Special issue

Forensic genetics: The evolving challenge of DNA cross-border exchange

Lucia Scaffardi*

ABSTRACT: Forensic genetics has significantly reshaped the investigations' methods and simultaneously brought numerous ethical and legal challenges, especially in the area of DNA data exchanges. By retracing the history of DNA cross-border exchanges within the so-called Prüm framework, this paper aims to underline not only the current inhomogeneity of Member States' legislations in this complex field but also the existing inefficiencies in the implementation and application of the "Prüm system". On this basis, potential developments and possible reform solutions are analysed, with the purpose of explaining and reflecting on the opportunities and risks enshrined in the so-called Next Generation Prüm.

KEYWORDS: DNA; DNA databases; genetic forensics; Next Generation Prüm

SUMMARY: 1. The DNA on trials: what has been uncovered and what remains hidden – 2. Learning from experience. The history of DNA cross-border exchanges and their expansion – 3. The inhomogeneity of Member States' legislations and the difficult implementation of the "Prüm system" – 4. The uncharted territory of Next Generation Prüm.

1. The DNA on trials: what has been uncovered and what remains hidden

The outbreak of DNA analysis as forensic evidence in criminal investigations and Courts has brought important legal and ethical issues.[1] Indeed, the deployment of such new methodology has made crystal clear that the "circulation" of genetic data is linked not only has undeniable advantages but also potential risks related to the use of genetic information. Moreover, methods of collection, retention and deletion of data, both within the European Union and around the world, may differ significantly according to different domestic legislations; therefore, many difficulties arise with regards to the use and exchange of such data.[2] When we discuss forensic evidence related to genetic data, it is important to remember that the perspective may shift beyond the specific individuality of a person and become ultra-personal. Thus, it is essential to understand how a new axiological arena has taken shape and how different rights and freedoms, from personal

**Associate Professor in Public Comparative Law at the University of Parma. Mail: lucia.scaffardi@unipr.it.* *The article was peer-reviewed by the editorial committee.*

[1] On this point, see a recent and comprehensive contribution: H. MACHADO, R. GRANJA, *Forensic Genetics in the Governance of Crime*, Singapore-Braga, 2020.

[2] For a broader reflection on this specific issue, see: L. SCAFFARDI, *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche dati del DNA a fini giudiziari*, Milano, 2017.

ISSN 2284-4503

freedom to privacy, from the right to health to informed consent, could be balanced with other subjective legal positions.

This paper aims to provide an evolving discussion on how the use of DNA fingerprint has reshaped the debate on some of the rights involved. Courts and judges have played, in this context, an important role, given that judgments have become essential to building a new interpretation of the subject, inherently linked with its practical dimension and with relentless technological progress.

The impulse brought by rulings has been essential to provide interpretative parameters guaranteeing individual and ultra-personal rights. New and interesting developments are nowadays characterising this subject, which is still far from being untangled. Possible enhancement in the use and exchange of genetic data and non-genetic data may in fact be found in the innovations proposed in the Next Generation Prüm, which will be analysed in the following paragraphs. It is therefore evident, in such a scenario, that genetic data, as forensic evidence, represents an open and always evolving challenge.

2. Learning from experience. The history of DNA cross-border exchanges and their expansion

The use of DNA for identification purposes dates back to 1985 when Alec Jeffreys paved the way for this new methodology,[3] analysing and comparing the genetic material found on a crime scene with the one of a suspect. Thanks to the continuous enhancement of molecular technology techniques, it became possible to implement DNA repositories, which allow an electronic comparison of the data contained within them. Obviously the creation of specific databases has further increased the possibilities to solve police investigation, turning genetic tests into a real "operational system": in 2007 Grimm underlined that the USA genetic database[4] was able to analyse 100.000 profiles in 500 microseconds.[5] In the European context, it can be pointed out that the total number of identifiable

[3] See A.J. JEFFREYS, V. WILSON, S.L. THEIN, *Individual-Specific "Fingerprints" of Human DNA*, in *Nature*, Vol. 316, 1985.

[4] For a reconstruction of the debate, occurred in the USA, around different methods that led to an increasing expansion of the central database, see J. D. ARONSON, *On trial! Governing forensic DNA technologies in the USA*, in R. HINDMARSH, B. PRAINSACK (a cura di), *Genetic Suspects: Global Governance of Forensic DNA Profiling and Databasing*, Cambridge, 2010, 254 ff.

[5] D.J. GRIMM, *The demographics of genetic surveillance: familial DNA testing and the hispanic community,* in *Columbia Law Review*, Vol. 107, 2007, 1169. In order to understand the swirling increase (updated to December 2020) of the DNA profiles' number currently at the disposal of USA authorities at both national and federal level see: https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics. Within the vast bibliography on this topic, particular attention should be given to the following contributions and the references cited therein: S. KRIMSKY, T. SIMONCELLI, *Genetic Justice. DNA Data banks, Criminal Investigations and Civil Liberties*, New York, 2011; M. TAYLOR, *Genetic Data and the Law. A critical Perspective on Privacy Protection*, Cambridge, 2012; K. J. STROM, M. J. HICKMAN, *Forensic Science and the Administration of Justice,* in *Critical Issues and Directions*, London, 2015.

ISSN 2284-4503

persons' profiles stored in national databases amounts to approximately 11,5 millions, along with 1,6 million of data that refer to non-identifiable persons.[6]

The potential of such data should be considered not only with regard to their possible use at national level but also as important information to be exchanged between Member States in order to improve the investigative cooperation.

In the last few decades, the rise and development of forensic genetic databases have been strongly affected by the possibility of cross-border exchange of data[7] (within and beyond EU borders) and by the constant technological process, which has led to increasingly pervasive methods of production, collection and retention of data.[8] On the other hand, crimes have progressively taken on a cross-border dimension –international terrorism, drug trafficking or human smuggling and, moreover, irregular migration and organised crime. It has become more and more essential to provide law enforcement authorities with investigative tools that can cross borders and enhance information exchange and transnational cooperation.

In this context, for what specifically in relation to genetic data, DNA exchange systems have proliferated; such systems can be defined as mechanisms of DNA cross-borders exchange (which allow for the comparison and matching of DNA profiles) that can assume different and constantly evolving dimensions and characteristics.[9]

An interesting and recent attempt at systematization[10] has shown that there are different types of *exchange systems,* among which particular attention may be given to*:* (1) *international database,*

[6] European data provided by European Network for Forensic Science Institutes (ENFSI) in 2017 and available at www.enfsi.eu. For a comprehensive study about data collection in various continents see INTERPOL, see *Global DNA Profiling Survey Results*, 2019.

[7] In order to understand such developments, it is interesting to see the scientific study developed between 2011 and 2015, reporting data concerning DNA profiles' exchange among EU Member states. This study represents the first systematic analysis in this field, based on official statistics drafted pursuant to the adoption of the so-called Prüm system. It clearly shows that the difficulty of finding statistic data, which is still a complicated and outstanding problem, is a main issue. Another challenging topic is related to the fact that, still nowadays, it is very complex to properly establish the concrete results deriving from implemented policies and to consequently guarantee transparency and accountability vis-à-vis citizens. Nonetheless, the study underlines the implementation of one-to-one exchanges between some Member states, among which Belgium, France, Netherlands and United Kingdoms. See F. SANTOS, H. MACHADO, *Patterns of exchange of forensic DNA data in the European Union through the Prüm system*, in *Science & Justice*, Vol. 4, no. 57, 2017, 307-313.

[8] It is essential to specify that the notion of "genetic data", in this context, needs to be interpreted in a specific way: in particular for what concerns the information exchange system among Member States for investigative purposes, "genetic data" refers to the information resulting from the non-coding part of the DNA. Data to be exchanged do not contain information that could lead to the direct identification of a subject, at least in the first phase of the exchange system, which will be analysed below.

[9] This constant evolution of cooperation and data exchange system is influenced by both a growing number of States that decide to implement national DNA databases and a continuous technical-scientific progress that allows for the development of new research methods and innovative investigative systems based on genetic data. Consider, as an example, the so-called familial searching technique, analysed in this Journal in G. FORMICI, *From "familial searching" to "forensic genetic genealogy": new frontiers – and challenges – of DNA analysis in criminal investigations*.

[10] A.O. AMANKWAA, *Trends in forensic DNA database: transnational exchange of DNA data*, in *Forensic Sciences Research*, no. 1, 2019.

such as the Interpol database;[11] (2) interrelated and connected national DNA databases, that can be found in the EU system based on the Prüm Treaty; (3) bilateral or multilateral agreements concerning the exchange of genetic data following the request of a national authority.[12]

Given that one of the main potentials uses of databases is the possibility to compare data and exchange information, it goes without saying that a national system should not be considered on its own but, rather, regarded within the general context of European rules, that strongly affect domestic choices.

The value of these tools is evident[13] but it is, at the same time, important to take into proper consideration the risks that may be inherent to the sharing and exchanging of sensitive data like genetics. The invasiveness of these operations is significant, especially with regards to privacy and data protection, therefore it is essential to think carefully about the need to provide rules that fully guarantee the rights of the individual, in the context of sharing and exchanging information.

Consequently, it is evident that the main challenge that national and supranational legislators are facing is finding the correct balance between security[14] and respect of privacy and data protection rights.[15] Indeed, the former calls for fully operating systems of collection, retention, access and exchange of data while the latter requires conditions able to guarantee that every interference in the personal sphere of the data subject is proportionate to the purpose being pursued.

Facing such a complex challenge, the European Union has demonstrated great attention to this, deciding to "Europeanise" the provisions of the Prüm Treaty (i.e., encompassing them into its normative framework), which namely, DNA exchange, fingerprint data and information about the registration of vehicles.

In doing so, the EU imposed its Member States to adopt national legislation governing collection and exchange of genetic data for judicial purposes, in compliance with supranational criteria. Member States were required to develop national databases, as an essential prerequisite of comparing and matching different profiles coming from other Member States' authorities and for the subsequent exchange of information of the identified suspect.

---

[11] Built in 2002, this database contains more than 180.000 genetic profiles, gathered with the cooperation of more than 84 Member States: "Police can submit a DNA profile taken from offenders, crime scenes, missing persons and unidentified human remains, with a search result provided within minutes. Our database has enabled investigators around the world to link offenders to different types of crime including rape, murder and armed robbery. There is no nominal data attached to the profile, which is submitted in the form of an alphanumerical code. Member countries retain ownership of the information, in line with our rules on the processing of data. Countries can also choose which other countries they share their data with", https://www.interpol.int/How-we-work/Forensics/DNA

[12] This category includes the important bilateral agreements concluded between USA and other Countries around the world, which define specific conditions for genetic data exchange (The agreement with Italy dates back to May 28th 2009).

[13] See P. GILL, *National DNA Databases, Strength of Evidence and Error Rates*, in P. GILL (ed), *Misleading DNA Evidence*, Cambridge, 2014, in particular 81 ff.

[14] See L. SCAFFARDI, *Banche Dati del DNA e scambio internazionale fra esigenze securitarie e tutele dei cittadini,* in L. SCAFFARDI (ed), *La banca Dati italiana del DNA. Limiti e prospettive della genetica forense*, Bologna, 2019.

[15] These rights are ensured, at the EU level, within the context of the Charter of fundamental rights of the European Union, incorporated as additional protocol by articles 7 and 8 of the Lisbon Treaty.

Consequently, it is obvious that the creation of a national databases' network, formally separated but tied together by cooperation obligations, had a huge impact on the domestic system of each Member state. It should however be pointed out that the supranational legislation has left a certain degree of discretion to national legislators, which resulted in different approaches. Thus, it is essential, in a comparative perspective, to reflect on the similarities (i.e. homogeneity of legislative choices) and/or on the differences that characterise domestic strategies that, within a continuous dialogue with the EU level and among Member States, will affect the capability and the efficiency of the whole system.

3. The inhomogeneity of Member States' legislations and the difficult implementation of the "Prüm system"

The inclusion of specific provisions regulating the use and exchange of genetic data for judicial purposes, within the EU legal framework, was a long and troubled journey. In 2005 seven Member States decided to sign the so-called Prüm Treaty, open to all other Members wishing to join, with the aim of encouraging the implementation of a system of collection, access and exchange of data, such as DNA, fingerprints and information about registration of vehicles, in order to enhance the mechanisms of police cooperation. The Treaty stemmed from the need to fight criminal activities in a more efficient way that were, at that time, rapidly expanding (e.g., terrorism, illegal immigration, organised crime). By understanding the importance of that agreement and being willing to include it in the EU legal framework, the Council adopted, in 2008, the Decisions 2008/615/JHA and 2008/616/JHA, after a long and trouble *iter*, often characterised by setbacks and concerns expressed by the EU institutions involved.[16] These Decisions replicated the provisions of the Prüm Treaty[17] and provided Members states with the possibility of "sending" a DNA profile to another Member state if the identification process didn't result in a match, at national level within their own DNA database. The ither Member States, receiving the DNA profile, can subsequently verify if they can find a matching profile within their own DNA national databases. This first "hit/no hit" phase is fully-automated and is carried out by the so-called national points of contact; it does not require a proper exchange of personal data but rather a mere comparison – by means of "silent codes" – between the profile sent by the requesting Member state and the ones collected in all other national databases within the EU. Only in the case of a positive response (hit), does a second phase take place and the personal information related to that profile can be requested so that it becomes possible to trace the identity of the person to whom that profile belongs. This procedure, dived into two separate steps, allows for a greater speed in the first phase and guarantees a higher level of data protection, by imposing a disclosure of personal data only in the second phase and only if the automated operation of comparison and matching resulted in a positive outcome. The abovementioned exchange of data

[16] Both the European Data Protection Supervisor and European Parliament expressed doubts with regard to the decision and the employed normative source and proposed some amendments to the text draft elaborated by the Council.

[17] Decision 2008/615/JHA, point 10.

can only take place after the implementation of the EU Decisions at national level:[18] it is necessary to set up national databases, through which the operations of checking will be conducted, along with the establishment of "Contact points" and formalised ways of requesting and replying to other Members States' demands. All these requirements need to be implemented by national legislators who are also required to define the criteria and conditions for the entry of genetic data (samples or profiles) into the national databases.[19]

Some harmonizing measures were also introduced with the Council Decisions: for example, legislators are asked to comply with some specific common requirements,[20] such as defaulting European standards (ESS; ISSOL). It is moreover compulsory to conform to others technical standards: with regard to the processing of the data that will be exchanged, each Member State must guarantee a certain degree of data protection within its domestic framework.[21]

This drive to harmonize the system, is reaffirmed by the fact that the Council has implemented a control procedure which allows them to check if Member States are complying to European standards and thus gives them to the power to authorize or deny access to the national databases' network.

Although the Union has repeatedly underlined the necessity to reach a complete harmonisation of national provisions, there are still many disparities among Member States concerning both the correct implementation of the abovementioned Decisions and the normative choices in this field. Such a complex scenario also emerges from the Fifth progress report towards an effective and genuine Security:[22] "In the area of information exchange between Member States, the Prüm Decisions of 2008 introduced procedures for fast and efficient data exchanges among Member States by laying down rules and providing a framework to allow Member States to search each other's DNA analysis files, fingerprint identification systems and vehicle registration data bases. Prüm was a tool that helped French investigators after the Paris terrorist attacks of November 2015. Considerable progress has been made in the implementation of Prüm in recent months with increasing volumes of data exchange. However, a number of Member States have still to implement the Decisions almost a

[18] Art. 25(2), Decision 2008/616/JHA.

[19] It is up to national legislators to adopt national laws that define conditions and criteria for the data processing and exchange, conditions that requesting Member States must always comply with (art. 26(1), Decision 2008/615/JHA).

[20] "Member States shall observe common technical specifications in connection with all requests and answers related to searches and comparisons of DNA profiles, dactyloscopy data and vehicle registration data. These technical specifications are laid down in the Annex to this Decision", art. 3, Decision 2008/616/JHA.

[21] The Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, establishes that: "Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA", Par. 94.

[22] Report from The Commission to the European Parliament, the European Council and the Council, *Fifth progress report towards an effective and genuine Security Union*, COM/2017/0203 final.

decade later. The Commission has therefore used the enforcement powers it acquired under the Treaty of Lisbon in the Justice and Home Affairs area to launch infringement".

In this context, the Commission launched infringement procedures against Croatia, Greece, Ireland, Italy and Portugal, due to the failure to ensure the automated exchange of two out of three data categories and the lack of implementation of the European Decisions. This move by the Commission was aimed at encouraging those Member States to rapidly create national databases and to increase the efficiency of police cooperation in EU territory. Notwithstanding the Commission's intervention, this problematic non-compliance situation still persists today: considering the data provided by the Council of the EU Council in the Document 5197/1/20 Rev 1 of June 25th 2020,[23] infringement procedures against Italy and Greece are still open. In its study on the implementation and future of the "Prüm system", the Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament has underlined that "these delays may be attributed to various factors, primarily linked to financial and technical difficulties. For example, Greece, Italy and Ireland did not have DNA *database*s or dedicated legislation when the Prüm Decisions were adopted. Besides, these countries were severely hit by financial crisis".[24]

In addition to these considerations, influenced by the particular situation that still characterizes Italy and Greece and significantly affected the implementation process of the Prüm Decisions of other Member states, what should be carefully considered is the profound complexity characterizing the concrete implementation procedure of the data circulation and data exchange mechanisms.[25]

Even considering the Member States that have actually implemented the recalled Decisions, many differences can be identified, related to (a) the entry criteria for individual profiles;[26] (b) exclusion criteria of collected profiles;[27] (c) retention or destruction of biological samples;[28] (d) authorities asked to run and control the databases and officials responsible for safeguarding and protecting the retained data.[29]

[23] Council of the EU, *Implementation of the provisions on information exchange of the "Prüm Decisions"*, 5197/1/20 Rev 1, June 25th 2020.

[24] Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament, *Police information exchange*, cit., 19.

[25] See art. 36, Decision 2008/615/JHA.

[26] In some Countries (Austria), data of convicted individuals - without distinction regarding the seriousness of the crime - are included in the national databases, while in other cases only data of individuals convicted for a "serious" crime are included (Belgium, France).

[27] Profiles of convicted individuals can be stored in national databases for different amount of time (depending on the national legislation) after the conviction or even after the death of the convicted person (Finland). By contrast, data of individuals suspected of a crime but then not convicted or considered not guilty, are generally deleted from the database.

[28] "Biological samples" refer to biological liquids or tissues from which a DNA profile may be obtained. Some national provisions require the immediate destruction of biological samples right after the profiles have been obtained (Belgium), while in other Member states biological samples are subject to the same rules envisaged for DNA profiles.

[29] Generally, they are public officials within the law enforcement structure or under the guidance of the Ministry of Justice.

On the basis of these distinctions,[30] some macro patterns may be identified: one particular group of Member States (that includes, for example Austria and Finland) has adopted national legislations that allow for the collection and retention of a significant number of profiles and consequently ensures the possibility of exploiting and large amount of information for the hit/no hit operations. In doing so, those Member States demonstrated the tendency to enhance security to the detriment of citizens' privacy and data protection. Another group of States has instead opted for a higher level of protection of fundamental rights, determining restrictive criteria for the collection, entry and retention of genetic data in national databases; this choice demonstrated its limits, by negatively affecting the efficiency and effectiveness of the whole system (one example above all, Portugal). There are then some models that can be placed in between these two approaches, such as the French emergency-type one (affected by actual historical circumstances) or the German one which aims at developing a system characterised by a fine balance between the need for a high level of protection of citizens' rights and not creating conditions that are too stringent.[31]

An interesting legislative choice had been taken by Italy[32] where the national DNA database[33] was placed under the control of the Ministry of Internal Affairs, while a central laboratory responsible the sequencing and retention of biological samples was implemented within the structure of the Ministry of Justice. The decision to create two different structures of storage within two separate Ministries shows the intention to ensure a high level of expertise in each field and provide specific guarantees for the individuals engaged in the data collection: the operations of collection and matching of DNA profiles occur in a place physically separated from the place where the operations of extracting and retention of DNA samples are carried out.

The Italian legislator, despite the great delay, has achieved an appropriate balance between crime prevention and privacy and data protection, with particular regard to the delicate issue of data erasing. They have shown themselves to be aware of certain implications derived from the fundamental judgment of the Court of Strasbourg in the Marper case,[34] according to which an indiscriminate collection of genetic data, also for judicial purposes, constitutes a violation of art. 8 of

[30] F. SANTOS, H. MACHADO, S. SILVA, *Forensic DNA databases in European countries: is size linked to performance?*, in *Life Sciences, Society and Policy*, no. 9, 2013. For a more generic overview on this issue see L. SCAFFARDI, *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, 37-64.

[31] For a thorough analysis of these models, in particular the ones adopted by Germany, UK and Portugal, see L. SCAFFARDI, *Giustizia genetica e tutela della persona*, cit., 69 ff.

[32] With the entry into force of Law no. 85 of June 30th 2009, published on the Official journal on 13th July 2009, Suppl. Ordinario n. 108, the national DNA database has been established. See on this point: G. GIOSTRA, *Gli importanti meriti e i molti limiti della nuova disciplina*, in G. CONSO, G. GIOSTRA (eds), *La disciplina del prelievo biologico coattivo alla luce della l. 30 giugno 2009, n. 85*, in *Giur. it.*, 2010, 1217 ff.; P. FELICIONI, *L'Italia aderisce al Trattato di Prüm: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici*, in *Dir. pen. proc., Speciale Banche dati*, 2, 2009, 6; L. SCAFFARDI, *Giustizia genetica e tutela della persona*, cit., 179 ff.

[33] After a long and complex legislative path, ended with the above mentioned Law no. 85/2009, the system became fully operative in 2018 after the adoption of the necessary implementing regulations and decrees during 2016 and 2017, that allowed the practical implementation of the national database.

[34] European Court of Human Rights, *S. and Marper v. United Kingdom decision*, [2008] ECHR 1581, 4th December 2008.

the ECHR.[35] In that case the Court was asked to evaluate the compliance of an English law, in force at that time,[36] to the fundamental rights protected by the ECHR: the Judges affirmed that the national provisions interfered with the right to privacy of the concerned individuals[37] due to the indiscriminate nature of the DNA samples' retention as well as the quantity and quality of personal information collected.

The Grand Chamber pointed out the undeniable utility of this forensic evidence (also including fingerprint conservation) and defined the conditions for proper use: the Court took the opportunity to reflect and make several useful observations related to the risks of stigmatization or indiscriminate use of forensic evidence.[38]

This important leading case brought about the revision of the English legislative framework in place at that time, but it also served as an important reference point for the development of similar legislation in other Member States.

4. The uncharted territory of Next Generation Prüm

The inefficiencies, delays and operative difficulties described in the previous paragraphs, together with the constant technological progress and the rise of new scientific techniques and investigative tools based on the use of personal data – genetic or biometric data for example – as well as the challenges determined by the spread of terrorism, organised crime and *cyber-crimes,* have prompted EU institutions, in particular the Council, to launch new initiatives by promoting studies, research and debates among experts and Member States 'authorities in order to modernise the Prüm Decisions, more than twelve years after their adoption. These intentions clearly emerge from the *Council*

[35] On the Marper case cfr. *ex plurimis*: A. SUTERWALLA, *DNA Discrimination*, in *New Law Journal*, Vol. 158, 2008, 505 ff.; A. JACKSON, *Public: Whose right is it anyway?*, in *New Law Journal*, Vol. 159, 2009, 187; C. NYDICK, *The British Invasion (of Privacy): DNA Databases in the United Kingdom and United States in the Wake of the* Marper *Case*, in *Emory International Law Review*, Vol. 23, 2010, 609 ff.

[36] In relation to *Section 64* of *Police and Criminal Evidence Act* of 1984, as modified in 2011 by the *Criminal Justice and Police Act*.

[37] The case was related to the claims lodged by two individuals: L.S., a minor arrested in 2001 and accused of attempted robbery and subsequently acquitted of charges, and Mr Marper, initially charged with sexual harassment on his wife, who then dropped the charges. Both subjects requested the destruction of their fingerprints and biological samples, previously collected and retained by the police during the investigations. After the rejection of their requests and having expired all internal remedies without success, they lodged their complaints before the European Court of Human Rights

[38] The Court underlined some considerations of the Nuffield Council on Bioethics, an independent body composed of physicians, jurists, philosophers, scientists and theologians who discuss about these delicate issues, similarly to the Italian Committee on Bioethics. See point 38: "According to a recent report by the Nuffield Council on Bioethics, the retention of fingerprints, DNA profiles and biological samples is generally more controversial than the taking of such bioinformation, and the retention of biological samples raises greater ethical concerns than digitised DNA profiles and fingerprints, given the differences in the level of information that could be revealed. The report referred in particular to the lack of satisfactory empirical evidence to justify the present practice of retaining indefinitely fingerprints, samples and DNA profiles from all those arrested for a recordable offense, irrespective of whether they were subsequently charged or convicted. The report voiced particular concerns at the policy of permanently retaining the bioinformation of minors, having regard to the requirements of the 1989 UN Convention on the Rights of the Child."

Conclusions on the implementation of the "PRÜM DECISIONS" ten years after their adoption (Conclusions 11227/18 18th July 2018): in order to reach the goals set by the Renewed Internal Security Strategy *2015-2020,*[39] the "effective and efficient use of the "Prüm Decisions" is considered essential for intensifying information exchange, cross-border law enforcement cooperation, for increasing mutual trust and for supporting solving of serious crime and conducting terrorist investigations" (p. 2).

On this basis, the Council requested that a possible amendment of the Prüm Decisions be considered, in order to extend the scope of their application and update the technical and legal requirements necessary for the functioning of the exchange system.

A wide and detailed discussion concerning possible modifications and forms of modernisation was opened by the *Working Party on Information Exchange and Data Protection* (hereinafter, DAPIX), [40] a preparatory body that, through the contribution of groups of experts,[41] started to evaluate the possibility of enhancing the so-called Next generation Prüm, keeping into consideration the necessity to guarantee the protection of personal data, as established in the GDPR and the Directive 2016/680.

The debate regarding possible modifications has moved along three different directions: a) innovate provisions governing data circulation and exchange in order to improve efficiency and effectiveness of the system; b) enhance the coordination between the Prüm system and other cooperation mechanisms for investigation and crime-fighting purposes; c) expand the categories of data included into the Prüm exchange mechanism.

A first important document about the potential developments of the Prüm mechanism is represented by the study conducted by Deloitte, upon request of the European Commission, concerning *the feasibility of improving information exchange under the Prüm Decision*, released in May 2020. In that document existing difficulties of the current system and possible feasible solutions have been considered with the goal of maximising efficacy of data circulation considering also the positive drive for new and more sophisticated technologies.

[39] The so-called European Agenda on Security that defines the agenda, goals and priorities in this field, (COM(2015) 185 final. Strasbourg, 28.4.2015).

[40] The Council of the EU's official website explains that DAPIX "handles work relating to the implementation of legislation and policies on the information exchange and protection of personal data in the field of law enforcement. It also closely cooperates with Europol, especially regarding the Information Management Strategy (IMS) on streamlining cross-border information exchange. With respect to information exchange the working party is responsible for improving information exchange between law enforcement authorities of member states. With respect to data protection the working focuses on ensuring data exchange in compliance with current principles and rules on personal data protection", https://www.consilium.europa.eu/it/council-eu/preparatory-bodies/working-party-information-exchange-data-protection/.

[41] Four focus groups have been established, dedicated (respectively) to the evaluation of possible changes and improvements related to the exchange of: genetic data, fingerprints, data of vehicles' registration and finally – a relevant novelty – biometric data related to facial images deployed in systems of facial recognition. The four groups have been established with the aim of "setting out how to further develop the current information exchange mechanisms and to support the Commission's feasibility study on improving information exchange under the Prüm Decisions. The three groups focused on the existing data types already exchanged, whereas facial recognition was the subject of a fourth group established by the Council (Document 13356/19, 30 October 2019, not publicly available", Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament, *Police information exchange*, cit., 25.

ISSN 2284-4503

Moving from the first of the mentioned areas, the envisaged solution is the introduction of new provisions on data exchange at EU level so as to make sharing and automated exchange easier and more efficient, in particular in the second phase of the *Prüm* mechanism, namely the step following the match between the data requested by a Member State and the one contained in the national database of another Country. As explained before, only in that case is the personal data of the subject linked to that genetic profile are actually shared. In such a delicate phase, different standards and procedures (e.g. some Member states require the intervention of a judicial authorities to authorise the submission of the data, while other prescribe supplementary controls) can ultimately represent an obstacle to the proper and efficient functioning of the exchange system.

For these reasons, enhancing automatic methods of communication of personal data may constitute a possible solution, in particular with regard to the exchange of fingerprints, considering the limited risk of false positive cases. The creation of a *central router*[42] goes in the same direction, aiming at receiving and sending all the requests coming from Member States' competent authorities with automated procedures: in this way the existing limits and problems related to the bilateral procedures of request and matching between two Member States could be overcome.[43]

Similarly, the EU institutions are now evaluating the possibility to modernize the existing Prüm system and to connect it with other cooperation or shared information systems among national law enforcement authorities: for example, cooperation with the European Search Portal (ESP)[44] or the

[42] On this point it is interesting to notice that this solution has been considered more appropriate than the creation of a "centralised information system, which has been rejected due to legal constraints on storing such data outside the national territory, for various reasons; processing personal data at EU level will be avoided; accurate statistical data at central level will be produced and technical difficulties posed by bilateral connections will be eliminated", Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament, *Police information exchange*, cit., 9.

[43] Another issue that has been underlined in this study is the inclusion, among the possibilities to activate and exploit the Prüm mechanism, of the purpose of searching missing persons: "new purposes will have to be added to the revised Prüm legal framework, so that searches with the aim of locating missing persons and identifying human bodies/remains could take place, even if no direct link to a criminal investigation exists". This obviously implies the necessity to define specific rules governing the guarantees for missing persons with regard to data protection "the fact that missing persons may include vulnerable groups of individuals, such as elderly persons, persons with mental health issues or children, should be taken into account. As a result, concerns are raised about the handling of data concerning missing persons in the same systems that process information on convicted criminals. Therefore, additional safeguards are required in relation to the retention of such data on missing persons", Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament, *Police information exchange*, cit., 27. Therefore it is evident that the political and legal debate on the issue is particularly delicate: the importance of guaranteeing a high level of protection of privacy and data protection rights (especially when referring to special categories of data like biometric and genetic data) along with the modernization and improvement of the Prüm system must be kept in mind.

[44] The European search portal has been established by art. 6 of Regulation (UE) n. 2019/817 of 20th May 2019 that establishes a framework for interoperability between EU information systems in the field of borders and visa. The portal aims at facilitating "the fast, seamless, efficient, systematic and controlled access of Member State authorities and Union agencies to the EU information systems, to Europol data and to the Interpol databases for the performance of their tasks and in accordance with their access rights and the objectives and purposes of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN" (art. 6). As it can be read in the considering n. 10, "Interoperability between the EU information systems should allow those systems to supplement each other in order to facilitate the correct identification of persons, including unknown persons who are unable to identify

possibility for Europol and Interpol to have access to data exchanged among Member States or Third Countries according to the Prüm mechanism.[45]

Beside these innovations, a last area of intervention that should be carefully considered and evaluated is represented by the expansion of the data categories covered by the Prüm exchange mechanism, considering the huge impact that this decision could cause on the rights to privacy and data protection.

The study developed by the Commission has in fact taken into consideration the feasibility and utility of including, together with DNA, dactyloscopic data and data concerning vehicles registration, also facial images[46] – another biometric data alongside fingerprints – which represent the basis of advanced artificial intelligence technologies and cutting-edge systems of facial recognition.

Although these matters fall outside the scope of this paper, it is nonetheless essential to consider how the inclusion of these kind of data, particularly discussed among scholars[47] for their potential discriminatory outcome (also due to potential malfunctioning of algorithmic systems or possible still unexplored technical problems),[48] may result in a "*oversouveillance society*",[49] with significant

---

themselves or unidentified human remains, contribute to combating identity fraud, improve and harmonise the data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of EU information systems, strengthen the data security and data protection safeguards that govern the respective EU information systems, streamline access for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences".

[45] A specific and complex question relates to the particular relationship with the UK: within the delays of the troubled Brexit process, specific agreements defining conditions, tools and procedures for data circulation – also comprised in the Prüm mechanism – have still to be concluded. This complex subject is intertwined with the provisions of the GDPR related to data sharing with Third Countries (status that will be acquired by the UK at the end of the Brexit process), which provide specific regulation and determine high standards and conditions to ensure that the data transfer is carried out according to a high level of data protection, even outside EU borders.

[46] "Given the maturity of the technology and its capability within the context of forensic law enforcement, recommends that the exchange of facial images be adopted in next Generation Prüm", Report conducted by Deloitte upon request of the European Commission (DELOITTE, *Study on the feasibility of improving information exchange under the Prüm Decisions*, 2020, 18).

[47] On this point see the considerations of the European Data Protection Supervisor in W. WIEWIOROWSK, *Ai and Facial Recognition: challenges and opportunities*, 21 February 2020, available at https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en. See also B. BUCKLEY, M. HUNTER, *Say cheese! Privacy and facial recognition*, in *Computer Law and Security Review*, 6, 2011; C. POPE, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, in *Journal of Law and Policy*, 2, 2018; R. KRISHAN, E. MOSTAFAVI, *Biometric technology: security and privacy concerns*, in *Journal of Internet Law*, July 2018.

[48] "The degree of accuracy in facial recognition technology is vital, so as to minimize the risk of false positive matches, namely results that may be unrelated to the investigation, or false negative results, when the facial recognition algorithm fails to identify correct matches. This is crucial since facial recognition technology will be used in the course of criminal investigations with the aim of identifying unknown perpetrators, therefore national authorities will perform searches on the basis of a facial image (a mug shot or a probe retrieved from a camera) against the full content of other national databases and the top results will be ranked. False positive matches in particular may have important consequences for individuals, who may be bothered by the police because of incorrect matching, be subject to criminal investigation and even be subject to discriminatory practices by national authorities", Policy Department For Citizens' Rights And Constitutional Affairs Of The

impacts on privacy and data protection of European citizens. The risk is to create a system of even more pervasive surveillance, along with a widespread genetic screening linked to the growing expansion of genetic databases.

All these considerations allow us to clearly understand how delicate the political and legal debate is around the expansion and modernisation of the existent Prüm system.

It becomes thus evident that it is necessary to deeply reflect, within the implementation of this new and important mechanism, on the implications and consequences on privacy and data protection rights, as well as on the principles of necessity and proportionality, that are meant to guide the processing of personal data, with particular attention to the so-called special categories of data, such as the genetic or biometric.[50]

The next steps towards the definition of new data exchange strategies should give a proper answer to the concerns and still open questions that characterize the extension of the Prüm mechanism.

Notwithstanding the direction that the reform of the Prüm mechanism will take in the coming years, the discussion around its modernisation shows the importance and the efficacy of the existing European data exchange system and at the same time reveals the inclination of the system itself to become what Wienroth has described as an *aspirational regime.* According to the author, "this regime provides context to the development and application of forensic genetic innovations by materially and discursively rationalizing and operationalizing research and technology uses at the transnational level. They are "aspirational" since their rationales and objectives are future-oriented: to develop technologies and techno-legal systems that can solve or prevent crimes, produce state security and public safety".[51]

Using this effective expression and extending its scope to all data collection and exchange systems of data, Toom and other authors affirmed that the *Next generation Prüm* project, while representing the evolutionary nature of such an exchange system, will also inevitably require "further investments in material infrastructures, including software packages, laboratory facilities, paperwork and (legal) rules and standards".[52]

In explaining such issues, it becomes clear that technological innovations and scientific progress in the data sharing field find a limit in their concrete implementation, which requires a huge effort by European and national legislators as well as law enforcement authorities.

European Parliament, *Police information exchange. The future developments regarding Prüm and the API Directive (Study requested by the LIBE Committee)*, September 2020, 19.

[49] The risk of an *oversurveillance society* through the use of genetic database has already been stressed by various authors, among which: P.E. TRACY, V. MORGAN, *Big Brother and His Science Kit: DNA Databases for 21st Century Crime Control?*, in *Journal of Criminal Law & Criminology*, 2, 2008, 635-690; R.E. RODRIGUES, *Big Bio-Brother is Here: Wanting, Taking and Keeping you DNA*, in *British & Irish Law, Educ. & Tech. Ass'n*, Vol. 2, 2007. Today the issue may become even more complex, following the potential implications deriving from the use of facial recognition systems.

[50] For a broader analysis on the provisions concerning these data within the GDPR framework, see R. DUCATO, *I dati biometrici*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

[51] M. WIENROTH, *Socio-technical disagreements as ethical fora*, in *BioSocieties*, 15, 2018, 1-18.

[52] V. TOOM, R. GRANJA, A. LUDWIG, *The Prüm Decisions as an aspirational regime: reviewing a decade of cross-border exchange and comparison of forensic DNA data*, in *Forensic science international: genetics*, 41, 2019, 54.

In the past, these challenges have already been able to restrain the expansion and effectiveness of the Prüm system, which faced delays in the development of databases and difficulties in the implementation of adequate and clear legislations, that were capable on the one hand to design solutions that guaranteed security and on the other hand could protect fundamental rights enshrined in the Nice Charter and in national Constitutions.

The legislator must find a proper equilibrium between the drive to exploit the potentialities of new technologies and the great quantities of data and, at the same time, respect fundamental rights which are today strongly safeguarded at European level, also through the case-law of the Luxembourg judges.[53]

[53] See for example on this subject the well-known case law of the CJEU on data retention for security purposes, starting with the judgment in Digital Rights Ireland (joined cases C-293/12 and C-594/12 of 8 April 2014) on the balance between the efficiency of the fight against serious crimes and the protection of privacy and data protection rights by the Luxembourg courts in this complex line of jurisprudence, ex multis O. POLLICINO, M. BASSINI, *La Corte di giustizia e una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto penale contemporaneo*, 9 gennaio 2017; E. CELESTE, *The CJEU and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019. The EDU Court too has given a wide ruling on the massive monitoring and protection of fundamental rights, with relevant decisions, including recent ones, such as Centrum for Rattvisa c. Sweden and Big Brother Watch c. United Kingdom, currently referred to the Grand Chamber. See on this regards G. FORMICI, *La digital mass surveillance al vaglio della Corte Europea dei Diritti dell'Uomo: da Zakharov a Big Brother Watch*, in *Federalismi.it*, 23, 2020.