

This article is published in a peer-reviewed section of the Utrecht Law Review

## DNA and Law Enforcement in the European Union: Tools and Human Rights Protection

Helena Soletó Muñoz  
Anna Fiodorova\*

### Introduction

Since its first successful use in criminal investigations in the 1980s, DNA has become an important tool to identify the guilty and to absolve the innocent. It provided the impetus to set up national DNA databases and legal provisions to use DNA-related data as forensic evidence.

Today, given the prospect of an increasingly interconnected society, in which technical resources and technological advances allow a confusingly fast flow of people and instantaneous information on a worldwide level, the evolution of the phenomenon of crime is not lagging behind, but is keeping in step with the process of transnationalisation and is taking advantage thereof.

In view of this situation, the investigation and prosecution of crime have to overcome borders by means of various judicial and police cooperation instruments, in particular those on mutual assistance and information exchange.

One of the most important boosts provided over the last few years in combating transnational crime has been the development of the Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (the Prüm Treaty) and its partial transformation into a EU-wide cooperation tool under Council Decision 2008/615/JHA<sup>1</sup> and Council Decision 2008/616/JHA.<sup>2</sup>

Within this cooperation framework, the exchange of DNA profiles and related personal data acquires great relevance, given the usefulness and universality of the information it offers for investigations and prosecutions. However, there is also a grey area concerning this issue, as it poses a series of risks for fundamental rights and not all aspects of DNA collection, analysis and exchange are unified on the EU level while national provisions vary a great deal.

---

\* Prof.Dr. H. Soletó Muñoz, email: [helena.soletoto@uc3m.es](mailto:helena.soletoto@uc3m.es), is Professor of Procedural Law at University Carlos III in Madrid, and a former adviser at the National Commission for forensic DNA, Spain. A. Fiodorova LLM, email [anna.fiodorova@uc3m.es](mailto:anna.fiodorova@uc3m.es), is a researcher and PhD candidate in Law at University Carlos III in Madrid (Spain), and a former counsellor in Justice and Home Affairs at the Permanent Representation of Lithuania to the European Union. The research for this paper ended in July 2013.

1 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008. p. 1.

2 Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008. p. 12.

The article aims to:

- present the importance of DNA-related data for criminal investigations;
- study the EU information exchange dimension in this area and to discover the possible reason for its success;
- analyse which DNA collection, analysis, use and storage aspects are regulated by EU and national law and how they vary; and
- examine possible violations of or limitations to fundamental rights while using DNA for criminal investigation purposes.

## **1. DNA as data which are of interest in crime investigation and prosecution**

The first conviction based on DNA profiling evidence took place in 1987 in England. Colin Pitchfork was thereby sentenced to life imprisonment for the rape and murder of two girls.<sup>3</sup>

In many cases of violent crime body fluids are transferred between the victim, the suspect and the crime scene and DNA profiling could be a key element in the investigation.<sup>4</sup> Thus far, DNA profiling has been very valuable in the investigation and prosecution of homicides and rapes, especially those that amount to serial crimes. For example, in the well known case of the rape and murder of a 13-year old English girl, Caroline Dickinson, in Pleine Fourgeres (Northern France), the attacker was of Spanish nationality, with a criminal record in the United Kingdom and he had committed similar attacks in Unites States of America (USA). An American civil servant had read about the crime in the UK, linked it through the modus operandi with the crimes committed in the USA, and the identification of the perpetrator was later confirmed through DNA analysis. In this case, DNA profiling assisted in not only finding the real offender, but also in acquitting another suspect.<sup>5</sup>

In 2010 DNA profiling helped to identify and convict an Afghan national of committing a number of violent sex attacks in California between 2002 and 2004 and of a rape in Austria in 2009.<sup>6</sup>

Very recently DNA samples proved to be useful in an investigation into the ‘Boston Strangler’ case – rapes and murder committed in 1964: ‘Analysis of the DNA samples extracted from a water bottle drunk by the suspect’s (died in 1973) nephew showed a strong family link to DNA recovered from the crime scene. This allowed the authorisation of the exhumation of the suspect’s body for the final DNA testing.’<sup>7</sup>

The practice also reveals the utility of DNA profiling in some investigations related to organized crime as well. According to information by the International Criminal Police Organization (INTERPOL) in the case of the organised gang ‘Pink Panthers’ ‘DNA samples recovered from crime scenes in France, Liechtenstein, Switzerland and the United Arab Emirates revealed links between three different types of crime – armed robbery, prison escape and the use of forged travel documents – and between a group of individuals.’<sup>8</sup>

According to INTERPOL’s Global DNA Profiling Survey 2008, 120 countries use DNA profiling in criminal investigations, 54 of them have national DNA databases and 26 plan to introduce a national DNA database.<sup>9</sup>

---

3 See <<http://www.exploreforensics.co.uk/forensic-cases-colin-pitchfork-first-exoneration-through-dna.html>> (last visited 30 November 2012).

4 See L. Alleyne et al., *INTERPOL Handbook on DNA Data Exchange and Practice. Recommendations from the INTERPOL DNA Monitoring Expert Group*, 2009, p. 7.

5 See the speech by John Dickinson ‘Why the international exchange of DNA is important’ at the 5th International DNA users’ conference for investigative officers, available on <<http://www.interpol.int/News-and-media/Speeches#n5734>> (last visited 25 October 2012).

6 <<http://www.interpol.int/News-and-media/News-media-releases/2011/PR103>> (last visited 7 July 2013).

7 <<http://www.reuters.com/article/2013/07/11/us-usa-crime-bostonstrangler-idUSBRE96A00820130711>> (last visited 17 July 2013).

8 <<http://www.interpol.int/INTERPOL-expertise/Forensics/DNA>> (last visited 30 November 2012).

9 Ibid.

For example, in Spain a comprehensive juridical structure regulating databases for identifiers obtained from DNA was established by Organic Law 10/2007.<sup>10</sup> Until then databases that included DNA profiles were functioning outside a specific and unified nationwide set of regulations.<sup>11</sup>

## 2. Transnational DNA-related data exchange: a focus on the European Union

The contemporary trend of globalization and the openness of movement and communications has its dark side as it is being used to facilitate the preparation and commitment of crime and to escape from justice.

The examples provided in the previous part show that the collection of DNA samples and their analysis provides only partial advantages for the investigation; more advantageous is the possibility of their cross-border exchange and comparison.

On 9 June 1997 the Council of Europe adopted a Resolution on the exchange of DNA analysis results and invited EU Member States to establish compatible national DNA databases in order to exchange data from the non-coding part of the DNA molecule.<sup>12</sup> Later, the Council Resolution of 25 June 2001 on the exchange of DNA analysis results<sup>13</sup> (with the relevant amendments made in 2009)<sup>14</sup> established a minimum number of DNA markers (loci) that have to be used for forensic analysis.

Outside the EU, interest is also being shown in the exchange of DNA files: 'the G8 Ministers have commented on the importance of using DNA-based evidence in the investigation of terrorism and other crimes, and urged their experts to continue to examine ways of improving the exchange of this kind of data'.<sup>15</sup>

Not long ago DNA profiles were only exchanged on an individual basis through different cooperation channels: by sending requests to other countries through INTERPOL's or the European Police Office's (Europol) national units and liaison officers, through bilateral or multilateral liaison officers posted in foreign countries or regions, or other legally established ways (mainly on the basis of bilateral or multilateral agreements).

The exchange of individual DNA profiles, however, does not prove to be very useful; first of all, the request must be made to each state which is thought likely to possess information, or in some cases there is no clue as to the possible geographic location of the sought DNA profile and different channels are needed to send a request, and secondly, the requesting authority is not permitted to search for and compare profiles and the whole administrative burden of a search and comparison falls on the shoulders of the requested country.

This situation changed a decade ago with the establishment of INTERPOL DNA Gateway and the development of an automated DNA profile searching system within the EU that will be the object of the following analysis.

### 2.1. Cooperation in the EU

In May 2005 Austria, Belgium, France, Germany, Luxemburg, the Netherlands and Spain signed the Prüm Treaty on the stepping up of cooperation to combat terrorism, cross-border crime and illegal

---

10 Organic Law 10/2007 of 8 October regulating the police database for identifiers obtained from DNA (*Ley orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN*), *Official State Gazette* No. 242, 9.10.2007, pp. 40969-40972.

11 However, various police forces were already in possession of DNA databases prior to the above-mentioned law coming into force. Firstly, for the purposes of criminal investigations, as was the case with the 'ADN-Veritas' file system managed by the National Police Force and the analogous 'ADNIC' that was used by the Civil Guard and which were unified by means of the national police database created in October 2007 as provided for by Organic Law 10/2007, a milestone was reached which was made possible thanks to the efficient implementation of the SUBA unification project, within a policy of improving the coordination of the two law enforcement authorities with a view to revising the files and sharing them, which started in 2005. And, secondly, for humanitarian purposes, with reference to the collection and comparison of samples relating to missing persons and in situations where natural disasters may have occurred. This is also the case with the current databases – the Civil Guard's 'FENIX' archive and the National Police Force's 'ADN-HUMANITAS'.

12 Council Resolution 97/C 193/2, OJ C 193, 24.6.1997, p. 2.

13 Council Resolution 2001/C 187/01, OJ C 187, 3.7.2001, p. 1.

14 Council Resolution 2009/C 296/1, OJ C 296, 5.12.2009, p. 1.

15 National DNA Database Strategy Board, United Kingdom, *National DNA Database Report 2005-2006*, 2006, p. 43.

migration. The main objective of the Treaty was to enhance cooperation by a system of exchanging information, including DNA-related data.

Subsequently, some other EU Member States joined the Prüm Treaty, and finally, with the initiative of Germany in 2007, many of its provisions had been approved by the Council of the European Union as Council Decisions and became part of the *acquis communautaire*.<sup>16</sup> 'It supposes to offer legal and technological instruments to fight terrorism and international crime more efficiently, compensating potential negative spill-overs of the Schengen area'.<sup>17</sup>

Council Decision 2008/615/JHA obliges EU Member States to establish national databases and provides for rules for the competent authorities of other EU Member States to search in national DNA, dactyloscopic and vehicle registration databases and is the first EU instrument that foresees direct access to the national databases of other countries.

It is important to point out a distinction between direct access to a DNA database and direct access to all the data stored in a DNA database. Member State A is allowed to search for a DNA profile in Member State B's DNA database and receives either a positive or negative reply (hit/no hit) 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 A directly receives only reference data that can be called 'anonymous',<sup>18</sup> but there is *no direct access* to data related to the matched DNA profile. In order to obtain personal data from the DNA database it must send an additional request to Member State B.

That means that the searching Member State will never obtain data about a DNA profile that does not match the one submitted for the search and personal data will only be provided on the basis of a DNA profile match and the provision of additional information about the purpose of obtaining this data.

The procedure for obtaining data related to the 'hit' depends on the national law of the requested Member State and this could be carried out according to mutual assistance procedures, bilateral agreements on information exchange, Council Framework Decision 2006/960/JHA<sup>19</sup> and other legal instruments. It means that at the 'post-hit' stage relative information will be provided according to the rules on law enforcement or judicial cooperation, depending on the national law of the requested Member State and whether the requesting Member State will only use this information for an investigation or also for prosecution purposes. In the latter case, 'post-hit' information exchange will usually take the form of judicial cooperation. In all cases the establishment of 'hit' and 'post-hit' stages allows Member States to maintain absolute control over the data associated with DNA profiles.

In the context of DNA profile exchanges, under Council Decision 2008/615/JHA a few additional issues should be mentioned. First of all, only designated contact points that are usually either forensic science services, as they have direct contact with and expert knowledge on DNA profiles, or law enforcement units responsible for information exchange can perform searches in the national DNA databases of other countries. Secondly, Article 4 of Council Decision 2008/615/JHA allows a comparison, prior to bilateral consent, of the unidentified DNA profiles from one EU Member State with all DNA profiles from another national DNA database for the investigation of criminal offences.<sup>20</sup>

The DNA-related data exchange mechanism established by the Prüm Treaty and Prüm Decisions differs a great deal from the international mechanism applied by INTERPOL. INTERPOL has its own DNA Database, but it acts simply as a channel for the exchange and comparison of information between

16 In comparison with the Prüm Treaty, Council Decisions do not include provisions on illegal migration and 'air marshals'.

17 R. Bellanova, 'The "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange?', in E. Guild & F. Geyer (eds.), *Security versus Justice? Police and Judicial Cooperation in the European Union*, 2008, p. 204.

18 See M. de Hoyos Sancho, 'Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos', in C. Arangüena Fanego (ed.), *Espacio Europeo de Libertad, Seguridad y Justicia: Últimos avances en cooperación judicial penal*, 2010, p. 162.

19 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89.

20 This kind of cooperation and direct access to the national databases is also followed in the European Criminal Records Information System (ECRIS). Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33) sets up a communication system in which the EU Member States retain access to their Criminal Records' databases; a new database is not created, but rather a homogenous computerized system for direct access through the central authorities. In addition to data about criminal records, the transmission of other personal data such as fingerprints, amongst others, is allowed and makes it possible to identify the subject, and so this is a possibility with regard to DNA profiles. This system was launched in April 2012.

different states, without nominal data linking the DNA profiles contained therein to specific persons and each country retains ownership of its DNA profile data and has a responsibility to process it according to national law.<sup>21</sup>

The level of the use of both mechanisms facilitating DNA-related data exchange is reflected in the table below on the basis of statistics from 2012.

<i>Statistics on the exchange of DNA-related data from 2012</i>		
	Exchange under Prüm Decisions*	Exchange through the INTERPOL DNA Database**
Number of countries providing DNA profiles	16 operational 3 authorised	67
Number of DNA profiles available for the exchange	4,358,904	136,000
Number of 'hits'	52,507	84

\* Council document ST 7146/2/13.

\*\* See <<http://www.interpol.int/INTERPOL-expertise/Forensics/DNA>> (last visited 17 July 2013).

There could be different reasons for such a huge difference in figures. Firstly, as the countries have to submit information about DNA profiles to the INTERPOL DNA Database and retain control over the destruction of and access to the DNA profiles by other countries, this is an additional administrative burden in addition to the maintenance of national databases. Secondly, the requested country has to check whether its requesting counterpart fulfils data protection requirements, whether the data provided will be used in accordance with its purpose, etc. Thirdly, in most cases EU Member States first consult the national databases of other EU Member States, as due to free movement within the Schengen area there is a major probability that a person has remained within the EU.

But the most important reason for such a significant difference is mutual trust among countries.

## *2.2. Mutual trust – the reason for an efficient DNA data exchange in the EU*

The Stockholm Programme emphasises that mutual trust is a tool which is necessary for efficient cooperation between law enforcement bodies, judicial authorities and decision-makers.<sup>22, 23</sup>

In the case of DNA data exchange mutual trust means:

- Trust in the searching country that searches of DNA profiles will be performed and DNA-related data will be used strictly for the purposes for which it was provided, with respect for human rights and appropriate legal and technical measures for data protection.
- Trust in the requested country that the data provided is accurate and has been obtained according to the law and using appropriate technical standards.

Article 25(2) of Council Decision 2008/615/JHA establishes that the supply of personal data may not take place until data protection provisions are implemented in national law and the Council unanimously decides concerning every Member State and every category of data exchanged (DNA, dactyloscopic data, vehicle registration data) whether this condition has been met.<sup>24</sup> According to Article 20 of Council Decision 2008/616/JHA the Council takes its decision on the basis of an evaluation report which is prepared by experts from the already operational Member States. The report is based on information

21 See M.J. Cabezedo Bajo, 'La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal', in A. De la Oliva Santos et al. (eds.), *La justicia y la carta de derechos fundamentales de la UE*, 2008, pp. 327-342.

22 The Stockholm Programme, OJ C 115, 4.5.2010, p. 5.

23 Since several decades one of the main pillars for cross-border cooperation between the Nordic countries has been mutual trust and it has proved to be one of the main aspects of its success. See more in H. Fode, 'Cooperation on Law Enforcement, Criminal Justice and Legislation in Europe: Nordic Experience', in H.G. Schermers et al., *Free Movement of Persons in Europe*, 1993, p. 65.

24 It should be noted that this requirement is not applied to Member States that have started to exchange data under the Prüm Treaty.

in a questionnaire, an evaluation visit and a pilot run of the relevant database and it states whether the evaluated Member State has established a data protection system and technical and legal requirements for making automated searches and obtaining data from other EU Member States and whether its database is compatible with the databases of other Member States. This means that before giving the Member State in question direct access to national DNA databases and the right to exchange DNA-related information, other Member States have a possibility to become acquainted with the level of its 'trustworthiness'.

Besides this, in 2009 Council Framework Decision 2009/905/JHA was adopted.<sup>25</sup> Its goal is the accreditation of EU Member States' forensic laboratories to the same EN ISO/IEC 125 standard so that the results of their activities (DNA profiles and dactyloscopic data) can be recognized and treated as being equally reliable in other EU Member States.<sup>26</sup> The accreditation of EU Member States' forensic laboratories to the same standard will significantly contribute to mutual trust concerning DNA collection and analysis and the quality of DNA profiles and related data.

### **3. DNA use for crime investigation vs. fundamental rights**

#### **3.1. Possible violations of fundamental rights**

DNA sample collection, analysis, its submission to a DNA profile database, and a search and comparison are linked to fundamental rights.

Fundamental rights can be affected at various stages: firstly, when the DNA sample is taken, and secondly, when it is analysed. At these stages the limitation of these rights is different depending on whether the analysis is performed with respect to a known person or is carried out on material left behind by an unknown subject, because when the DNA profile is obtained from the crime scene or the victim, the key datum of identification is missing, and therefore no limitation exists with regard to the contents of the profile or its presence on a database.

Thirdly, citizens' rights can be limited when DNA profiles are submitted and processed (including in a search) in databases, and fourthly, on every occasion the data are transmitted to another country.

With the collection, analysis and processing of DNA profiles different fundamental rights could be violated, e.g. the right to physical and moral integrity, the right not to be subject to degrading treatment, the right not to incriminate oneself, the right to family privacy together with that of not incriminating descendants or relatives in general, the right of children to personal development and the right to informative self-determination.

According to Article 52 of the Charter of Fundamental Rights of the European Union, limitations on fundamental rights are allowed if they are '(...) subject to the principle of proportionality, (...) if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.<sup>27</sup>

As DNA-related data are usually helpful instruments in the investigation of crimes that threaten the security of society some limitations to fundamental rights are allowed in this regard.

It has to be said that international legislation, with the exception of data protection, usually does not specify possible limitations on fundamental rights, but leaves this to the jurisprudence of national and international courts and national legislation.

In national legislation, such limitations on fundamental rights are in principle justifiable and proportional in the context of criminal proceedings, provided they are subject to the guarantees established in international and internal procedural regulations. For example, in Spanish legislation the proportionality criterion has partly been covered by establishing the possibility of collecting samples and storage profiles in a database when these are related to serious crimes, the identification of corpses and inquiries into missing persons.

Thus, if a DNA has been collected and its profile stored according to the regulations, a limitation on the rights of the subject is justified.

<sup>25</sup> Council Framework Decision 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities, OJ L 322, 9.12.2009, p. 14.

<sup>26</sup> Measures on laboratories' accreditation related to activities with DNA profiles have to be implemented by 30 November 2013.

<sup>27</sup> Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000, p. 21.

Carrying out a search in the database by national competent authorities fulfils the natural purpose of the database and so the act is justified, providing it is performed in accordance with the criteria of reasonableness and proportionality, which would exclude, for example, a search for family members.

The transfer of DNA profiles and related data to another country is more complicated in view of fundamental rights as the principle of proportionality has to be assured by the law of both countries involved and not only by means of national law, but also international legal provisions common to those countries.

Council Decision 2008/615/JHA establishes broad rules on opening DNA files and the storage of DNA profiles for the purpose of investigating criminal offences, without specifying whether the criminal offence is serious or not. But it does not prohibit Member States from establishing stricter rules on DNA database content, as is done, for example, in Spain, limiting it to only DNA profiles related to serious crimes. Nevertheless, on the basis of Council Decision 2006/615/JHA, other EU Member States are allowed to make automated searches for DNA profiles for the investigation of any criminal offence without specifying whether it is serious or not. But in order to obtain personal data related to a matched DNA profile stricter national rules by the requested country are often applied, as the exchange of information and data depends on the laws and limitations of the Member State whose DNA database is being searched, for example if an automated search has been made for the investigation of any kind of crime and has resulted in a 'hit', Spain will only provide DNA-related data if the search was related to a serious crime.

### 3.2. DNA sample collection and fundamental rights

It must be stressed that, as mentioned previously, the collection of samples from a suspect, whether that suspect has been arrested or is accused, represents the first of several possible infringements of fundamental rights, although the taking of samples in order to analyse DNA has traditionally fallen within the same category as external body searches or intrusive body searches involving physical intervention, depending on the degree of invasion the collection of the sample involves.

Consequently, it could be said that the fundamental rights that would be threatened with regard to the collection of samples, as the first step to be carried out in order to obtain DNA evidence, are the right to physical and moral integrity, the right not to be subjected to degrading treatment, the right to privacy and the right to non-self-incrimination.

With regard to the right to physical integrity, evidently it is not affected by the collection of saliva or hair samples, the most common samples which are taken these days, unlike other forms of physical intervention.

Concerning the right not to be subjected to degrading treatment, it is evident that there is no breach if the procedure itself cannot harm the person's dignity, provided it is performed within the framework of respect for the citizen.

With regard to self-incrimination, submitting samples for DNA analysis is very similar to alcohol-measuring or blood test analyses and both international and national jurisprudence do not consider such procedures to amount to self-incrimination. For example, the former European Commission on Human Rights in case *X. v the Netherlands* recognized that submission to a blood test does not constitute a presumption of guilt which contravenes Article 6(2) of the European Convention on Human Rights.<sup>28</sup> As the results of the test could be positive or negative, this method of proof can be 'an advantage or disadvantage for the accused'.<sup>29</sup>

According to the case law of the Spanish Constitutional Court (*Tribunal Constitucional*, TC) there is no relation between the right not to incriminate oneself and the right not to submit to such a test, and given that 'these analyses cannot be considered as, nor are, comparable to making a statement, not only does the right not to submit to them not exist, but in fact there is an obligation to do so'.<sup>30</sup> The TC makes

28 European Convention for the Protection of Human Rights and Fundamental Freedoms, [213 U.N.T.S. 221, E.T.S. 5].

29 *X. v the Netherlands*, [1978] ECHR (D.R. 15), p. 5

30 The Spanish Constitutional Court's case law: judgment 107/1985, *Official State Gazette* No. 265, 2.11.1985, p. 23; judgment 103/1985, *Official State Gazette* No. 265, 2.11.1985, p. 11; judgment 195/1987, *Official State Gazette* No. 309, 26.12.1987, p. 25; judgment 76/1990, *Official State Gazette* No. 129, 30.5.190, p. 13; judgment 161/1997 *Official State Gazette* No. 200, 30.10.1997, p. 69.

a reference to the 'generic legitimacy the authorities have, in this kind of action, to proceed to investigate, by means of the judicial police, the detection of the commission of crimes, the aim or object which the study of the DNA of a person who could be classified as a suspect in a crime clearly serves'.<sup>31</sup>

In conclusion, it could be said that only 'the right to privacy and the consistent rights to informative self-determination and genetic identity could be affected by the collection of DNA samples'.<sup>32</sup> As these rights are closely related to data protection, they will be touched upon in Section 4.

### 3.3. Heterogeneity in procedural DNA sample collection guarantees

In order to be admitted as evidence, DNA samples shall be collected according to the rules of the criminal process that are established by national legislation that determines from whom and subject to which conditions they can be taken. As the penal policies of different countries greatly vary, there are also differences in DNA sample collection guarantees.

For example, in the Spanish system there is a dual requirement for the legitimacy of proceeding to take a sample, namely, that the passive subject must at least be suspected<sup>33</sup> of having committed an offence in the context of an investigation, and that the offence should be of sufficient importance, or seriousness, thus guaranteeing the principle of proportionality in the limitation of citizens' rights.

In general, the category of being a suspect is not defined and does not exist as such in Spanish law, unlike in other countries, for example Portugal – remember the case of Madeleine McCann<sup>34</sup> – but its use in practice has been adopted by the law, which implies legal acceptance for the status of being a suspect. This term has crept into the Spanish Law of Criminal Procedure (*Ley de Enjuiciamiento Criminal*, LECrim)<sup>35</sup> from police practice, justified by the procedural need to allocate a category to persons who are subject to the measure, even if they have not been formally charged, as this must be normal practice where the measure is applied at a stage when the evidence against a person is not strong enough to actually accuse him or her. Article 363 of LECrim foresees that if a person refuses to provide a DNA sample, the police can apply to a judge for an order or warrant requiring the person to provide a sample. In this case no more would be required than the category of a passive subject being a 'suspect'.<sup>36</sup>

Additional Provision 3 of Organic Law 10/2007 also refers to the status of 'under arrest' regarding persons who are subjected to having a sample taken, and in this case their right to defence is guaranteed.

The Supreme Court's (*Tribunal Supremo*) case law during the last few years has explained the peculiarities of a sample collection from detainees that requires corporal intervention.<sup>37</sup> The judicial police can obtain saliva or other fluids for which corporal intervention is needed only when the assistance of a lawyer is assured and a detainee gives his consent. The requirement of assistance by a lawyer has appeared in the case law since 2010 and is based on the constitutional rights for effective defence and the process concerning all guarantees. If no consent is given to samples being taken, they can only be obtained on the basis of judicial authorisation. These requirements are not applied to the taking of samples where corporal intervention is not required, e.g. collecting samples left behind by the detainee.

In the first half of 2013 the Supreme Court of the United States in the case of *Maryland v King* stated that in the case of an arrest supported by probable cause which justifies holding the suspect on

31 J. López Barja de Quiroga, 'El derecho a guardar silencio y a no inculparse, in Derechos procesales fundamentales', 2005 *Manuales de Formación Continua*, no. 22, p. 617.

32 J.F. Etxebarria Guridi, *Los análisis de ADN y su aplicación al proceso penal*, 2000, pp. 61, 190, refers to the right to informative self-determination and genetic identity, originating from the right to privacy or a private life. Similarly, J. Moreno Verdejo, 'ADN y proceso penal: análisis de la reforma operada por la Ley Orgánica 15/2003, de 25 de noviembre', 2004 *Estudios Jurídicos*, p. 1803.

33 In Additional Provision 3 of Organic Law 10/2007, a person who is subject to the obligation to provide a sample is described as 'a suspect, a person under arrest or an accused'.

34 In the case of the disappearance of the infant Madeleine in the Algarve, Portugal, her parents were formally declared to be 'arguidos', or suspects, and had the right to remain silent and to legal representation and, furthermore, suspects can be subject to mild precautionary measures such as limitations on their personal liberty, in the form of being required not to leave a certain location, etc.

35 Law on Criminal Procedure promulgated by the Royal Decree of 14 September 1882, *Official State Gazette* No. 260, 17.9.1882, p. 803.

36 E. Cortés Bechiarelli, 'Muestras biológicas abandonadas por el sospechoso y validez de la prueba de ADN en el proceso penal: o sobre la competencia legislativa de la Sala Segunda del Tribunal Supremo', 2006 *Revista Penal*, no. 18, p. 53, considers that the status of suspect must be limited to cases in which there is a circumstantial connection between the subject and the events giving rise to the proceedings, and that it would have been more accurate if the law had referred to the accused.

37 Spanish Supreme Court judgment 685/2010, <<http://supremo.vlex.es/vid/-233213306>> (last visited 12 December 2012), Spanish Supreme Court judgment 827/2011, <<http://supremo.vlex.es/vid/334186094>> (last visited 12 December 2012).

suspicion of having committed a serious crime, the collection of DNA samples from the arrestee is, just like fingerprinting and photographing, a legitimate police booking procedure. It also compares DNA sample collection with searching a person and as a lawful arrest authorises a search, it can also be treated as authorisation for DNA sample collection.<sup>38</sup> It has become a revolutionary opinion giving the green light to collect DNA samples from an arrestee without his consent and without judicial authorisation if he has been lawfully arrested and in relation to a serious offence.

According to British legislation, if someone is arrested, the police also have the capacity to collect DNA samples, subsequently influenced by the question of whether the criminal act is of a 'recordable' nature or not, i.e. liable to be recorded on the police computer in accordance with the regulations in force at the time. Bearing in mind the fact that nowadays almost all crimes are of this nature, this could lead to mass sample collection or, to put it another way, affect many people, based on them committing some kind of offence, irrespective of its gravity.

In the same way one can observe significant disparities between the different national legislations regarding suspects under the age of eighteen. Spanish law does not refer to whether minors are subjected to the collection of DNA samples and both doctrine and the public clearly have different opinions, as it is thought that this could represent a more serious intrusion into their personal lives than would be the case for an adult.

In the United Kingdom this is widespread practice, as well as in many States in the USA, where samples are taken depending on the gravity of the offence, and are almost always taken with regard to sexual offences despite the age of an arrestee.

Due to the sensitive nature of this issue additional guarantees should be applied, such as the consent of the minor and his/her parents, guardian or defence lawyer, or judicial authorization, and subject to the condition that it is in connection with an investigation into a serious crime.

### 3.4. Database storage requirements

Once the DNA profile is added to the database, it is subjected to a comparison and subsequent storage. Collected DNA samples (cellular material) are also kept. The question of storage is usually more controversial than the collection of DNA samples and could affect: the right not to incriminate oneself, the right to family privacy together with that of not incriminating descendants or relatives in general, the right of children to personal development and the right to informative self-determination. In the case of *S & Marper v United Kingdom* the European Court of Human Rights (ECtHR) has stated that while the original taking of the DNA sample aims to link a particular person with a particular crime, the retention of cellular material and the DNA profile 'pursues the broader purpose of assisting in the identification of future offenders.'<sup>39</sup>

The ECtHR considers that the storage of cellular material is more dangerous for the right to privacy than the storage of the DNA profile, as an analysis of cellular material can reveal much more personal data.

The most controversial question is related to the storage of cellular material and DNA profiles that belong to acquitted persons. The legislation of some countries (Belgium, Hungary, Ireland, Italy and Sweden) requires such information to be destroyed upon acquittal and the discontinuance of the criminal proceedings. Other countries (Germany, Luxembourg, the Netherlands) permit the retention of DNA profiles where there are still suspicions about the person or if further investigations are needed in a separate case.<sup>40</sup> The case of *S & Marper v United Kingdom* reveals the position adopted by the ECtHR in that the unlimited retention of such data is not justifiable and results in a violation of the right to privacy.

But the situation changes if the DNA profile belongs to a convicted person. In its decision in the case of *Van der Velden v the Netherlands* the ECtHR stated that if compilation and retention of a DNA profile serves the legitimate aims of the prevention of crime and the protection of the rights and freedoms of others, it can be stored even if it 'played no role in the investigation and trial of the offences committed'.<sup>41</sup>

38 *Maryland v King*, 569 US (2013) (not yet reported).

39 *S and Marper v United Kingdom*, [2008] ECHR, p. 6

40 *Ibid.*

41 *Van der Velden v the Netherlands*, [2006] ECHR, p. 335.

*S & Marper v United Kingdom* also deals with the storage of minors' DNA profiles. S was a minor whose sample was collected when he was aged 11 as part of an investigation into an attempted robbery; he was acquitted, but his samples and DNA profile were retained in the custody of the police indefinitely and against his will. The ECtHR stated that juveniles should be protected from any detriment that may result from the retention of their private data by the authorities following an acquittal from a criminal offence.

The storage of the DNA profiles of minors should be different from the storage of the profiles of adults. The best option would be the creation of a special database containing minors' profiles, provided that these are destroyed when they reach the age of majority. Similarly, the storage of profiles should be excluded automatically when minors have not been convicted or are declared non-imputable – not liable for prosecution – and, if they are prosecuted, their files should receive special treatment.

Different from the process of DNA sample collection, the storage of DNA profiles is regulated not only by national legislation. Recommendation No. R(92)1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system<sup>42</sup> and Council Decision 2008/615/JHA establish a specific set of rules on the use and storage of DNA profiles. The Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data<sup>43</sup> and its Additional Protocol foresee general rules on the storage of automatic processing of personal data.

## 4. Data protection

### 4.1. Current data protection rules on DNA-related data

One of the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights, is the right to the protection of personal data.

The Court of Justice of the European Union in the joined case of *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen* underlined that the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.<sup>44</sup>

DNA profiles do not offer personal information beyond identification itself, but the set of identification data can be classified as personal data and have to be protected at the stage of adding the DNA profile to the database, its storage, and consultation and exchange.

In view of the panorama surrounding these issues, W. Hassemer has noted that there has to be a 'linking' of the databases 'to a purpose', preventing their use for any purpose other than the original one, and he claims that only when this principle is included amongst those of criminal proceedings can data protection be achieved therein.<sup>45</sup> Thus, if DNA analysis is limited to establishing genetic profiles based on the loci, with non-coding content, the storage of data will not lead to an interference with the right to privacy, although it will do so with regard to the informative self-denomination issue, but only to the same extent as other databases such as lophoscopic ones, the legitimacy of which is not questioned.

To protect personal data strict rules on their access, storage, use and deletion have to be established. In the case of DNA-related data national legislation is not sufficient as very often a DNA profile travels beyond the borders of the state of its origin and after crossing the border the state then lacks the necessary competence to control the data protection regime. In this case it helps if there is trust in the data receiving state and its data protection mechanism. The basis of this trust is the application of the same minimum data protection standards established by multilateral agreements, conventions and EU law.

Council Framework Decision 2008/977/JHA<sup>46</sup> lays down the main principles in *transnational* information exchange (lawfulness, proportionality and purpose). But its Recital 39 foresees that it does

---

42 <<https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2>> (last visited 10 July 2013).

43 Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108, Strasbourg, 28.1.1981].

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

45 W. Hassemer, '¿Proceso penal sin protección de datos?', in R. Casabona, *La insostenible situación del Derecho Penal*, 2000, p. 127.

46 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

not affect data protection provisions in acts such as those governing the functioning of Europol, Eurojust, Schengen or the Customs Information System and Council Decision 2008/615/JHA as well.

The title of Council Decision 2008/615/JHA defines the purpose of cross-border cooperation: ‘combating terrorism and cross-border crime’ that at the same time is the basis for automatic search and data exchange. Article 3 specifies that the automated search of DNA profiles in the database of another EU Member State can be conducted for the investigation of individual cases of criminal offences. Its Chapter 6 establishes general provisions on data protection and includes requirements on: the purpose for which a search and data exchange are conducted, the authorities which are competent to exchange data, the storage of data, technical and organisational measures to ensure data protection and data security, and a data subject’s rights to information and damages. But it does not regulate such issues as data transfer to private parties, third states or international bodies and according to Recital 40 of Council Framework Decision 2008/977/JHA, for the aspects not regulated by specific acts, the rules of this Council Framework Decision should be applied.

Both legal acts establish quite similar principles on data protection, but Council Decision 2008/615/JHA goes one step further by ensuring that the principles and minimum data protection standards are in force and in Article 25 it lays down that a EU Member State can only participate in the DNA data exchange process after the Council’s unanimous decision that this Member State fulfils all the data protection requirements. As was mentioned in Section 2.2 such a decision is taken by the Council on the basis of an evaluation visit, a pilot run and the relevant report on the EU Member State’s legal and technical readiness to make searches of DNA profiles and to exchange DNA-related data.

Such a requirement is advantageous as every EU Member State is obliged to fulfil all data protection requirements in order to be allowed to use this crime-combating instrument with direct access to EU Member States’ databases and a further exchange of data.

Different from Council Decision 2008/615/JHA, Council Framework Decision 2008/677/JHA does not have measures to control and to force EU Member States to apply EU-level data protection rules. According to the Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29(2) of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters adopted on January 25 2012 (three years after the adoption of Council Framework Decision 2008/977/JHA), only 14 EU Member States indicated that they had implemented it, 9 had implemented it partially, 3 had not implemented it at all while 1 had not replied.<sup>47</sup> This leads to the conclusion that those data protection aspects that are not covered by Council Decision 2008/615/JHA are regulated only by national legislation, as the standards foreseen in Council Decision 2008/977/JHA are barely followed by half of the EU Member States.

#### ***4.2. Looking for a security and data protection balance***

One of the novelties brought about by the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community in the area of freedom, security and justice is the new Article 16 of the Treaty on the Functioning of the European Union that foresees that ‘The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.’<sup>48</sup>

Declaration 21 ‘On the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation’, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, foresees that ‘(...) specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police

<sup>47</sup> See COM(2012) 12 final.

<sup>48</sup> Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union European Community, OJ C 83, 30.3.2010, p. 55.

cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.<sup>49</sup>

On this basis, on 25 January 2012 the European Commission adopted:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: Draft General Data Protection Regulation);<sup>50</sup> and
- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (hereinafter: Draft Data Protection Directive).<sup>51</sup>

The obligatory character of the regulation and the directive will force EU Member States to follow established data protection standards.

The Draft Data Protection Directive has a double objective: to protect personal data and to ensure its exchange between competent authorities. It goes a few steps further than Council Framework Decision 2008/977/JHA as:

- its scope is not only limited to the regulation of cross-border data exchange, but also the harmonization of data exchange on the national level;
- it obliges a distinction to be made between different categories of data subjects (suspects, those convicted of a criminal offence, victims, third parties in criminal offences (witnesses, etc.), persons who do not fall within any of these categories);
- it covers the exchange of genetic data;
- it establishes as a general rule that data could be transferred to a third country or an organisation if the Commission has decided that that country or organisation ensures an adequate level of data protection;
- it foresees that bilateral and multilateral agreements concluded by Member States have to be amended according to the provisions of this Directive.

Besides all the mentioned improvements, the Draft Data Protection Directive does not cover all areas of freedom, security and justice as it states that the data protection rules of previously adopted acts of the EU for judicial and police cooperation in judicial matters (including Council Decision 2008/615/JHA) remain, for the time being, unaffected and within three years after the entry into force of this Directive, the Commission will evaluate the need to align their provisions with those of the Directive.

This and other aspects of the Commission's Draft have resulted in criticism from the European Data Protection Service. According to the European Data Protection Supervisor's opinion on the data protection reform package, the Draft Data Protection Directive:

- is weaker than the Draft Data Protection Regulation;
- leaves unaffected, without justification, specific acts in the area of police and judicial cooperation in criminal matters, such as the rules for Europol, Eurojust, and data exchange under Council Decision 2008/615/JHA;
- being a self-standing instrument, misses an opportunity to clarify and ensure the consistent application of rules which are applicable to situations in which information exchange has to take place between competent authorities and other public bodies or the private sector.<sup>52</sup>

---

49 Ibid. p. 345.

50 COM(2012) 11 final.

51 COM(2012) 10 final.

52 See European Data Protection Supervisor, Report 2012/C 192/05, OJ C 192, 30.6.2012, pp. 13-15.

The same concerns were expressed by the European Parliament that believes that with proper modifications<sup>53</sup> this package can provide more legal certainty in the area of data protection<sup>54</sup> and emphasises ‘stronger incentives for data protection by design and by default’.<sup>55</sup>

Data protection is certainly vital in all areas of life and most of the comments by the European Data Protection Supervisor and the European Parliament are reasonable, especially those on unified data protection rules in all areas of justice and home affairs. Nevertheless, it would be more effective to look for efficient responsibility mechanisms for law enforcement institutions and the EU Member States in applying data protection rules rather than establishing too many new data protection restrictions.

## 5. Conclusions

Identification opportunities that lie within DNA have made it a reliable tool for the investigation and prosecution of crimes and in some cases have become pivotal forensic evidence. The increased mobility of crime has made it necessary to create new legal bases and technological possibilities for the transnational exchange of DNA-related data and has resulted in mechanisms such as the automated search for and comparison of DNA profiles in the national databases of other countries. Although cooperation under Council Decision 2008/615/JHA has only been in effect for a few years, the number of searches that have resulted in a ‘hit’ (20,561 hits in 2011 and 52,507 hits in 2012) proves the high rate of crime mobility and the necessity for such cooperation.

The analysis of the legislation applied to DNA collection and use for criminal investigation and prosecution purposes has revealed a few findings:

1. EU legislation obliges Member States to create DNA analysis files (databases), foresees some rules on the forensic analysis of samples and establishes rules on direct access to and automatic searches in national DNA databases. Nevertheless, the rules on DNA sample collection and ‘post-hit’ data provision are subject to national regulation and vary a great deal, beginning with the taking of samples without a person’s consent and the subsequent judicial authorisation and finishing with the provision of DNA-related data only within the framework of judicial cooperation. An attempt to establish common rules for sample collection was made in Council Framework Decision 2009/905/JHA, but it covers only the technical part of the collection process, leaving it to the national rules of criminal procedure to determine the subject and circumstances of DNA sample collection.
2. While in the collection, analysis, use and storage of cellular materials and DNA profiles limitations to or even violations of some fundamental rights appear, international law establishes that some fundamental rights (such as the right to privacy) are not absolute and can be proportionally limited for the sake of public security. Such limitations are usually established by national law and differ in the same way as the above-mentioned regulations on DNA sample collection. Nevertheless, international jurisprudence emphasises that limitations on fundamental rights have to be proportional and restricted to those which are necessary.  
In other cases international jurisprudence has come to the conclusion that relevant fundamental rights (such as the right not to incriminate oneself) are not violated by the collection of DNA samples.
3. A process of converging legal provisions leading to greater homogeneity between the data protection regulations in the EU Member States is taking place within the EU. EU legislation foresees minimum standards to be followed and facilitates the building of mutual trust among EU Member States that results in permission for direct access to national databases that was unthinkable a few decades ago.

---

53 At the end of the investigation the European Parliament did not yet adopt the Reports on this package. The Draft Report on the Draft General Data Protection Regulation contained 350 amendments and the Draft Report on the Draft Data Protection Directive contained 169 amendments.

54 See the Draft Report of the European Parliament, PE501.928v02-00.

55 Working Document of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, PE497.802v01-00.

From another point of view, establishing only minimum standards puts EU Member States with stricter rules in a difficult position, as evidence gathered in other countries with a less harsh procedure in force is not recognized as sufficient and reliable evidence.

One solution would be to opt for the application of the procedural legislation in force in the State requesting the procedure (if it is stricter), in order to ensure its validity once it is sent to the interested party. This would lead to the logical conclusion that all processing and storage of DNA profiles intended to be included in an international database would have to be carried out in such a way as to respect the guarantees common to all the countries with access to this source of information, which, although differently expressed, would actually be another way of homogenizing the procedural guarantees concerning the collection and storage of genetic data. ¶