which regulates the issue of collection and retention of personal data by the police in the manner and to the extent *necessary to achieve a legitimate goal with the possibility of erasure of these data from the police records if there is no further need for their retention.* The government accepted that this case was about state interference in the applicant's personal life but argued that this interference was very limited in scope and based on the law to achieve the legitimate goal of crime prevention and detection. The Court analyzed the legal solutions and practice of the respondent state from the aspect of "necessity in a democratic society".[38] The Court tested the legal solutions and practice of the respondent state from the aspect of requirements of "necessity in a democratic society". The Court preliminarily indicated that the personal data contained in the DNA profiles differ from the personal data obtained by taking a fingerprint or taking a photo and that personal data contained in DNA profiles, assuming their indefinite retention, may call into question the privacy of persons who are biologically related to the holder linked. The court removed the argument of the defendant stating that there is no difference between retaining the DNA

[37] *Ibid.,* p. 56.

[38] See *Supra* note. 24, p. 44.

profile until the death of the holder (or until someone certain time after his death) and the indefinite retention of those data. The court rejected the defendant state's argument that a greater number and longer duration of data retention correlates with crime prevention. Such an argument could lead to the indiscriminate collection and retention of biometric data from the entire population, which would prima facie contradict Article 8 of the Convention. This is similar to the case of S. and Marper, which concerned the retention of DNA profiles for persons who were not convicted. In the current case, the court concluded that the non-selective, time-limited retention of DNA profiles (including fingerprints and photographs) without taking into account the seriousness of the committed criminal offense and without realistic and effective opportunities for reviewing the further retention of the profile is not per the requirements of Article 8. The court unanimously concluded that the defendant state exceeded the margin of judgment in a manner that cannot be deemed necessary in a democratic society.

Similar to the *Gaughran* case judgment is *Trajkovski and Chipovski v. North Macedonia case*, which was decided in 2020. The case involved two applicants who argued that their right to privacy had been violated by the police taking DNA samples without their consent or a court order. The first applicant had been sentenced to probation for aggravated theft in 2010 and had a DNA sample taken during his arrest and his sample was used as evidence in the proceedings against him. The second applicant was arrested in 2009 on suspicion of theft, and a DNA sample was taken from him during the arrest. The sample was later also used as evidence in his conviction for aggravated theft in 2014.[39] Both applicants complained to the Directorate for the Protection of Personal Data, based on the longevity of the retention period of their DNA materials, which rejected their complaints. The applicants argued that the national legal framework did not provide sufficient clarity and precision regarding the collection, use, and retention of DNA material and that the retention of their DNA samples violated their right to privacy protected by the European Convention of Human Rights and the Constitution of the Republic of North Macedonia. The Court accepted this argument, pointing to the vague provision of Article 5 of the Personal Data Protection Act, which states that *personal data cannot be kept longer than is necessary for the purpose for which they are collected*.[40] The Court found that this provision left room for different interpretations and the unlimited retention of DNA material in practice.

---

[39] See *Supra* note 25, p. 1-15.

[40] See Article 5 of the Law on the protection of personal data, Official Gazette of the Republic of North Macedonia. 2020 (No. 42/20), available at: [https://azlp.mk/azlp/propisi-i-dokumenti/domasni_propisi/], Accessed 23 april 2023.

The Court also noted that the national legislation did not prescribe any additional criteria or gradation concerning the gravity of the committed criminal act, possible restitution, etc., and that there was no prescribed procedure for periodic review of the need for further retention of DNA samples. The Court concluded that the defendant state had failed to proportionately limit the private interest of the individual to the public interest and that by exceeding the margin of judgment, it had violated Article 8 of the Convention. *The Trajkovski and Chipovski case* highlights the need for clear and precise legal frameworks regarding the collection, use, and retention of DNA material to avoid the violation of an individual's privacy rights.

As seen from these cases The Court emphasizes the importance of distinguishing between these different categories of individuals, as the legal framework and margin of judgment for retaining their DNA material may vary. Derencinovic, Primorac, and Becker argue that when it comes to individuals who have been acquitted or had their criminal proceedings suspended, he notes that there is a significant narrowing of the state's judgment, especially about time-limited retention of personal data, particularly for minors.[41] There is a European consensus on this matter, which limits the state's ability to indefinitely retain DNA profiles of individuals who were not ultimately convicted. However, the margin of judgment widens when it comes to individuals who have been legally declared guilty as seen in *Gaughran and Trajkovski and Chipovski*. Also, Derencinovic on this notes that this does not mean that the state has unlimited power to retain its DNA material indefinitely. Rather, the state must adhere to the principle of proportionality, which is derived from a series of guarantees designed to prevent a blanket and indiscriminate restriction of the right to privacy. These guarantees include a model of gradation of the severity of the criminal offense, judicial control of data retention, periodic checks, and expert opinions on the validity of data retention.[42] Furthermore, the Court emphasizes the importance of evaluating additional circumstances, such as the type of final court decision, rehabilitation, served or completed the sentence, amnesty, age of holder, and type of personal data. This is especially important with DNA material, which can affect not only the right to privacy of the data holder but also of persons who are biologically related to the holder. Also, here we can acknowledge the fact that the Court's reasoning in these cases has been subject to criticism, particularly regarding the equalization of the margin of judgment for individuals who have been legally declared guilty versus those who have been acquitted or had their proceedings suspended. Nevertheless, the Court's conclusions should be supported, as they provide essential protections for personal data.

41 See *Supra* note 35, p. 438.

42 See Derenčinović *et al.*, *op. cit.*, note 4, pp. 373–404.

From the jurisprudence of the Court of Justice of the European Union, there is the joined case of "*Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*", which emphasized that the right to personal data protection is not absolute but should be evaluated about its role in society.[43] While DNA profiles do not contain personal information beyond identification, the set of identification data should be classified as personal data and protected during the process of adding it to the database, its storage, and its exchange. W Hassemer noted that the databases need to be linked to a purpose to prevent their use for any other purpose than the original one, and this principle should be included among the criminal proceedings' principles to achieve data protection. If DNA analysis is limited to establishing genetic profiles based on non-coding loci, the storage of data does not interfere with the right to privacy. However, strict rules on access, storage, use, and deletion of personal data must be established to protect them. National legislation is often not enough to ensure protection since DNA profiles cross borders. Therefore, trust in the receiving state's data protection mechanism is essential, based on the application of minimum data protection standards established by multilateral agreements, conventions, and EU law.[44]

The one criterion that stands out in the jurisprudence of both courts is the *quality of the law* criterion which is used for testing the legality, the legitimate aim, proportionality, and necessity in a democratic society elements of the case. The Quality of the law criterion understands that when measuring whether the national law truly protects the right to privacy of the individual in terms of a gathering of DNA materials, is based on: a) accessibility; b) clarity; c) foreseeability of the law. The accessibility, clarity, and foreseeability of the law are crucial for protecting the rights of individuals in any society.[45] It's interesting to note that the European Court of Human Rights (ECtHR) has not yet questioned the accessibility of the law in any case. However, member states have developed their systems to make new laws accessible to all citizens, usually through publication in a manner specified by national practice. When it comes to clarity, the scope of discretion exercised by public authorities must be reasonably clear. This means that people should have a minimum degree of protection and legal safeguards in place to prevent arbitrary implementation of the law. In universal databases, legal protections should be in place to ensure that the implementation of the law is predictable for everyone involved. Finally, sufficient foreseeability is essential to ensure that individuals know the circumstances and conditions under which authorities are entitled to act on

---

43 See: Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen,* [2010] ECR 1-11063.

44 *Ibid.,* p. 54.

45 See Primorac *et al.*, *op. cit.* note 12, pp. 3-7.

matters that affect their rights. These elements of accessibility, clarity, and foreseeability work together to protect the fundamental rights of individuals in society.

4. THE TREATMENT OF DNA MATERIALS IN THE CROATIAN CRIMINAL JUSTICE SYSTEM

As we have seen above, the jurisprudence of the ECtHR made quite substantial changes in the treatment of DNA materials in Europe in terms of shaping national and supranational legislation. The case law of the ECtHR and the CJEU has set an important precedent for countries across Europe, guiding how to balance the interests of crime prevention with the protection of personal data in line with the provisions stipulated in Article 8 of the Convention. In the context of Croatia, these judgments are especially significant considering the Constitutional Court's 2012 decision[46] to declare several provisions of the Criminal Procedure Act unconstitutional, including the implementation of molecular genetic analysis in criminal proceedings. Croatia has not been sued before the Court for violating Article 8 of the Convention, which is a very positive trend. However, a comprehensive analysis of the Court's jurisprudence can be useful in identifying potential issues in the country's legislation and practice.

4.1. National Legal Framework

In the Croatian legal system, the collection, ramification, and storage of DNA data are subject to the general principles of data protection and privacy, which are enshrined in the Constitution of the Republic of Croatia[47], the GDPR[48], the Enforcement of Prison Sentence Law[49] and the Law on Criminal Procedure[50]. This legislation requires that the collection, use, and retention of personal data, including DNA data, be lawful, fair, and transparent, and that individuals be provided

---

46 See Constitution of the Republic of Croatia, Official Gazette No. 56/1990, 135/1997, 8/1998, 113/2000, 124/2000, 28/2001, 41/2001, 55/2001, 76/2010, 85/2010, 5/2014.

47 See Constitution of the Republic of Croatia, Official Gazette No. 85/2010, consolidated text, available at:
[https://www.sabor.hr/sites/default/files/consolidated-texts/2010-Constitution%20of%20the%20Republic%20of%20Croatia%20-%20consolidated%20text.pdf].

48 See Regulation (EU) 2016/679, available at:
[https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679], Accessed 23. April 2023.

49 See Act on the execution of the prison sentence, Official Gazette No. 14/21, available at: [https://www.zakon.hr/z/179/Zakon-o-izvr%C5%A1avanju-kazne-zatvora], Accessed 23 April 2023.

50 See Criminal Procedure Code, Official Gazette No. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 130/20, 80/22, available at:
[https://narodne-novine.nn.hr/clanci/sluzbeni/2008_11_152_3484.html].

with adequate information and safeguards to protect their rights. The Constitution of the Republic of Croatia in Article 35 guarantees the right to privacy. Article 37, envisages that personal data protection and safety is guaranteed and personal data can be used only in cases designated by law. The Constitution stipulates that this right can only be limited in cases of national security or for criminal investigations, pending a court order. The General Data Protection Regulation (GDPR) applies to the processing of personal data that relates to an identified or identifiable natural person. Since 2018 the GDPR in Croatia replaced the Law on Privacy and Data Protection. The GDPR include genetic data and is considered to be a type of sensitive personal data. In the context of DNA data privacy, the GDPR imposes specific requirements on organizations that collect, process, and store genetic data. These requirements include obtaining explicit consent from the individual for the processing of their genetic data, ensuring the security and confidentiality of the data, and providing individuals with access to their genetic data. Furthermore, the GDPR establishes the principle of data minimization, which requires organizations to collect only the minimum amount of genetic data necessary for their intended purpose. This means that organizations cannot collect more genetic data than what is necessary for their specific research or medical purposes.

The Enforcement of Prison Sentence Law in Article 58 pertains to the process of collecting and storing biological samples from convicted prisoners. It stipulates that prisoners who have received a minimum prison sentence of six months for a criminal offense are required to provide a biological sample, typically in the form of DNA, to the authorities for storage in a national database. The main objective of the Law is to aid in the prevention of future criminal offenses by the same individual and to assist in the investigation and prosecution of crimes. The collection and storage of these biological samples must adhere to the Personal Data Protection Act and the Criminal Procedure Act, which provide guidelines for processing and storing personal data. It is also noteworthy that the collected samples may only be utilized to identify or verify the identity of a convicted prisoner or for use in criminal proceedings. It is important to bear in mind that the collection and storage of biological samples from prisoners under this law must be carried out by the principles of human dignity and the right to privacy, as outlined in the Croatian Constitution and the Personal Data Protection Act.

The Croatian Law on Criminal Procedure regulates the collection, use, and protection of personal data in criminal proceedings through Articles 186-188. The Law sets conditions for the permitted collection and processing of personal data, such as prohibiting the processing of personal data related to racial or ethnic origin, political beliefs, religious or philosophical beliefs, or trade union membership. Exceptions are made for personal data related to health or sexual life, which may

be processed if necessary for detecting or proving a criminal offense punishable by a prison sentence of five years or more. The law allows for periodic checks to be conducted every five years to assess the need for further retention or storage of personal data. The law also prescribes deadlines for deleting personal data, such as longer storage for legally convicted persons compared to those whose procedures ended with an acquittal, suspension, or dismissal of charges. However, these provisions do not specifically address biological samples and data collected by molecular genetic analysis. The retention of that data or DNA data profiles, according to Article 327 p.2 is dependent on the severity and length of the crimes, with more serious offenses having longer retention periods. Furthermore, the periodic review of data obtained by molecular genetic analysis is indefinite, unlike other personal data that undergo periodic review to determine whether the goal for which they were collected has reached its legitimate aim. There is the concern of lack of control mechanisms related to their collection, use, and retention as the current legal solution is opposite of the *Marper* standards established by the Court. Furthermore, there are no specific provisions that make a difference whether the DNA was taken from an adult perpetrator or a minor, and there is no provision for DNA profile deletion procedures initiated by data holders. Derencinovic argues that this is in direct contradiction to legal provisions relating to other personal data of minors and the standards established by the Court. This is contradictory to the views of the Court, which considers this type of personal data to be particularly sensitive, and therefore stricter control mechanisms related to their collection, use, and retention should be implemented compared to mechanisms for other types of personal data. Also, the provisions do not allow data holders to initiate deletion procedures for DNA profiles from databases. Rehabilitation is meant to restore a person's good name and create a fiction of previous innocence.[51] DNA profiles can be kept in databases even after the deletion of criminal records and rehabilitation, which raises concerns about the rights of innocent persons. DNA profiles can also be retained in databases for victims of criminal offenses for the same period as unconvinced persons. These issues raise questions about compliance with the standards of the European Court of Human Rights, especially after recent decisions in cases *Gaughran and Trajkovski and Chipovski, and Petrovic.* Although these judgments do not impose legal obligations on the Republic of Croatia, the interpretive dimension of the Convention as a living instrument suggests the need to review and potentially revise the legal and institutional framework for the collection, use, and retention of DNA profiles.

[51] See Derenčinović *et al.*, *op. cit.* note 4., p. 375.

4.2. Compliance of the National Legislation with the ECtHR and CJEU Standards

After the significant rulings in *the Gaughran and Trajkovski and Chipovski* cases, it presents an opportune moment to reexamine these matters and rectify any potential legislative shortcomings promptly before they are potentially subjected to scrutiny under the Court's three-part *Marper* test. First and foremost, as mentioned above it is important to highlight the Constitutional Court of the Republic of Croatia's *Decision U-I-448/2009* which declared the unconstitutionality of certain paragraphs of Article 327 of the Criminal Procedure Act due to their violation of Article 3, which pertains to the requirement that laws derive from the principle of the rule of law, in connection with Article 37 of the Constitution and Article 8 of the Convention. The Constitutional Court found the delegation of legislative powers to the heads of administrative departments to regulate the handling of data collected through molecular genetic analysis impermissible. This was especially problematic in terms of the executive power's authority to prescribe a longer storage period for such data than what is prescribed by law. Subsequently, the Criminal Procedure Act was amended in response to the Constitutional Court's decision. However, questions arise regarding the extent to which these new provisions align with the constitutional and convention norms and standards.

The Criminal Procedure Act regulates the collection, use, and protection of personal data for criminal proceedings through Articles 186-188. It outlines the conditions under which the collection and processing of personal data are allowed and specifies the types of personal data that are prohibited or exceptionally allowed. It also addresses the use of personal data in other procedures and mandates periodic reviews every five years to assess the necessity of further data retention or storage. The law is fully compliant with the GDPR and sets deadlines for the deletion of personal data, which vary depending on factors such as the outcome of the proceedings or the age of the individual. However, these provisions do not apply to the taking of biological samples and data obtained through molecular genetic analysis.

According to Article 327a paragraph 2 of the Criminal Procedure Act, data obtained through DNA analysis from a legally convicted person are retained for twenty years after the conclusion of the criminal proceedings. In cases where the offense carries a prison sentence of ten years or more, or if it involves a criminal offense against sexual freedom with a prison sentence exceeding five years, the data can be retained for a maximum of forty years. In the event of a final acquittal, suspension of criminal proceedings, or dismissal of charges, the data is kept for ten years after the conclusion of the proceedings, after which the competent authority must delete it from

the records. These provisions lack several guarantees established in the Court's jurisprudence. Is notable that the legislator distinguishes between crimes based on severity and links the retention period of the DNA profile to the imprisonment term, however, it seems less justified to treat less serious offenses and more serious ones within the same category. It would be preferable, in line with the Court's practice, to establish multiple categories of criminal offenses based on their severity and make the retention period contingent on the gravity of the offense. Moreover, unlike other personal data regulated by Articles 186-188, data obtained through molecular genetic analysis remain in databases until the expiration of the prescribed periods without the possibility of periodic reviews to reassess their continued necessity. This discrepancy contradicts the Court's view on the particularly sensitive nature of this type of data and necessitates stricter control mechanisms compared to other types of personal data. The provisions also fail to differentiate based on the age of the data subject, resulting in the same retention period regardless of whether the holder is an adult or a minor. This contradicts not only the Court's standards, especially those established about cases involving minors but also the legal provisions concerning other personal data of minors. Similarly, these provisions do not grant data subjects the opportunity to initiate procedures for deleting their DNA profiles from the database. It appears illogical and disproportionate to retain this type of personal data even after the rehabilitation period has expired. The purpose of rehabilitation is to restore a person's reputation and create the fiction of a previous conviction to facilitate reintegration and other reasons. Therefore, the current solution, where DNA profiles can be kept in databases even after the deletion of data from criminal records and the onset of rehabilitation, as regulated by the Law on Legal Consequences of Conviction, Criminal Records, and Rehabilitation, seems problematic. Ultimately, the retention of DNA profiles in Croatia's databases for up to ten years, even for individuals who are acquitted or found not guilty, raises concerns about the violation of their rights. The extended retention period for innocent individuals may not meet the test of a pressing social need before the European Court of Human Rights. This provision also raises doubts about the presumption of innocence. Additionally, the retention of DNA profiles of victims for the same duration as individuals who have not been convicted is contentious, especially considering the invasion of privacy. These issues highlight the need for Croatia's legal and institutional framework to align with the human rights standards set by the European Court of Human Rights.

5. CONCLUSION

Without a doubt, DNA analysis is commonly used in criminal investigations for identifying suspects and providing forensic evidence. However, it's crucial to recognize that forensic science is not infallible and cannot determine guilt or inno-

cence with absolute certainty. In recent years, scientific errors have been found to contribute to a concerning number of miscarriages of justice. With the rise of cross-border crime, the exchange of DNA data between countries has become necessary, leading to the establishment of national DNA databases and regulations for data sharing. Nevertheless, variations in the rules for collecting DNA samples and sharing data can create challenges. The European Union (EU) is working towards harmonizing these rules to foster mutual trust and enhance database access. One approach is to apply the requesting state's procedures to ensure the validity of evidence. The case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) has set significant precedents for shaping national and supranational legislation on the handling of DNA materials across Europe. Although Croatia hasn't faced legal action for violating Article 8 of the Convention, the jurisprudence of the ECtHR and CJEU can be instrumental in identifying potential issues within the country's legislation and practices. In Croatia, the collection, use, and retention of personal data, including DNA data, are regulated by the Law on Criminal Procedure. However, concerns arise regarding the lack of control mechanisms for DNA data collection, use, and retention, the absence of specific provisions differentiating between adults and minors regarding DNA data, and the absence of procedures allowing data holders to initiate the deletion of DNA profiles from databases. The retention of DNA profiles even after the deletion of criminal records and rehabilitation raises concerns about the rights of innocent individuals. Croatia must review and amend its legislation to ensure compliance with the standards established by the ECtHR's *Marper* judgment. Stricter control mechanisms should be implemented for the collection, use, and retention of DNA data to safeguard individuals' rights.

REFERENCES

BOOKS AND ARTICLES

1. Alleyne, L. (2009). *Interpol handbook on DNA data exchange and practice – Recommendations From the Interpol DNA Monitoring Expert Group,* Vol. 2, 2009
2. Bozhinovski, A., *Addressing Wrongful Convictions in Croatia through Revision of the Novum Criterion: Identifying Best Practices and Standards*; Mali, J (eds.), Human Rights in Contemporary Society – Challenges From an International Perspective, Vol.1 2023, available at: [https://www.intechopen.com/online-first/86866], Accessed 4 April 2023
3. Becker, S.W., Derenčinović, D., Primorac, D., *DNA as Evidence in the Courtroom*; Primorac, D. and Schanfield, M., (eds.) Forensic DNA Applications: An Interdisciplinary Perspective, 2023, pp. 433- 448
4. Derenčinović, D., Roksandić Vidlička S., Dragičević Prtenjača, M., *'Innocence Projects' and Subsequent DNA Testing in Croatia: a Possible Reality or an Unattainable Desire?*. Zbornik Pravnog fakulteta u Zagrebu, Vol. 67, No. 3-4, 2017 pp. 373–404, available at:

[https://hrcak.srce.hr/clanak/275621], Accessed 3 May 2023

5. Kaye, D.H., *Maryland v. King: Per se unreasonableness, the Golden Rule, and the future of DNA databases*. Harv. L. Rev. F., 127, 2013 p. 39-48
6. Krstulović Dragičević, A., Sokanović, L., *Načelo zakonitosti pred izazovima europskog kaznenog prava.* Zbornik radova s medunarodnog savjetovanja „Europeizacija kaznenog prava i zaštita ljudskih prava u kaznenom postupku i postupku izvršenja kaznenopravnih sankcpija", Vol. 1, 2017, Split, pp. 25-45
7. Soleto Muñoz, H., Fiodorova, A, *DNA and law enforcement in the European Union: tools and human rights protection.*, Utrecht Law Review, Vol. 10, 2014, pp. 149-162
8. Primorac, D., Primorac, D., Butorac, S. S., & Adamović, M., *Analiza DNA u sudskoj medicini i njezina primjena u hrvatskome kaznenopravnom sustavu.* Hrvatski ljetopis za kazneno pravo i praksu, Vol. 16, 2009, pp. 3-26
9. Primorac, D., Schanfield, M., *Forensic DNA applications: An interdisciplinary perspective*. CRC Press, 2023 p. 1-42
10. Romeo Casabona, C.M., *La insostenible situación del derecho penal*., Granada: Comares, 2000., pp. 45-87
11. Tseloni, A., Pease, K; *DNA retention after arrest: Balancing privacy interests and public protection*. European Journal of Criminology, Vol. 8, No. 1, 2010, pp. 32–47. doi: [https://doi.org/10.1177/1477370810372133]
12. Tuazon, O.M., *Universal forensic DNA databases: acceptable or illegal under the European Court of Human Rights regime*?. Journal of Law and the Biosciences, Vol. 8, No. 1, 2021, pp. 18-27

LEGAL DOCUMENTS

1. Act on the execution of the prison sentence, Official Gazette No. 14/21, available at: [https://www.zakon.hr/z/179/Zakon-o-izvr%C5%A1avanju-kazne-zatvora]
2. Constitution of the Republic of Croatia, Official Gazette No. 56/1990, 135/1997, 8/1998, 113/2000, 124/2000, 28/2001, 41/2001, 55/2001, 76/2010, 85/2010, 5/2014
3. Council of Europe, Committee of Ministers, Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector. Adopted by the Committee of Ministers on 17 September 1987 at the 410th Meeting of the Ministers' Deputies, available at: [https://rm.coe.int/168062dfd4]
4. Council of the European Union, Council Resolution of 9 June 1997 on the Exchange of DNA Analysis Results" [1997] Official Journal of the European Communities L193
5. Council of Europe Committee of Ministers, Recommendation No. R (92) 1 of the Committee of Ministers to Member States on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system. Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies, available at: [https://rm.coe.int/09000016804e54f7]
6. Criminal Procedure Code, Official Gazette No. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 130/20, 80/22, available at:

[https://narodne-novine.nn.hr/clanci/sluzbeni/2008_11_152_3484.html]

7. The Council of Europe's Convention for the Protection of Individuals about the Automatic Processing of Individual Data and Protocols, ETS. No. 108 +, available at:: [https://www.coe.int/en/web/data-protection/convention108-and-protocol]
8. The Stockholm Programme [2010] OJ C 115 available at: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF]
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679]

ECtHR and CJEU CASES:

1. *Aycaguer v France* (2017), application no. 8806/12, 22 June 2017, available at: [https://hudoc.echr.coe.int], Accessed 3 April 2023
2. *Dragan Petrovic v Serbia* (2020), application no. 75229/10, available at [https://hudoc.echr.coe.int], Accessed 4 April 2023
3. Court of Justice of the European Union, Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen, Cases C-92/09 and C-93/09, [2010] ECR I-11063
4. *Gaughran v the United Kingdom* (2020), application no. 45245/15, 13 February 2020, available at: [https://hudoc.echr.coe.int], Accessed 3 April 2023
5. *S. and Marper v United Kingdom* (2008), application no. 30562/04 and no. 30566/04, 4 December 2008, available at: [https://hudoc.echr.coe.int], Accessed 3 April 2023
6. *Trajkovski and Chipovski v North Macedonia* (2020) application no. 53205/13 and no. 63320/13, available at: [https://hudoc.echr.coe.int], Accessed 1 April 2023