

Additional Safeguards for Children Using Biometric Technologies in the European Union Multilevel System from the Perspective of Fundamental Rights Protection

Joaquín Sarrión Esteve

Assistant Professor in Administrative Law

University of Valencia

joaquin.sarrion@uv.es

Program

I. Motivation.

II. Methodology

III. The advances of biometric technologies. A particular focus on DNA technology.

IV. DNA technology legal framework

V. Fundamental rights protection in EU Multilevel System

VI. Additional Safeguards for Children


Conclusions?



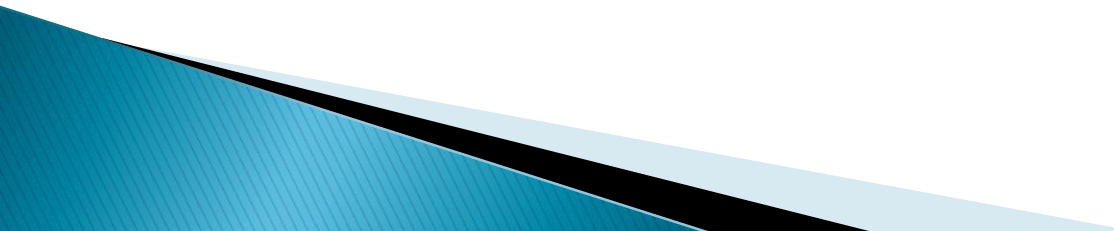
I. Motivation



I. Motivation

- Certainly biomedical research has experienced an exponential development in recent years, in part due to the profound transformations in biotechnology.
 - In fact, actually biometric data represent a challenge for security systems in the actual global world..
 - As we know, new technologies (particularly the so called biometric technologies) help us to identify individuals using for example:
 - ✓ **fingerprint/palm print identification**
 - ✓ **iris identification**
 - ✓ **face recognition** and
 - ✓ **DNA technology.**
- 

I. Motivation

- However, we need to respect fundamental rights when we are using these technologies. If this objective is important *per se*, it is much more so **in the case of minors that require special attention and specific (additional) guarantees.**
 - In this paper we present that the advances of these biometric technologies and their use have as a challenge their use our security systems with respect to fundamental rights, with a focus on DNA technology and particularly regarding the additional safeguards for children
- 

II. Methodology



II. Methodology

➤ We want to identify the requirements for the respect of fundamental rights in the use of biometric technologies in the context of the ***European multilevel system*** in which we live (the compliance with applicable fundamental and human rights standards).with a particular focus on **Children's additional Safeguards.**

➤ And to do it, we use two keys:

- 1) the ***multilevel constitutionalism perspective*** with attention to different legal systems with effect to right's legislation and interpretation (Gómez Sánchez, 2011); and
- 2) the need to use biometric technologies in order to guaranty their **legality** (maximum respect of fundamental rights and legal guarantees) and **effectiveness** (Cabezudo Bajo, 2011).

➤ 1) ***The Multilevel constitutionalism perspective approach***

▪ Today the different levels or legal systems are becoming progressively more interconnected, and therefore we need to explain the relation and identify the correct criteria to integrate them from the perspective of fundamental rights protection (Gómez Sánchez, 2011), particularly in the **EU complex system**.

✓ There are at least three levels to take into account:

- International level (International instruments on human rights, and particularly European Convention Human Rights standard)
- EU Level (EU Fundamental Rights Charter standard / and Fundamental Rights as General Principles of EU Law in the ECJ case law)
- National Level ([Constitutional] fundamental rights standards, and in some countries maybe regional rights)

2) *The legal and effective use of biometric technologies*

➤ We need to use biometric technologies in order to guaranty their **legality** (maximum respect of fundamental rights and legal guarantees) and **effectiveness** (using the appropriate scientific methods)

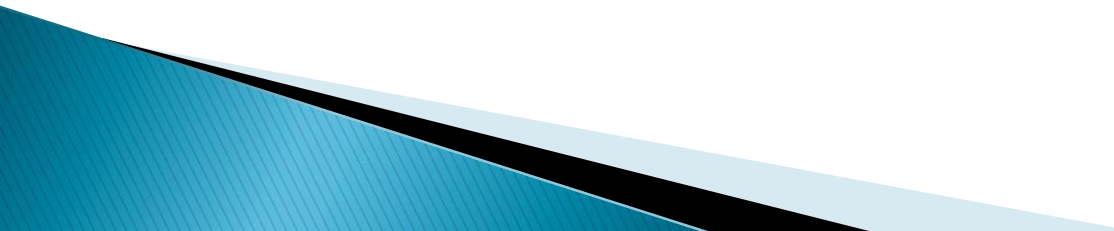
▪ As Cabezudo Bajo pointed out, in order to obtain a valid DNA evidence we need to guarantee the legality and effectiveness of the so called forensic use of DNA (Cabezudo Bajo, 2011, 2012). We can apply these requirements in the use of any biometric technology.

▪ The aim of using biometric technologies is to identify persons, particularly in the scope of Public Security policies, and we need to do it with the respect of legal guarantees, and in a effective way.

III. The advances of biometric technologies. A particular focus on DNA technology.



➤ New technologies, particularly the so called biometric technologies, help us to identify individuals using for example:

- ✓ **fingerprint/palm print identification**
 - ✓ **iris identification**
 - ✓ **face recognition**
 - ✓ **DNA technology.**
- 

➤ Fingerprint/palm print identification.

✓ Using a database of known and unknown fingerprints/palm print, we can match a fingerprint/palm print, in order to identify persons.



Source: Subarno Banerjee, <http://www.all-about-forensic-science.com/fingerprint-identification-points.html>

➤ Iris identification

✓ We can use mathematical pattern-recognition techniques – iris recognition- (on images of individual's eyes irises), or ocular technology –retinal scanning- in order to identify persons.

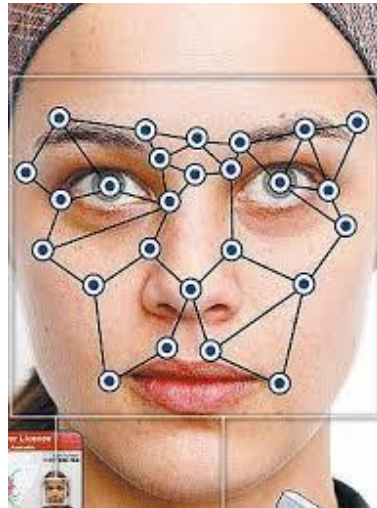


Source: An iris recognition machine at the Schiphol Airport

www.macrumors.com

➤ Face recognition.

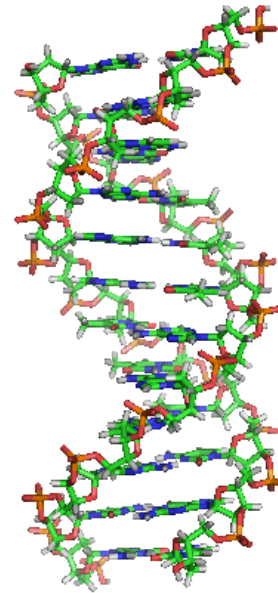
- ✓ Face images can be captured in order to identify persons.



Source: www.dailytelegraph.com.au

➤ DNA technology.

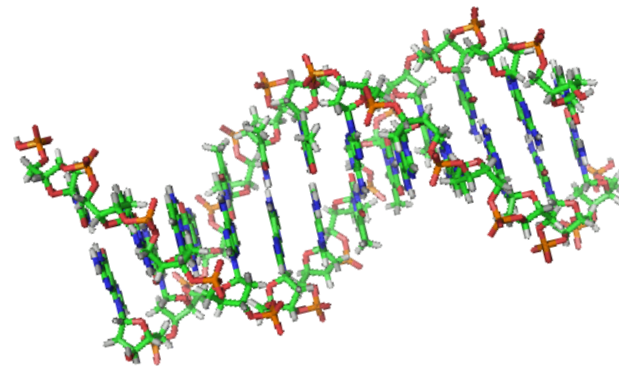
✓ It is based on the characteristics of all living organisms, including humans, who are determined by information contained within DNA. We can use this information in order to identify individuals.



➤ DNA technology.

✓ The molecules of DNA (deoxyribonucleic acid) contain information that is of great importance for their special features since except for identical twins, each individual has a different, unique, and unrepeatable DNA.

✓ The exclusivity of DNA facilitates its use for both investigation of paternity, and identifying persons in criminal investigation, obtaining DNA or genetic profile, which is composed of DNA or genetic data resulting essential.



➤ DNA technology.

✓ The called “DNA fingerprint” (Jeffreys, Wilson, Thein, 1985) is actually:

- the new “language of truth” (Hindman & Prainsack, 2010, 1)
- the new “gold standard” (Colle & Lynch, 2010, 123)

➤ DNA technology.

✓ We can use for criminal investigation the called **non-coding DNA, defined as the one that providing a characteristic of each individual**, it is an anonymous code distinguishing feature and it can be useful for identifying the identity but **it does not provide information on to physical or phenotypic traits of the individual** (the called coding DNA). But **we also use the provision of the sex characteristic of the subject.**

▪ **Problem: The progress of Science can convert non-coding DNA in coding DNA** (Gómez Sánchez, 2007)

➤ DNA technology.

✓ Really, the problems in relation to this goal arise at three levels: the technical conditions (**effectiveness**), the respect of fundamental rights and legal guarantees in the realization of the DNA evidence (**validity**), and the interpretation of the results (**probability**)

▪ Nevertheless, my research is focused on the **validity of the DNA evidence, and particularly regarding fundamental rights protection**; within the aim of see if DNA criminal databases are effective against serious national and transnational crime (Cabezudo Bajo, 2013)

❖ The violation of fundamental rights: nullity (prohibited evidence). Are there **additional Safeguards to protect Children?**

➤ DNA technology.

✓ *The three stages structure of the called “forensic use of DNA technology”*

▪ The called forensic use of DNA technology can be structured in three different stages:

1) the **sample collection**,

2) the **extraction of DNA profile**, and

3) The **treatment of the DNA data in a criminal database**

▪ And we should obtain a DNA evidence with the maximum respect of fundamental rights in the three stages) (Cabezudo Bajo, 2011, 2012)

IV. DNA technology legal framework

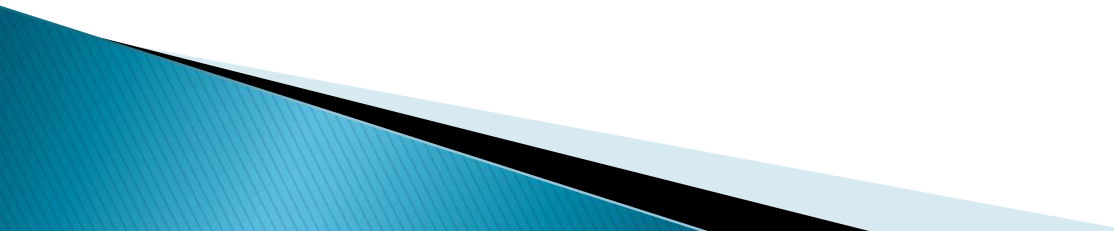
➤ The use of DNA technology is based on different legal instruments:

- ✓ International legal framework

- ✓ EU legal framework

- ✓ National legal frameworks.

➤ According to the aim of this paper, we are interested in the international and particularly the EU legal framework. But it is important to note that international and EU legal instruments are usually implemented by national bodies applying national legal frameworks.



IV. The DNA technology legal framework

➤ **International (non EU) Legal Framework**

✓ **Bilateral Agreements** between States (for example the recent Agreement between UK and Australia)

✓ **Interpol DNA Gateway**

▪ Interpol member states can upload DNA profiles, and others can use the central database (It is a central DNA database or DNA central record)

▪ Interpol Standard Set of Loci (ISSOL) (24 loci)

IV. The DNA technology legal framework

➤ **The EU Legal Framework (Assumption of Prüm Convention regime)**

✓ 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 (known as Prüm decision)

✓ 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.

✓ Council Decision **2010/482/EU of 26 July 2010** on the conclusion of the Agreement between the European Union and Iceland and Norway on the application of certain provisions of Council Decision 2008/615/JHA and Council Decision 2008/616/JHA

➤ The EU Legal Framework

▪ DNA Prüm system.

✓ Use of DNA national databases connected with national contact points on so called hit/non hit basis (the result is yes/no, and if it is yes: request of the personal information). **It is very different from the Interpol Gateway. Under Prüm mechanism, EU Member states retain their DNA profiles in their own DNA databases.**

✓ (Recommended) use of the European standard set of loci (EES) (7) established in 2001 (EU Council Resolution 9192/01), extended to 12 loci in 2009 (EU Council Resolution 2009/C 296/01). But they can use also the Interpol Standard (ISSOL).

✓ According to the Annex of the Council Decision 2008/616/JHA, chapter 2, Member States must use DNA profiles containing at least “six full designated loci”

✓ The EU Council Resolutions are not binding... they call upon European countries to use the EES (a lot of EU Member States use CODIS (USA loci CODIS))

➤ The EU Legal Framework

▪ Loci Standards

Locus	European Standard (ESS)	Interpol Standard (ISSOL)	USA (CODIS core-loci)
D1S1656	X	X	
D2S1338		X	
TPOX		X	X
D2S441	X	X	
D3S1358	X	X	X
FIBRA (FGA)	X	X	X
D5S818		X	X
CSF1P0		X	X
ACTBP2 (SE33)		X	
D7S820		X	X
D8S1179	X	X	X
D10S1248	X	X	
TH01	X	X	X
VWA	X	X	X
D12S391	X	X	
D13S317		X	X
Penta E		X	
D16S539		X	X
D18S51	X	X	X
D19S433		X	
D21S11	X	X	X
Penta D		X	
D22S1045	X	X	
Amelogenin		X	X

Source: ENFSI, 2014, and own elaboration. The loci in yellow are the first European Standard Set (EES)

➤ The EU Legal Framework

➤ According to Prüm Decisions on 26 August 2011 EU Member States had to comply with the automated searching provisions in order to be willing to exchange DNA data between them.

▪ However, the reality is very different. Today [data of 20 January 2015], **only 22 of the 28 EU Member States have operational their DNA databases** in order to share DNA data. And UK, after the opt-out decision is not operating under Prüm Decisions Regime.

▪ Regarding the rest (21) of the operational EU Member States, it is important to note that not every of them are prepared to share DNA data between them.

[Presidency, 'Implementation of the provisions on information exchange of the "Prüm Decisions" - overview of documents and procedures - overview of declarations - state of play of implementation of automated data exchange (9377/EU XXV.GP)', 20.01.2014. Available at: http://www.parlament.gv.at/PAKT/EU/XXV/EU/00/93/EU_09377/imfname_10434179.pdf, accessed on 10 July 2015]

➤ The EU Legal Framework

▪ The UK opt-out decision

✓ One of the actual trends related to the EU Legal Framework on DNA technology is the eventual consequences of the recent UK opt-out decision regarding the measures in the field of police co-operation and judicial co-operation in criminal matters adopted prior to Lisbon Treaty, including the Prüm regulation, according to the article 10(4) of Protocol 36 to the Lisbon Treaty, after the ends of the transitional period on 1 December 2014 .

▪ Report "The UK block opt-out in police and judicial cooperation in criminal matters: recent developments",
www.parliament.uk/briefing-papers/SN06930.pdf)

➤ **The EU Legal Framework**

▪ **The UK opt-out decision**

✓ The involved consequences of the UK opting out decision of EU Criminal law was well pointed out two years ago, and particularly regarding Prüm Decision. It was noted that "UK would be relieved of any duty to provide automated access to its databases (...) At the same time, UK law enforcement authorities would not be able to have direct and automatic access to other Member States' databases" (Hinajeros & Spencer & Peers, 2012: 18).

✓ One of the problems is that the opt out is on block. Certainly the UK notified the Council on 24 July 2013 that it would exercise this block opt-out option.

✓ After that the UK negotiated opting back into 35 measures. However, Prüm Decision is not within them. Nevertheless, to opting back, the EU Member States must agree unanimously on it, and at the General Affairs Council on 24 June 2014, some EU Member States expressed reservations. Therefore, on 6 November 2014 the UK Government published the Draft Criminal Justice and Data Protection (Protocol 36) Regulations 2014 which aim to transpose into UK law further measures to fully implement 11 of the 35 measures.

➤ The EU Legal Framework

▪ The UK opt-out decision

✓ In order to solve the eventual problems of the Prüm decision opt out (and to replace it), the UK seems to compromise to share DNA data with EU Member States, but with a limited access to the UK'S DNA database ("Police to share DNA database with Europe's force", Financial Times, 12 November 2014, www.ft.com/cms/s/0/5213f5ae-6a82-11e4-8fca-00144feabdc0.html#axzz3NHceO94Z [Accessed on 29 December 2014])

✓ However, **the actual situation is very unclear**. In fact, the information available at the document cited on the Implementation of the provisions on information exchange of the "Prüm Decisions", is that UK is "Currently evaluating a range of options for the changes necessary to deliver the significant business and technical changes required to meet the obligations arising from the Prüm Decisions. Strategic planning and mapping of the way forward is continuing"

(Presidency, 'Implementation of the provisions on information exchange of the "Prüm Decisions" cit)

➤ The EU Legal Framework

▪ The UK opt-out decision

✓ Moreover, and according to the **European Council Decision 2014/836/EU** the UK is to undertake a full business and implementation case in order to assess the merits and practicals benefits of rejoining, and the necessary steps for it to do so (the results of which are to be published by **30 September 2015**). And if the result is positive, the UK will decide, by **31 December 2015** whether to notify the Council, within the following four weeks, of its wish to participate in the Prüm Decision.

V. Fundamental rights protection in EU Multilevel System

V. Fundamental rights protection in EU Multilevel System

➤ *Multilevel constitutionalism perspective*

- ✓ There are at least three levels to take into account:
 - International level (International instruments on human rights, and particularly European Convention Human Rights standard)
 - EU Level (EU Fundamental Rights Charter standard / and Fundamental Rights as General Principles of EU Law in the ECJ case law)
 - National Level ([Constitutional] fundamental rights standards)

➤ The “forensic use of DNA technology” must guarantee the respect of fundamental rights in the three stages in which we can structure it [Cabezudo Bajo, 2011, 2012]: 1) the **sample collection**, 2) the **extraction of DNA profile**, and 3) the **treatment of DNA profile in a criminal database**.

V. Fundamental rights protection in EU Multivel System

➤ From the perspective of an EU exchange of DNA data (Prüm Decisions) regarding the fundamental rights protection, it is important to note that:

A) The 1) the **sample** collection, and 2) the **extraction of DNA** profile, and 3) the **national treatment of DNA data (the inclusion of the profile and its treatment in the national database) is made under the national law of the Member State in witch the DNA sample is collected, extracted and treated** in its national database

- ✓ Each EU Member State retains the responsibility of the DNA profiles to process them according to the national law (Cabezudo Bajo, 2008)

V. Fundamental rights protection in EU Multivel System

B) Regarding the exchange of DNA Data (always using the national contact point) the requesting Member State is allowed to conduct **automated searches** by comparing DNA profiles in other Member States (article 3 (1) Prüm Decision) and in case of a “hit” (match), the requesting Member State shall receive in an automated way the **reference data** which a match has been found (article 3(2) Prüm Decision).

- ✓ Searches may be conducted only for the investigation of **criminal offences** and in **individual cases** and in **compliance with the requesting Member State`s national law**” (article 3(1) Prüm Decision).

V. Fundamental rights protection in EU Multivel System

C) EU Member States can also (by mutual consent) and always via their national contact points compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other national DNA EU Member States database, and if the result is a hit (**mach**) the second one “shall, without delay, supply the other Member State`s national contact point with the reference data with witch a match has been found” (article 4 Prüm Decision)

✓ Searches may be conducted only for the investigation of **criminal offences**

V. Fundamental rights protection in EU Multivel System

✓ It is important to note that in both procedures (articles 3 and 4 Prüm Decision) the requesting State only obtains a “reference data” (a reference number, without personal information).

D) In order to obtain personal data, the supply of this information “shall be governed by the national law including the legal assistance rules, **of the requested Member State** (article 5 Prüm Decision).

✓ This “can be carried out according to mutual assistance procedures, bilateral agreements on information exchange, Council Framework Decision 2006/960/JHA [on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union] and other legal instruments” (Soletto Muñoz & Fiodorova, 2013, 152)

V. Fundamental rights protection in EU Multivel System

E) According to article 25(1) of Prüm Decision, regarding the processing of personal data “which are or have been supplied” each Member State shall guarantee a level of **protection of personal data in its national law at least equal to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol of 8 November 2001, and taking account of Recommendation No 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.**

✓ The supply of data may not take place until these provisions have been implemented in the national law. The Council shall **unanimously decide whether this condition has been met.** This condition shall not apply to States where the supply of personal data under Prüm Treaty has already started (article 25(2) and (3) Prüm Decision).

V. Fundamental rights protection in EU Multivel System

E) The Data Protection Directive (95/46/EC) explicitly excluded from its scope of application data processing “in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) **and the activities of the State in areas of criminal law**” (art. 3(2)).

✓ And the future data protection package??

V. Fundamental rights protection in EU Multivel System

- The future data protection package includes a General Regulation and a Directive 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.**
- However, the data protection package initially leaves **unaffected Prüm regime** as was pointed out by the European Data Protection Supervisor (Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, 443, page 68). But the Amendment 6 of EU Parliament (14 March 2014) introduced it. (EP legislative resolution of 12 March 2014 [COM\(2012\)0010](#) – C7-0024/2012 – [2012/0010\(COD\)](#)) Today (from 4 December 2014 is in discussion within the Council (<http://eur-lex.europa.eu/procedure/EN/201285>). Last access 10 July 2015)

V. Fundamental rights protection in EU Multivel System

➤ **Fundamental rights involved and different standards in the EU multilevel system.**

✓ Nevertheless, one problem is that data protection is not the only fundamental right which can be affected by DNA technology, because **we may identify fundamental rights affected in the three stages above referred:**

rights to private life

bodily integrity

home inviolability

the right to defence

the protection of personal data

...

V. Fundamental rights protection in EU Multilevel System

✓ And we may also identify the different ***protection standards*** involved in the EU Multilevel system...

- *International human rights level*
- *National level*
- *EU level*

Charter of Fundamental Rights of EU
(article 52)

Level of protection (art. 53) ?

Fundamental Rights as General
Principles of EU Law (ECJ case law)

European Convention of
Human Rights

Common constitutional traditions
in EU Member States.



Higher level of protection criteria ? (Sarrión Esteve, 2014)

Fundamental rights level protection, article 53 EU Fundamental Rights Charter.

*Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms **as recognized**, in their respective fields of application, by **Union law and international law** and by **international agreements** to which the Union, the Community or all the Member States are party, **including the European Convention for the Protection of Human Rights and Fundamental Freedoms**, and by the **Member States' constitutions.**"*

V. Actual data protection guarantees in Prüm Decision

V .Actual data protection guarantees in Prüm Decision.

Article 2:

1. *Member States shall open and keep national DNA analysis files for the investigation of criminal offences. **Processing of data kept in those files, under this Decision, shall be carried out in accordance with this Decision, in compliance with the national law applicable to the processing.***

2. *For the purpose of implementing this Decision, **the Member States shall ensure the availability of reference data from their national DNA analysis files** as referred to in the first sentence of paragraph 1. Reference data shall only include DNA profiles established from 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. Reference data which is not attributed to any individual (unidentified DNA profiles) shall be recognisable as such.*

...



V .Actual data protection guarantees in Prüm Decision.

Chapter 6 of the Prüm Decision is focused on the guarantees of data protection.

It is important to note:

- ✓ Article 25 (level of data protection),
- ✓ Article 26 (purpose),
- ✓ Article 27 (competent authorities) and
- ✓ Article 28 (Accuracy, current relevance and storage time of data)

Art. 25. Level of data protection:

1. *As regards the processing of personal data which are or have been supplied pursuant to this Decision, each Member State shall **guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol of 8 November 2001** and in doing so, shall take account of Recommendation No 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, also where data are not processed automatically.*

2. *The supply of personal data provided for under this Decision may not take place until the provisions of this Chapter have been implemented in the national law of the territories of the Member States involved in such supply. The Council shall unanimously decide whether this condition has been met.*

3. *Paragraph 2 shall not apply to those Member States where the supply of personal data as provided for in this Decision has already started pursuant to the Treaty of 27 May 2005 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 (Prüm Treaty).*

VI. Additional Safeguards for Children

VI. Additional Safeguards for Children .

➤ **Best minor interest principle.**

➤ **Application of general regulation** (Prüm Decision, and national legislation, in Spain: *Ley Orgánica 10/2007, reguladora de las bases de datos policiales sobre identificadores obtenidos a partir del ADN*), which does not provide special guarantees for Children.

➤ Nevertheless, there are **special guarantees** at national level, for example provided in Spain in the *Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores*:

✓ Public Prosecutor leads the criminal investigation in order to guarantee the rights of the minor (art. 6 LO. 5/2000). The general rule is that the Police leads the criminal investigation.

✓ The judicial resolution of the Minor's Judge is a requirement to restrict minor's fundamental rights (article 23.3 L.O. 5/2000), there is a special judge.

VI. Additional Safeguards for Children .

✓ Except for the arrest, any restrictive measure will be interested via Public Prosecutor to the Minor's Judge. The police can not request directly the measure. (art. 2.2. *Royal Decree 1774/2004, of 30 July approving the Regulation of LO 5/2000*).

❖ It would be advisable to reform the national regulation of police DNA database in order to introduce an specific regulation for Children. Direct police request? A Public Prosecutor binding report?

VI. Additional Safeguards for Children .

✓ **Biological sample collection:** 1) Public Prosecutor request to Minor's Judge; 2) Abandoned samples (like in general situation); 3) Child's consent?

❖ The consent must be the general rule for DNA sample collection, but in case of minors... the question is if a minor can consent itself, and if so at what age.

❖ L.O. 5/2000. Starting point for criminal responsibility: 14 years old (article 1.1.) would be the starting point in order to collect DNA samples with minor's consent.

❖ Instrucción 11/2007, de 12 de Septiembre de la Secretaría de Estado de Seguridad, por la que se aprueba el Protocolo de actuación policial con menores: DNA sample collection as a fundamental rights restricting measure is forgotten for minors under 14 years old.

VI. Additional Safeguards for Children .

- ✓ Doctrine has considered the possibility of use the DNA sample collection in order to avoid false self-accusations (Dolz Lago, 2008: 7), but others consider that it disproportionate, even in this cases (Navarro-Michel, 2014: 182)
 - ❖ A legal reform to adequate the regulation of DNA sample collection for minors in attention of the age?

✓ DNA data cancelation.

- Although there is a general regulation in L.O. 10/2007, in the case of minors as the time of prescription are also reduced, the cancellation terms are lower than in general cases (article 15.1 L.O. 5/2000).
- Moreover, the general rule of criminal records does not play, so whit the compliance of the punishment the DNA data must be cancelled.

Conclusions?



Conclusions?

- The so called biometric technologies help us to identify individuals using for example **fingerprint/palm print identification, iris identification, face recognition and DNA technology.**
- We need to use these technologies with respect to fundamental rights and legal guaranties (**legality**) and the use of best scientific practices (**effectiveness**). Regarding the legality question, **in the case of minors require special attention and specific (additional) guarantees.**
 - ✓ **Multilevel fundamental rights protection perspective-standards**
- **The need of a specific regulation for the use of these technologies in the case of minors, with special attention to their specific conditions.** Example: DNA technology in DNA sample collection.

➤ **References**

BILANCIA, P., DE MARCO, E., (coord.) (2004): *La tutela multilivello dei diritti. Punti di crisi, problema aperti, momento di stabilizzazione*, Giufrè, Milán. CABEZUDO BAJO, María José (2008): "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal", in De la Oliva Santos et al (eds), *La justicia y la Carta de Derechos Fundamentales de la UE*, 327-342.

CABEZUDO BAJO, María José (2011): "Valoración del sistema de protección del dato de ADN en el ámbito europeo", *Revista General de Derecho Europeo*, 25, 2011.

CABEZUDO BAJO, María José (2012): "La regulación del "uso forense de la tecnología del ADN" en España y en la UE: Identificación de cinco nuevas cuestiones controvertidas", *Revista General de Derecho Procesal*, 26, 2012.

CABEZUDO BAJO, María José (ed) (2013): *Las bases de datos policiales de ADN ¿son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza*, Dykinson.

COLLE, S.A., and LYNCH, M. (2010): "DNA profiling versus fingerprint evidence: more of the same?", en HINDMAN, R., y PRAINSACK, B., (Ed.), *Genetic Suspects. Global Governance of Forensic DNA Profiling and Databasing*, Cambridge, University Press

DOLZ LAGO, (2008). "Problemática de la toma de muestras de ADN a los menores y su tratamiento legal", *La Ley Penal*, 14.

GÓMEZ SÁNCHEZ, Y. (2007): "Los datos genéticos en el Tratado de Prüm", *Revista de Derecho Constitucional Europeo*, 7.

GÓMEZ SÁNCHEZ, Y. (2011): *Constitucionalismo multinivel. Derechos fundamentales*, Sanz y Torres.

HINAJEROS, A., SPENCER, J.R., PEERS, S. (2012): "Opting out of the EU Criminal law: What is actually involved?", CELS Working Paper, New Series, 1.

HINDMAN, R., y PRAINSACK, B., (Ed.) (2010): *Genetic Suspects. Global Governance of Forensic DNA Profiling and Databasing*, Cambridge, University Press.

JEFFREYS, A., WILSON, V., THEIN, S. (1985): "Individual-specific 'fingerprints' of human DNA", *Nature*, nº 316, 1985, pp. 76-79.

NAVARRO-MICHEL, M. (2014). L'enseignement aux élèves marocains de la deuxième generation dans le pays d'accueil. En M. Casado y M. Guillén (coord.). *ADN forense: problemas éticos y jurídicos*. Observatori de Bioètica i Dret (pp. 169-190)

SARRIÓN ESTEVE, J. (2014): "Sobre la necesidad de buscar el estándar o nivel más alto de protección de los derechos fundamentales en el sistema de tutela multinivel en la Unión Europea", *CEFLegal: revista práctica de derecho*, 162, pp. 155-184.

SARRIÓN ESTEVE, J., BENLLOCH DOMENECH, C. (2014): "Biometric Technologies Trends in Relation to Fundamental Rights Protection in European Union Security Policy: With a Particular Approach to DNA Technology". Available at SSRN: <http://ssrn.com/abstract=2542512> [30 December 2014]

Many thanks for your attention!

