ASSESSMENT OF THE DATA PROTECTION SYSTEM IN THE EXCHANGE OF DNA PROFILES

María José Cabezudo Bajo
Lecturer in Procedural Law. Universidad Nacional de Educación a Distancia (UNED)
mcabezudo@der.uned.es

Police DNA databases can only be truly effective, from a legal standpoint, in the fight against serious national and cross-border crime, in particular organised crime and terrorism, if the regulation thereof meets three requirements: first, the DNA evidence must be lawfully obtained; second, the DNA evidence must be obtained as reliably as possible and, lastly, the DNA evidence must be admissible in the relevant court of law. However, given that what I refer to as "the technology of DNA databases" includes three phases, namely, the first phase of collection of the DNA sample; the second phase of analysis of the DNA profile in the laboratory and, finally, the third phase of processing of DNA data in a database, such DNA evidence will only be admissible in criminal proceedings, if it was obtained lawfully, as reliably as possible and in compliance with the necessary requirements of admissibility in each and every one of the three phases.

In accordance with said methodological approach, this paper will focus on compliance with the required lawfulness of evidence, namely that evidence is obtained with the highest respect for fundamental rights which may be affected in each phase, although confined to the above-mentioned third phase concerning the processing of data in the DNA database. To this end, we will analyse the laws governing the activities involved in said processing and, where applicable, the legislation on data protection, mainly from the standpoint of the fundamental right to the protection of personal data, to determine whether said activities respect said right.

The first step to achieving this objective is the identification and initial analysis of data protection laws on the three primary levels that they apply, specifically, the international level, but limited to international agreements between EU Member States and third countries, the European Union level and the national level. This identification and initial analysis is not without difficulties given the barrage of legislation adopted in this field and the different scopes of application, indicating a clear lack of harmonisation of the level of data protection in each of the three said levels, as well as between them. The foregoing notwithstanding, I will begin this paper with an explanation of the motivation behind this work and close with my preliminary conclusions.

I. MOTIVATION BEHIND THE WORK

The legislation and standards governing DNA databases, internationally, and on the European and national levels, aims to improve the fight against major national and cross-border criminal activity, in particular organised crime and terrorism,. To this end, the relevant institutions across the three indicated levels are adopting rules aimed at ensuring that police DNA databases provide an effective tool in the fight against serious crimes. One of the measures to this end is the automated consultation and comparison of the two types of DNA profiles in the databases: the identified profiles, which are those taken from the body of the accused, and the unidentified profiles, that is, those left at the scene of a crime. The automated search is intended to achieve a match between DNA profiles, in particular, between an unidentified profile and an identified profile or between unidentified profiles from different crime scenes, linking the new crime with one already in the database to one or more suspects. By virtue of such a match, in the first case, the owner of the unidentified profile can be identified, thereby identifying the suspect who left DNA evidence at the crime scene, and in the second case, the DNA evidence will allow investigators to link one or more crime scenes with a single unidentified suspect. Ultimately, DNA matching contributes to the solving of crimes and often represents key expert evidence, which, together with other evidence, can help prosecutors achieve a conviction. Conversely, the lack of DNA match may be used as exculpatory evidence. These are the goals sought by the legislation on the national,

European and international levels. But such laudable goals are far from what was actually achieved by such legislation.

Accordingly, we are analysing the various laws comprising the legislative framework to answer the question that is the ultimate goal of our work: whether the police DNA databases are a truly effective tool in combating major national and cross-border crime. As a result of this analysis, we have identified several legal issues that will impede the collection of a expert DNA evidence. This, ultimately, prevents us from asserting that the police DNA databases are a truly effective tool in the fight against national and cross-border crime. To jointly analyse the legal problems that we have identified and design legally well-constructed solutions based on a common framework, we have formulated the following methodological approach.

So far, we believe that DNA databases can only be truly effective in the fight against major national and cross-border crime, in particular organised crime and terrorism, and therefore constitute admissible expert evidence, if the collection of the evidence meets three requirements: first, the DNA evidence must be lawfully obtained; second, the DNA evidence must be obtained as reliably as possible and, lastly, the DNA evidence must be admissible in the relevant court of law. However, given that what I refer to as "the technology of DNA databases" includes three phases, namely, the first phase of collection of the DNA sample; the second phase of analysis of the DNA profile in the laboratory and, finally, the third phase of processing the DNA data in a database, which falls within the scope of this paper, consequently such DNA evidence will only be admissible in criminal proceedings, if it was obtained lawfully, as reliably as possible and in compliance with the necessary requirements of admissibility in each and every one of the said three phases.

In my opinion, within the EU, which is the main focus of our work, the institutions of the European Union have adopted different rules that seek compliance with the requirements of lawfulness, greatest reliability possible and admissibility in each of the said three phases: 1) Regarding the lawfulness of evidence and the processing phase of DNA data in the database, which may impact the fundamental right to data protection, the EU has approved 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, together with the specific rules applicable to the DNA data provided by Decision 615/2008 (articles 24-32). In the previous phase, referred to the collection of the DNA sample, which may affect the fundamental rights to physical integrity, privacy, and inviolability of the home or the right to data protection, the EU has adopted rules on the collection of samples, either from the crime scene[1], or an identified person[2], being processed and an initiative is underway for the adoption of a Directive on the European Investigation Order[3]. 2) With

[1] Framework Decision 2003/577/JHA of 22 July 2003, developed in Spain by Law 18/2006 of 5 June, on the execution in the European Union of orders freezing property or evidence and Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters And this, with prejudice to that, for all matters not established therein, the Convention on Mutual Assistance in Criminal Matters of 29 May 2000, among others, shall apply. See footnote 6.

[2] Article 7 of Framework Decision 2008/615/JHA.

[3] Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a

respect to the reliability of the evidence in the extraction phase of the profile, the EU has adopted two rules: the first[4] requires that laboratory activities be conducted by forensic service providers which are accredited by a national accreditation body to certify that such activities comply with EN ISO/IEC 17025, the second[5] invites Member States, on the one hand, to use the 12 markers or *"DNA loci"* that make up the current European Standard Set of *"loci"* (ESS), and, secondly, to build up ESS analysis results in accordance with scientifically tested and approved DNA technology based on studies carried out by the ENFSI DNA working group. 3) In relation to admissibility, and in the process of obtaining a DNA sample, there is the initiative for a Directive regarding the European Investigation Order in criminal matters[6]. With these laws the legislators seek to prevent evidence from being inadmissible or having limited probative value as part of a criminal process taking place in a Member State due to the way in which the evidence was obtained in another. To this end, article 8.2 of said Directive provides that the executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Directive and provided that such formalities and procedures are not contrary to the fundamental principles of law of the executing State.

Thus, we are examining all the legal issues identified from the standpoint of the above methodological approach. This means that if the three common objectives relating to the lawfulness, greatest reliability possible and admissibility in each of the three phases are to be achieved, we must conduct a cross-sectional study of these three elements, across the entire three stages regarding the collection, analysis and processing of DNA data.

In this paper will focus on compliance with the required lawfulness of evidence, namely that evidence is obtained with the highest respect for fundamental rights which may be affected in each phase, although confined to the above-mentioned third phase concerning the processing of data in the DNA database given that said data is

---

Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters - JHA (2010) 3, published in the OJEU 24 June 2010, C 165.

[4] Framework Decision 2009/905/JHA of 30 November on the accreditation of forensic service providers carrying out laboratory activities.

[5] Council Resolution of 30 November 2009 on the exchange of DNA analysis results. The expansion of the number of DNA markers to 12 is due to the statistical value of DNA data corresponds to the probability of random coincidence and is completely dependent on the number of DNA markers which are reliably analysed.

[6] Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters - JAI (2010) 3, published in the OJEU 24 June 2010, C 165. This initiative aims to achieve a single new regulation, because, at present there are numerous mutual assistance laws in force, such as, among others, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 and rules on mutual recognition, such as the Framework Decision 2003/577/JHA of 22 July 2003, which applies to the preservation of evidence obtained in another Member State, but not its transmission, as well as Council Framework Decision 2008/978/JHA of 18 December 2008, which is limited to existing evidence or evidence that is available in the form of objects, documents or data, therefore, not applicable to obtaining a DNA samples because, according to the said decision, the European evidence warrant is not applicable to evidence that does not exist or is not directly available without further investigation or review, such as DNA samples. Conversely, both cases fall under the scope of the Directive currently being processed. In this sense, one can see the "Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility", COM (2009) 624 final of 11 November 2009.

considered personal. To this end, we will analyse the laws governing the activities involved in said processing and, where applicable, the legislation on data protection, mainly from the standpoint of the fundamental right to the protection of personal data, to determine whether said activities respect said right. Specifically, the processing of data in the DNA database includes various activities such as entry, organisation, consultation, comparison, blocking, erasure or destruction of the profile in the database. Given that said activities, ultimately, seek to achieve a "national" or "cross-border" match between an unidentified profile and an identified profile, allowing the resulting information to be incorporated, through expert evidence, in an oral trail in Spain, it only be used as evidence if it has been obtained as lawfully and reliable as possible and is therefore admissible evidence.

The first step to achieving this objective is the identification and initial analysis of data protection laws on the three primary levels that they apply, specifically, the international level, but limited to international agreements between EU Member States and third countries, the European Union level and the national level. This identification and initial analysis is not without difficulties given the barrage of legislation adopted in this field and the different scopes of application, indicating a clear lack of harmonisation of the level of data protection in each of the three said levels, as well as between them. The foregoing notwithstanding, I will begin this paper with an explanation of the motivation behind this work and close with my preliminary conclusions.

II. TRIPLE-LEVEL SYSTEM OF DNA DATA PROTECTION

As noted, the first step in the analysis of the legislation on the processing of DNA data in the database, from the standpoint of the fundamental right to data protection, is the identification and execution of an initial analysis of said laws. In order to carry out both tasks systematically, we will distinguish between the three levels of DNA data protection, the international level, limited for these purposes to agreements between the EU or its Member States with third countries, the European Union level and the national level. Given that DNA data to be exchanged between Member States and third countries are also performed in relation to the three levels.

1. International level: EU or Member States and third countries

In order to combat major international crime, there is a growing need to exchange information between states. Accordingly, in recent years, new laws have been enacted to allow the exchange and, in particular, consultation and automated comparison of DNA profiles through their databases. Specifically, on the international level, we will refer to the exchange of DNA information between the EU and its Member States and third States, which is governed under the specific laws adopted at EU level[7] and international treaties[8]. Which data protection laws are applicable to such

[7] Articles 13 and 26 of the Framework Decision 2008/977 of 27 November 2008 on the on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[8] For example, the Convention between the Kingdom of Spain and the United States on exchange of cooperation in preventing and combating serious crime. (Official State Gazette 225 of 17 September 2009. The U.S. has also signed similar agreements with Germany and Portugal. In fact, given the many agreements signed between EU Member States and the USA, an agreement is in the works

international exchange of DNA profiles? Below we identify and carry out a preliminary analysis of these laws.

Currently, there is no international system on the protection of personal data applicable to the international exchange of DNA profiles. Despite the extraordinary difficulty in the adoption of such a system, it is necessary and the authorities are working towards just such a system. But while no such international system, the exchange of DNA profiles with the EU or between its Member States and third countries are governed by the data protection laws, on the one hand, adopted at the EU level and, secondly, that contained in the individual international agreements.

Regarding the exchange of DNA profiles on the EU level, between the EU or its Member States and third countries, the question of the protection regime applicable to such data is not expressly regulated[9] in Decision 2008/615, which is subsidiarily applicable to the Framework Decision 2008/977. Specifically, the Framework Decision regulates the transfer of DNA data by a Member State transmitted or made available by another Member State to a third state or international body. This provides for two different scenarios in which the requirements to be met differ: 1) when dealing with third countries with which the EU or a Member State has signed an agreement in effect at the time the adoption of the aforementioned Framework Decision (Article 26), and 2) Conversely, when dealing with third countries with which the EU or a Member State has not signed an agreement in effect at the time or or after adoption of the said Framework Decision. In the first case, transfer to a third country of personal data obtained from another Member State shall be conducted in accordance with the provisions of said Agreement, given that the Framework Decision does not affect contractual obligations and commitments, although in applying these agreements the transfer must be made in accordance with the provisions of Article 13, section 1, letter c) or Article 13, section 2, as appropriate (article 26.II). In the second case, the provisions of article 13 (recital 38) would apply.

Specifically, article 13.1 establishes that Member States shall provide that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies, only if a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, b) the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the third state or international organization is responsible for receiving purposes described above, c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law[10]; and d) the third State or international body

---

between the EU and the USA on data protection in the framework of police and judicial cooperation in criminal matters.

[9] Only the article 35 includes provisions on the relationship of this decision to other cross-border cooperation instruments. Specifically, the Decision distinguishes between two cases: 1) whether Member States have signed agreements prior to this decision, in which case they may continue to apply, and 2) if the Member States intend to sign agreements after the adoption of the decision, in which case they may do so if such agreements comply the objectives of the decision.

[10] Even article 13.2 allows the transfer of data without consent only if transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time and the authority responsible for giving consent is informed without delay.

concerned ensures an adequate level of protection for the intended data processing, while also providing an exception to d) in Article 13.3[11], although these cases seem to be regulated in general, the decision should have insisted on their exceptional nature and, therefore, on a more restrictive interpretation[12]. Similarly, article 13.1 d) is particularly criticisable as it does not guarantee that the data transferred effectively enjoy an adequate level. Also, although article 13.4 does set out some criteria to consider, it does not provide any mechanism to assess the adequacy, or indicate the authority responsible for such a task. Therefore, if it is easier to transfer personal data to third countries than to other Member States, it would enable the "laundering of information"[13], to the extent that the competent authorities of the Member States could circumvent the strict rules of data protection y transferring the data to third countries or international bodies from which the competent authority of another Member State could obtain the information. In such a case, Article 13.4[14] could eventually allow each Member State to assess, at its discretion, the level of adequacy and the protection envisaged by the third State or international body, which is detrimental to the intended harmonisation.

Accordingly, from the standpoint of the protection of DNA data, there are two cases: 1) if in the case of an agreement in place before the adoption of Framework Decision 2008/977, the provisions of the agreement apply, except as provided in Art. 26.II of said Framework Decision, and 2) if an agreement is reached after the adoption of the Framework Decision, in which case, the provisions of article 13 apply, with the provisions of article 13.4 being especially criticisable. Therefore, in the first case, there as many provisions on data protection and, consequently, levels of data protection as there are agreements and, in the second, there are as many interpretations on the level of data protection as there are transfers. In both cases we would have to make the same criticism: the absolute lack of harmonisation in the level of data protection applied to international transfers between Member States and third countries.

This type of criticism has been highlighted in a Commission Communication[15] stating that the inclusion of specific provisions or principles regarding data protection in international agreements signed between Member States and third countries poses a problem that can lead to different texts that lend themselves to different interpretations. Similarly, Commission states that it cannot evaluate the adequacy of the level of data protection given that the Framework Decision 2008/977 does not allow for it unlike Directive 95/46/EC. However, the said Directive lacks sufficient clarity on what

[11] Art. 13.3 allows the transfer of data if 1) the national law of the Member State transferring the data so provides because of legitimate specific interests of the data subject or legitimate prevailing interests, especially important public interests due to legitimate interests or if 2) the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law.

[12] This was initially regulated under Article 15 of the initial Proposal. This has been pointed out in the third report by the EDPS , under item 27.

[13] As highlighted in the first report by the EDPS , under item 101.

[14] Art. 13.4 provides that "The adequacy of the level of protection referred to in paragraph 1(d) shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international body in question and the professional rules and security measures which apply."

[15] Communication from the Commission ... COM (2010) 609 final, pp. 16-18.

specific conditions the national legislation must meet for the Commission to conduct the evaluation. On the other hand, the Commission notes that in some Member States adequacy is evaluated by the controller, although sometimes after the fact, which ultimately means that the protection risk provided by a third country can be deemed differently from one Member State to another.

Accordingly, the solution to these problems would be to achieve a global legal framework on data protection as proposed by the European Commission in its Communication. In fact, given that the EU legal framework on data protection has often served as a benchmark for third countries when regulating data protection, the Commission has taken a first step with the proposed global approach to personal data in the EU, in its Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. In this regard, The Commission has indicated[16] that it intends to further promote the development of international legal and technical standards for the protection of personal data. Recognizing that this work to promote a comprehensive legal framework on data protection must be without prejudice to need to adopt specific regulations in the fields of police and judicial cooperation in criminal matters given the peculiar nature of these fields[17], in which the exercise by individuals of certain rights regarding data protection in a particular case may compromise the investigation. Specifically, among other courses of action, the Commission proposes to to define core EU data protection elements, which could be used for all types of international agreements concluded by the EU or its Member States and also intends to enhance its cooperation, to this end, with third countries and international organisations, such as the OECD, the Council of Europe, the United Nations, and other regional organisations; strive for the principle of reciprocity of protection in the international actions of the Union and in particular regarding the data subjects whose data are exported from the EU to third countries, but also considers it necessary to strengthen the institutional arrangement for better enforcement of data protection rules and, in this context, believes that the Commission itself should strengthen its role, Data Protection Authorities should strengthen their cooperation and better coordinate their activities, and highlights the important role that can be played by the Article 29 Working Party. Reactions to this Communication have been diverse: on one side, very favourable to the Commission's position and the contribution of Article 29 Working Party and the Working Party on Police and Justice[18], which consider international agreements as an appropriate instruments for the protection of personal data in a global context and recognise that the future legal framework could include conditions that must be included in agreements with third countries, in particular, Binding Corporate Rules, while others were more cautious, such as the positions maintained by the U.S. and the UK[19].

On the other hand, the European Data Protection Supervisor, which meets annually to promote and discuss the need for high level of data protection worldwide in all areas, have recognised[20] this first step by the Commission, stressing the need for said

[16] Communication from the Commission ... COM (2010) 609 final, pp. 18 & 19.

[17] This is expressly stated in the Declaration 21 annexed to the Treaty of Lisbon.

[18] This was adopted on 1 December 2009 under the title "the future of privacy."

[19] The contributions from the USA and UK, among others, are accessible on: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm

[20] "Resolution on the need for a comprehensive data protection framework" adopted by the European Data Protection Commissioners' Conference held on 5 April 2011 in Brussels. The European Data Protection Authorities previously adopted a Declaration on leadership and the future of data

coherent and global approach and focusing, among other things, in the development[21] of international standards that are recognised worldwide.

In short, the need to harmonise in the level of data protection applied to international transfers between Member States and third countries could be achieved by identifying minimum standards of data protection and making them binding.

2. EU Level

In order to combat serious cross-border crime, the exchange of DNA profiles among Member States at the EU level, among other matters, is regulated in the Treaty of Prüm, which joined the EU acquits by virtue of Decision 2008/615/JHA and known as the Prüm Decision[22], and further developed by Decision 2008/616/JHA. Thus, under the Treaty of Prüm and Decision 2008/615/JHA, Member States shall open and keep national DNA analysis files for the investigation of criminal offences (article 2.1)[23], have the power to conduct automated searches and comparisons of DNA profiles in DNA databases of other Member States in order to verify possible matches (Articles 3 and 4)[24]. In the case of a match, the national contact point of the Member State conducting the search will receive automated reference data with which a match has been found. Also, in the case of a match between profiles, the supply of further available personal data and other information relating to the reference data shall be governed by the national law (article 5). But the European legislator has subordinated such exchanges to the elevation and harmonisation of DNA data protection. To this end, the EU has adopted legislation on data protection applicable to DNA data which

---

protection in Europe adopted by the European Privacy and Data Protection Commissioners' Conference on 23-24 April 2009 in Edinburgh, which was confirmed at the Spring Conference organised in Prague in the Resolution on future development of data protection and privacy adopted by the European Privacy and Data Protection Commissioners' Conference on 30 April 2010. They also highlighted their interest in the work of the Council of Europe and the OECD on the adoption of initiatives to review existing frameworks and identify areas for modernisation, and the Council of Europe's Initiative to encourage those who are not party to Convention 108 and its Additional Protocol, both member nations and others, to accede to the Convention.

[21] "International standards on the protection of personal data and privacy" adopted on 5 November 2009 in Madrid at the 31st International Conference of Data Protection and Privacy Commissioners, as well as the "Resolution calling for the organization of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data", adopted on October 29, 2010 in Jerusalem at the 32nd International Conference of Data Protection and Privacy Commissioners.

[22] Art. 35.1 states "For the Member States concerned, the relevant provisions of this Decision shall be applied instead of the corresponding provisions contained in the Prüm Treaty. Any other provision of the Prüm Treaty shall remain applicable between the contracting parties of the Prüm Treaty." Furthermore, article 36 of the Prüm Decision provides that Member States shall take the necessary measures to comply with the provisions of this Decision within one year of this Decision taking effect, with the exception of the provisions of Chapter 2 with respect to which the necessary measures shall be taken within three years of this Decision and the Council Decision on the implementation of this Decision taking effect, which was on the twentieth day following its publication in the OJEU on 6/8/2008.

[23] As established in both the Treaty and the Decision, the national files shall include reference data that will contain DNA profiles obtained by the non-coding part of DNA and a reference number. Reference data shall not contain any data from which the data subject can be directly identified.

[24] According to the ENFSI document on DNA-database management 2010, at the time of this paper, Austria, Germany, Spain, Luxembourg, France, the Netherlands (some of the Parties to the Treaty of Prüm), Finland Bulgaria and Romania were exchanging DNA profiles. Available at http://www.enfsi.eu/page.php?uid=98

coexists with other previously approved laws. These laws and our initial analysis follow.

In fact, in order to elevate and harmonise the level of data protection, the European legislator has adopted rules on data protection applicable to DNA data. These provisions are contained in Decision 2008/615, which establishes specific rules for DNA data (arts. 24-32) as well as rules applicable to personal data contained in Framework Decision 2008/977, which apply subsidiarily (Article 28 of the Framework Decision 2008/977). However, the Framework Decision 2008/977 does not replace the rest of the data protection rules, but coexists with other sectoral legislative instruments adopted within the framework of police and judicial cooperation in criminal matters, such as those regulating the functioning of Europol, Eurojust, the Schengen Information System (SIS) and Customs Information System (CIS), which either refer to data protection instruments of the Council of Europe or establish a specific protection system. Also, in the field of police and judicial cooperation, all Member States have endorsed the recommendation of the Council of Europe No. R (87) 15, which establishes the principles of Convention 108 for the police sector, although it is not a legally binding instrument.

Again, we would highlight that the lack of harmonisation on the level of data protection can be overcome if the initiative put forward by the Commission for a comprehensive approach to the protection of personal data is successful. This new global approach meets the challenges of globalisation and new technologies and has its legal basis in the Treaty of Lisbon. Indeed, the Treaty of Lisbon, by removing the pillar structure of the EU has established a new legal basis for broader protection of personal data in all EU policies, in view of the provisions of article 16 of the Treaty on the Functioning of the European Union. In this context and based on article 8 of the Charter of Fundamental Rights of the EU, the Commission[25] has highlighted the need for a "general protection system" and "strengthen the European Union's position regarding personal data protection in the field of all EU policies, including the police repression and crime prevention. " Therefore, the Commission added[26] it will consider whether to extend the application of general rules of data protection in the areas of police and judicial cooperation in criminal matters. And this is without prejudice, as previously indicated, to the fact that the field of police and judicial cooperation in criminal matters must have Specific rules given the specific nature of these fields as indicated in Declaration 21 annexed to the Treaty of Lisbon.

Having identified the laws governing data protection, we performed an initial analysis from the standpoint of the fundamental right to personal data protection. This analysis is of particular interest given that the Treaty of Lisbon not only introduces Articles 16 and 39 TFEU regulating the right to data protection, but also provides Article 8 of the Charter of Fundamental Rights of the European Union (Article 6 TEU), which recognises personal data protection as a fundamental right and is binding. But first I would like to highlight a problem that also indicates the need to harmonise the

[25] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: "A comprehensive approach on personal data protection in the European Union", COM (2010) 609 final, of 4.11.2010, which refers to the Commission Communications on the Stockholm Programme - COM (2009) 262, 10 June 2009 and the Stockholm Action Plan - COM (2010) 171, 20 April 2010.

[26] Communication from the Commission... COM (2010) 609 final, p. 16.

level of data protection across the EU and its Member States. The question is whether the current system of DNA data protection in the European Union, which applies only to "exchanged DNA data" is adequate to ensure effective protection of data transmitted between the Member States.

Indeed, the European system of protection applies only to the data being sent or having been sent pursuant to Council Decision 2008/615/JHA (Art. 24.2)[27]. This limited scope means that there will be a two-tier data protection system: one applicable to cross-border data and another for national data.

On one side, the cross-border protection regime applicable to exchanged DNA data, i.e., data transmitted or made available by another Member State. This system will be the one that implements the data protection provisions of Chapter 6 of Decision 2008/615 into the national law of the Member States involved in such supply under said Decision, may not take place until the provisions of this Chapter have been implemented (article 25.2 Decision 2008/615). The Council will decide whether the States have complied with this requirement, which does not apply to Member States exchanging DNA data under the Prüm Treaty (article 25.3). Alternatively, the national DNA data protection system, which is the one regulated in the Member State and applicable to data obtained from each State which been involved in an exchange.

However, this dual system can involve dire consequences for the effectiveness of the measure[28]. In fact, some of these negative effects were presented by the European Parliament[29] and the European Data Protection Supervisor[30] during the processing of Framework Decision 2008/977. Such objections may also be extended to data protection rules laid down in Decision 2008/615/JHA. In particular, we highlight the following arguments:

Firstly, the difficult determination, at any particular time, of the applicable regime to national or community data, when it is collected or processed and it is not known whether or not it will be a subject further exchange between Member States. Similarly, the increasingly frequent occurrence of different levels of protection of data contained in criminal records of many Member States, some from other Member States authorities and others obtained at home. Thirdly, it is difficult to consolidate an environment of mutual trust because, in the absence of common standards for national and cross-border data, it will make it difficult to accept the data exchanged between

[27] And this in contract to the provisions of various instruments of the Council of Europe, which do not provide such a distinction, such as Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Additional Protocol on control authorities and the transfer of data (No. 181) and Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, adopted by the Council of Europe on 17 September 1987, which, although it was endorsed by all Member States, is not a binding legal instrument.

[28] These points are widely discussed in CABEZUDO BAJO, M. J., "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal", in the Charter of Fundamental Rights of the European Union, Madrid, ed. Colex, 2008, p. 335-336.

[29] This can be read in the Explanatory Memorandum to the Report on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [COM (2005) 0475 - C6-0436/2005- 2005/0202 (CNS)] of the Committee on Civil Liberties, Justice and Home Affairs of 18.05.2006. The reference is PE 370.250v02-00.

[30] In this context, please see the Second opinion (2007/C91/02), paragraphs 10 to 17, as well as the Third Opinion (2007/C139/01), paragraphs 16 to 19, issued by the EDPS on this Framework Decision.

Member States. Lastly, the weakening of the position of the EU in its negotiations with third countries as USA, due to the inability submit the communication of personal data to an appropriate level of internal protection[31].

To avoid the aforementioned negative effects, there are two complementary solutions: first, that Member States develop a national protection regime in a way similar to the protection regime applicable to the exchanged data.

Alternatively, as indicated in a previous paper[32], that European institutions extend the cross-border regime already approved in EU rules to their national data. Perhaps this could occur if we take advantage of the possibilities offered by the Treaty of Lisbon. In this sense, we now know, thanks to the new legal framework established by the Treaty of Lisbon on the protection of personal data (article 16 TFEU), that the Commission[33] has undertaken to examine the possibility of extending the application of general rules of data protection in the areas of police and judicial cooperation in criminal matters, even for national processing.

With these considerations in mind, we will now undertake an initial analysis of the protection system for exchanged data. We will focus on the relevant provisions of Decision 2008/615[34] and, in general, Framework Decision 977/2008, in that Convention 108 is considered to have been replaced by Decision 2008/977[35], without prejudice to the fact that the Convention applies to the national data protection system and because the Recommendation No. (87) 15 is non-binding. Both the regulation contained in Council Decision 2008/615, and Framework Decision 2008/977 address to the protection of fundamental rights which may be affected under the "processing of personal data"[36]. This safeguard is achieved mainly through the inclusion of a number of provisions in the Prüm Decision, among others, on the purpose of the data (article 26), the quality of the data (article 28) technical and organisational measures (article 29) and logging and recording (Article 30), which are complemented by provisions in Framework Decision 2008/977, among others, on the principles of lawfulness, proportionality and purpose (article 3), the quality of the data (article 4), confidentiality

[31] The EDPS, in its first opinion (OJ C 47/39, 25.2.2006), paragraph 101, states that paradoxically personal data could be transferred to third countries — disregarding any adequate protection of personal data — more 'easily' than to other Member States anfd that this would give rise to possibilities of 'information laundering'

[32] CABEZUDO BAJO, "DNA databases: methodological approach, family searches and DNA data protection system in the EU" in Kengyel and Nemessany, *Electronic Justice. How new technology can make the procedure more effective*, Springer, 2011.

[33] Communication from the Commission ... COM (2010) 609 final, pp. 15 & 16.

[34] Many of the deficiencies that the Prüm Treaty contains in relation to the fundamental right to data protection have been highlighted by FREIXAS SANJUAN, T., "Protección de datos y globalización". La Convención de Prüm", RDCE, no. 7, January-June, pp. 14-19; ACED, E., "Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm", RDCE, no. 7, January-June, 2007, pp. 82-92; CAMARA, G., "La garantía de los derecho fundamentales afectados por la Convención de Prüm", RDCE, no. 7, January-June, 2007, particularly, pp. 107-117.

[35] This Framework Decision has been analysed by ALCAIDE FERNÁNDEZ, J., in.,"La Unión Europea, la Sociedad de la Información y la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal: la Decisión marco 2008/977 JAI del Consejo, de 27 de noviembre de 2008, Revista General de Derecho Europeo, no. 19, October 2009, who stressed the fact that the Framework Decision provides general provisions applicable in the absence of anything more specific.

[36] Articles 24.1 a), 24.2 of Council Decision 2008/616 and articles 1, 2. a) and 2. b) of the Framework Decision 2008/977.

(art. 21), security of processing (article 22), Penalties (article 24), defining the right of access (article 17), the right to rectification, erasure or blocking (article 18), the right to compensation (article 19) and the right to judicial remedies (article 20) . In particular, we will offer two considerations regarding data quality and data processing, as well as on the limitation of the purposes of such processing, since these issues were very controversial during the processing of the Framework Decision 2008/977.

As for the quality of the data (articles 28 of the Decision 2008/615 and 8, in relation to article 4, of the Framework Decision 2008/977), it is true that the latter states that the competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available and take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. This provision is extremely accurate, since the police often use unverified data, based on mere presumptions. Nevertheless, it has abolished the distinction between different types of people that data can relate to (suspects, convicts, victims, witnesses, etc), that by contrast, was established in article 4.3 of the Commission's initial proposal. In this regard, the EDPS[37] emphasised the quality of data and, in particular, understood that this distinction was an essential safeguard that should not be deleted from the final text of the decision, mainly regarding the differential treatment which should be given to these people, especially when it comes to individuals who are not even suspects. In this sense, the Commission[38] has recently undertaken the commitment to examine the need for specific and harmonised provisions in the new framework for data protection, for example, in regard to the distinction of the different categories of data subjects as established principles 2 and 3 of Recommendation No. R (87)15.

Lastly, in relation to the processing of the data and the limited purposes to which the data may be put (article 26 Decision 2008/615 and article 3 of the Framework Decision 2008/977) rightly regulates the principles of lawfulness, proportionality and purpose of processing. The above principles provide that personal data may be collected by the competent authorities only for specific, explicit and lawful purposes within the scope of their activities, and "processed" only for the same purposes for which they were collected. Such processing must be lawful, adequate, relevant and not excessive. Following such a rule, both Decision 2008/615, and Framework Decision 2008/977 establish the same exception, while the Framework Decision 2008/977 adds two more. While these exceptions may be fortunate, since they refers to the fact that these goals are not incompatible with the purposes for which data were collected and their processing is necessary and proportionate to them for other purposes, the case provided in both community laws is criticisable. Said laws allow for the processing of data for other purposes solely with the prior authorisation of the Member State administering the file and subject only to the national law of the receiving Member State. According to these provisions (art. 26.1 Prüm Decision and 3.2 b Framework Decision 2008/977), the contents of this exception could be left to the discretion of national legislation, which is harmful to achieving the intended harmonisation of data protection laws.

Consequently, after the Treaty of Lisbon it is not only possible but also necessary to extend the scope of the laws on personal data protection to cooperation in criminal matters, subject to legal recognition of their own specialities. Also, these rules

[37] Please see their second report, item 18.
[38] Communication of 4.11.2010 COM (2010) 609 final, p. 15.

have to be more respectful of the fundamental rights concerned, especially the fundamental right to protection of personal data, at least in relation to data quality as well as in connection with the processing of data and limitation of purpose. Lastly, in order to achieve complete harmonisation of the level of personal data protection within the EU and among the Member States, it would be necessary to extend the protection system laid down at the EU level, not just on the data exchanged, but also to national data.

3. National level:

Nationally, the first country to legally establish a DNA database was the United Kingdom (1995), followed by the USA and other countries around the world[39]. In the EU, most of the 27 Member States have regulated police DNA databases and in other cases, such regulation is pending. Therefore, one might ask, if Member States have regulated the protection of personal data, would it be applicable to DNA data?. While this is a question we have to answer, the truth is that on the national level there is a problem of double system of data protection. This means that Member States will have to legislate a general system of protection for exchanged data, on the one hand, and another system for national data, on the other, for criminal matters and applicable to DNA data.

As for the general system of protection for exchanged data, applicable to the DNA data, as already indicated, the European legislator has subordinated such an exchange to the implementation in the national law of the Member States of the data protection provisions of Decision 2008/615, except in Member States that were part of the Prüm Treaty (article 25.2 and 25.3). In addition, Member States must develop the provisions of Framework Decision 2008/977, as it applies subsidiarily to the Prüm Decision. In any case, each Member State shall ensure that the law offers a level of data protection at least equivalent to that resulting from the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Additional Protocol of 8 November 2001, and follow Recommendation R (87) 15, of 17 September 1987 of the Committee of Ministers of the Council of Europe to the Member States regulating the use of personal data in the police sector, even when the data are not processed by computer (art. 25.3). With regard to the general national data protection system applicable to DNA data, it should still take into account the special characteristic of criminal law.

Specifically, in our country the police DNA database is regulated by Organic Law, 10/2007 of October 8, regulating the police database on identifiers obtained from DNA. Said Organic Law was developed by RD 1977/2008 of 28 November, which regulates the composition and functioning of the National Commission for the forensic use of DNA. This regulation has met the constitutional requirements (article 81 SC) stating that fundamental rights, in this case, the rights to the protection of personal data (article 18.4 SC) and privacy (article 18.1 SC) must be developed by Organic Law. And this in comparison with the criticism against the previous situation, in which DNA

[39] The three surveys conducted by INTERPOL, the last in 2008, aimed at determining the use of DNA profiling in criminal investigations among its 188 Member States were answered by 172, with the responses saying that 120 countries have used DNA profiling in police investigations and 54 have national DNA databases. Available at: http://www.interpol.int/Public/ICPO/Publications/HandbookPublic2009.pdf

databases of the National Police (VERITAS) and the Civil GUARD (ADNIC), were regulated by Ministerial Orders[40]. By virtue of said Organic Law, although not explicitly stated, the Scientific Police may make inquiries and comparisons between profiles "nationwide" and the databases may be shared by Spain in an exchange of DNA information with third countries in accordance with international conventions ratified by Spain and in effect (article 7.3.a), in order to achieve a cross-border match. Organic Law 10/2007 contains inadequate data protection standards specifically applicable to the DNA data and that referring to the security level required (article 8) and the cancellation, rectification and access to data (article 9) is insufficient. In fact, the Organic Law refers to all matters not covered thereby to the Organic Law on Personal Data Protection (Second Additional Provision). If we make a first analysis of said regulation, taking into account the need to provide a dual system of data protection, we could highlight some shortcomings.

In this regard, the cross-border regime would conflict with the Data Protection Act (LOPD), because it excludes from its protection of data "files established for the investigation of terrorism and other serious organised crime"(article 2.2 c)[41]. Therefore, Spain would have to establish a general system of protection for data exchanged within the EU, admissible in Spanish criminal proceedings, which would also apply to files established for the investigation of terrorism and other serious forms of organised crime[42]. Such regulation would have to respect the requirements of the principle of proportionality. As for the national system developed specifically in the OL 10/2007 (articles 8 and 9), although the law itself provides for the direct application of the Personal Data Protection Act, which, as indicated, does not apply to files for the investigation of terrorism and organised crime. Therefore, Spain would have to identify a national system of protection for data admissible in Spanish criminal proceedings, which would also apply to files established for the investigation of terrorism and other serious forms of organised crime. Similarly, given the impact on fundamental rights, this legal provision should be respectful of the requirements of the principle of proportionality.

Member States and, particularly, Spain will have to establish similar general system of protection for data exchanged on the one hand, and a national system, on the other, which is admissible in Spanish courts of law, and which would also apply to DNA data.

IV. CONCLUSIONS

Police DNA databases can only be truly effective, from a legal standpoint, in the fight against major national and cross-border crime, in particular organised crime and terrorism, if the regulation thereof meets three requirements: first, the DNA evidence must be lawfully obtained; second, the DNA evidence must be obtained as reliably as possible and, lastly, the DNA evidence must be admissible in the relevant court of law.

[40] Said Ministerial Orders are INT/3764/2004 of 11 November on computer files of the Ministry of Interior and INT/1751/2002 of 20 June on the computer files of the Directorate General of Police.

[41] Said exclusion from the scope of application of the Personal Data Protection Act established under Article 2.2 was already highlighted in Gomez Sanchez, Y., "Los datos genéticos en el Tratado de Prüm", RDCE no. 7, January-June 2007, p. 144.

[42] This has been highlighted by BAYO, J., "La cooperación internacional policial a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos" en *La protección de datos en la cooperación policial y judicial*, Pamplona, Thomson Aranzadi, 2008, p. 31.

However, given that what I refer to as "the technology of DNA databases" includes three phases, namely, the first phase of collection of the DNA sample; the second phase of analysis of the DNA profile in the laboratory and, finally, the third phase of processing of DNA data in a database, such DNA evidence will only be admissible in criminal proceedings, if it was obtained lawfully, as reliably as possible and is admissible in each and every one of the three phases

Internationally, it is necessary to harmonise the level of data protection applied to international transfers between Member States and third countries. This could be achieved by identifying minimum standards of data protection implemented in each of the international agreements and making them binding.

After the Treaty of Lisbon it is not only possible but also necessary to extend the scope of the laws on personal data protection within the EU to cooperation in criminal matters, subject to legal recognition of their own specialities. Also, these rules have to be more respectful of the fundamental rights concerned, especially the fundamental right to protection of personal data, at least in relation to data quality as well as in connection with the processing of data and limitation of purpose. Lastly, in order to achieve complete harmonisation of the level of personal data protection within the EU and among the Member States, it would be necessary to extend the protection system laid down at the EU level, not just on the data exchanged, but also to national data.

Member States and, particularly, Spain will have to establish similar general system of protection for data exchanged on the one hand, and a national system, on the other, which is admissible in Spanish courts of law, and which would also apply to DNA data.

Topics discussed in this paper have been raised in order to highlight some preliminary conclusions but continue being studied, mainly in relation to other new issues.

ACKNOWLEDGEMENTS

This work was performed under the research project funded by the Plan Nacional de I+D+I (2009-2012), DER 2009-08071, MICINN, Spain.