Journal of Forensic and Legal Medicine 66 (2019) 155–161

Contents lists available at ScienceDirect

Journal of Forensic and Legal Medicine

journal homepage: www.elsevier.com/locate/yjflm

Privacy and data protection in the surveillance society: The case of the Prüm system

Sara Matos

Communication and Society Research Centre (CECS), University of Minho, Campus de Gualtar, 4710-057, Braga, Portugal

ARTICLE INFO

Keywords:
Privacy
Data protection
Criminality
Surveillance
Sociotechnical imaginaries

ABSTRACT

The simultaneous localisation and globalisation of 'terrorist threats' and cross-border criminality have led to increased expansion of surveillance activities and greater cross-border police and judicial cooperation, placing a greater priority on these activities within the political agenda of the EU. In this scenario, the expansion of technological systems for surveillance and monitoring, and the large-scale exchange of citizens' personal data play a pivotal role in the "fight against crime". This paper explores the multiplicity of data protection regimes in different EU Member States within the framework of the Prüm system. While EU regulations establish minimum standards for personal data flows at the transnational level, local and domestic practices are extremely heterogeneous.

Based on analysis of 37 interviews conducted with professionals involved in the automated exchange of forensic genetic profiles, this paper provides empirical data that highlights the tensions between the local and the global within DNA data exchanges across the EU. These tensions relate to differentiated sociotechnical imaginaries regarding the protection of personal data flowing between Member-States. In sum, this paper analyses the potential threats to human rights created by the exchange of personal data with regards to issues of privacy and data protection.

1. Introduction: the European landscape

The Schengen Agreement[1] was signed on June 14, 1985, aiming to abolish all internal borders within the European Union, leaving just an external border. The Schengen area represents a territory that guarantees the free movement of persons. However, facilitated mobility of persons has posed several challenges to the European Union, in particular, those related to security concerns at the transnational level. For example, security-related issues came to the fore as a result of terrorist attacks in several European cities.[2] The scenario of increasing mobility of citizens in the European area, combined with various threats to European Union security, has culminated in the expansion of surveillance systems and greater cross-border police and judicial cooperation.

Given the context of insecurity experienced by the European Union, the implementation of networks of sophisticated technological systems for identification and control of "suspect populations" have benefited from renewed legitimacy in the public arena.[1–3] The following examples are representative of these large IT systems. The European Asylum Dactyloscopy Database (EURODAC)[3] was created in 2003 with the aim of examining asylum applications by comparing fingerprint datasets. The Visa Information System[4] (VIS), in operation since 2011, aims to share data about visas between Member-States in the Schengen area. The Prüm Decisions (Council Decision 2008/615/JHA[5] and Council Decision 2008/616/JHA[6]) aim to foster the exchange of information related to genetic data (DNA profiles), fingerprints and vehicle registration in order to combat terrorism and cross-border crime.

The adoption of various systems of surveillance has stimulated discussion about the balance between the proportionality of surveillance activities and the need to protect citizens' fundamental rights. Some European Institutions, such as the European Agency for

E-mail address: saramatos@ics.uminho.pt.

[1] Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33020&from=PT, February 7, 2019.
[2] Madrid (2004), London (2005), Paris (2015), Brussels (2016).
[3] Retrieved from https://ec.europa.eu/knowledge4policy/dataset/ds00008_en, February 7, 2019.
[4] Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en, February 7, 2019.
[5] Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615, February 7, 2019.
[6] Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF, February 7, 2019.

https://doi.org/10.1016/j.jflm.2019.07.001
Received 15 April 2019; Received in revised form 4 July 2019; Accepted 8 July 2019
Available online 10 July 2019
1752-928X/ © 2019 Published by Elsevier Ltd.

Fundamental Rights (FRA),[7] have attempted to achieve a balance through analysis of the pros and cons of different surveillance mechanisms/technologies. The report "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU",[8] produced in 2017 by the FRA, documents an attempt to balance individual rights and collective safety. In brief, the FRA explored the challenges that new surveillance technologies pose to the fundamental rights of European citizens. The report emphasised the importance of surveillance for the security of Member States but also mentioned that this practice could be harmful to several fundamental rights, specifically privacy and data protection. In addition, disproportionate surveillance could also pose risks to democracy and citizenship due to transparency issues. The aforementioned document was requested by the European Parliament in 2013 following the widely publicised case of Edward Snowden. He was a US government employee working for the country's intelligence services (NSA), who until then had been anonymous.[4,5] Snowden's revelations brought into the public sphere the massive and disproportionate surveillance of ordinary citizens and leaders within the European Union and the USA.[4,6] These revelations created a space to reflect upon surveillance practices operated at a dimension that was not envisioned by US citizens, nor by the European Union. The revelations had two main consequences. First, European countries' trust in the US came into question. Second, the revelations weakened European citizens' trust in their own security agencies.[4]

Looking specifically at efforts to reduce crime, the opening of the European Union's internal borders led to the adoption of several security strategies. One of these strategies was the implementation of forensic DNA databases and, later, the transnational exchange of the genetic information stored on these databases for criminal investigation purposes.[7–11] The creation of forensic DNA databases sometimes led to debates on ethical, social and political challenges, particularly in terms of privacy and data protection. Some authors argued that expansion of these databases was allied to an increase in control and surveillance over individuals and would result in the criminalisation and vulnerability of certain populations,[12–15] and consequently, would increase their stigmatisation.[16–19] This article intends to be a reflection on the sociotechnical imaginaries[20] of data protection performed in this context of transnational cooperation and more expansive surveillance.

The paper will cover the most representative topics about privacy and data protection in the Prüm system that were shared by the interviewees. First, participants found that the judicial system is more effective in protecting personal data, but exchanging data via this method is generally slower (this is one of the biggest criticisms of the Prüm system). Second, the decision to exchange personal data (step 2) varies between Member-States. Some countries choose to exchange information about a suspect regardless of the crime, but other countries only exchange information in certain situations. This relates to the relevance of sending personal data to third countries for crimes that, according to NCPs, may not be sufficiently serious to justify the exchange. In this way, countries that only share information when relating to serious crimes, have a narrower conception of the data that they must protect. The third topic brought up by some interviewees had to do with the need for trust between Member-States within the Prüm system. For the Member-States, it is imperative that countries trust that the personal data that they are going to send will be treated in accordance with good privacy and data protection practices. The participants considered that if there is a lack of trust, transnational cooperation may be more limited and, as such, may not achieve its full potential. On the last topic, the interviewees expressed their opinion on the expansive or restrictive approach of data exchange in their countries.

2. The Prüm system

The transnational exchange of information from national DNA databases for criminal intelligence purposes is operated through the so-called Prüm Treaty.[21,22] It was originally signed in 2005 by seven Member States of the European Union - Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain - and later by Finland, Italy and Portugal. The Treaty was later transposed into European Union law, in 2008.[9] This decision made it compulsory for all Member-States to set up and maintain databases for the mutual access and exchange of DNA profiles, fingerprints and vehicle registration data. For the purposes of this article, only the exchange of information related to DNA profiles will be considered. The Treaty aimed to foster technical and scientific standardisation, and also legislative harmonisation, in order to guarantee the protection of the right to privacy. In this way, the sociodemographic information of an individual is dissociated from his or her genetic profile when a country searches the DNA database of another country.

The correspondence between DNA profiles in the Prüm system is achieved using a two-step approach.[7,10,23] In step 1, Member States confirm whether or not the DNA profile of their database matches the profile that exists in another Member State's database. After a hit/match confirmation, this will trigger step 2 if requested, i.e. the exchange of further information about the DNA's owner. The information exchange is performed in accordance with the data protection law of both countries[24] as well as the minimum criteria established by the European Commission for data protection. The two-step process allows for evaluation of national legislation, in order to check whether the exchange falls within legal parameters, and confirm whether or not the data protection measures are in force with respect to the exchange of personal data[7(p316)].

The Prüm system, as a technical-scientific standardisation element, was intended to facilitate transnational cooperation between police and judicial institutions, by neutralising legal, cultural and political differences in the different Member States[10,11,25(pp4−5)]. The flow of information is closely dependent on the creation of standards that seek to ensure interoperability[9,17,26–28] between national forensic DNA databases. However, technological and scientific harmonisation has as its main challenge the legislative diversity of the countries of the European Union.[11,24] Even with the two-step approach established by the Prüm System, there are different sociotechnical imaginaries[20] about the personal information data that should be exchanged between Member-States. These divergences show that European countries have different ways of conceiving the notions of privacy and data protection of their citizens.

The legitimation of this particular system of genetic surveillance follows the same line of argument used to justify other technological surveillance mechanisms. Generally speaking, political narratives reflect the idea that there is a need to balance individual rights (privacy and data protection) and collective safety in order to 'fight' terrorism and organised crime.[26] Nevertheless, one of the criticisms of the Prüm system concerns its transnational scope. According to several authors, it is important that the Prüm system also covers the processing of personal information conducted in national contexts.[29] That said, National Contact Points have different 'epistemic cultures'[30] relating to privacy and data protection, while operating without a transnational policy capable of accommodating different national practices when balancing security and the protection of fundamental human rights.

[7] European Agency for Fundamental Rights (FRA) - http://fra.europa.eu/en.

[8] Retrieved from http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega, January 24, 2019.

[9] Council Decision 2008/615/JHA and 2008/616/JHA – Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0005 & https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528203232723&uri=CELEX:32008D0616, January 24, 2019.

3. Prüm system: sociotechnical imaginaries

Science and Technology Studies scholars have critically analysed and explored the implementation and subsequent expansion of forensic DNA databases for criminal investigation purposes.[31–35] The present article uses the conceptual framework of STS and focuses on the concept of sociotechnical imaginaries.[20] This concept allows us to understand the reception of science and technology by non-scientific actors and institutions[20(p119)]. Jasanoff and Kim describe sociotechnical imaginaries as "collectively imagined forms of social life and social order reflected in the design and fulfilment of nation-specific scientific and/or technological projects"[20(p120)]. With this concept, the authors moved away from the classic notion of imagination as fantasy or illusion.[36] On the contrary, imagination, as a cultural resource, allows the projection of goals and objectives that, in turn, guide the social actors to new ways of life. In this sense, Jasanoff and Kim (2009) argue that "imagination helps [to] produce systems of meaning that enables collective interpretations of social reality"[20(p122)]. The notion of sociotechnical imaginaries thus allows us to understand the conceptions of social order and priorities, in order to reduce risks. In my study, I argue that the sociotechnical imaginaries can guide the production of laws and/or norms to one direction regarding the transnational exchange of information from DNA profiles.

Science and technology with direct application to the objectives of modern nation-states, such as ensuring security, have been secured by policies that aim to ensure continual development. The establishment of forensic DNA databases and the transnational exchange of DNA data could be assumed to be one example. The political promotion of science and technology has two important dimensions. Firstly, we find "national visions of desirable futures driven by science and technology"[20(p121)]. This idea is shaped through national imaginaries related to the transnational exchange of forensic data as a way of solving crimes not only at a national level but also at an international one. Secondly, there are "fears of either not realising those futures or causing unintended harm in the pursuit of technological advances"[20(p121)].

Terrorist threats and criminality have put pressure on States to improve the protection and security of their citizens. The interpretations of these risks by States are usually accompanied by ideals of expansive surveillance of individuals. Under this scenario, the appropriation of DNA technologies by governments aims to mitigate the risk of crime/terrorism/illegal migration. The Prüm system could be considered to be the materialisation of the appropriation of DNA science by political and/or police institutions which are constituted by actors - such as the Prüm National Contact Points (hereafter NCPs) - for use in their surveillance assemblages. Even recognising the advantages of information exchange for criminal investigation purposes, States have concerns about potential moral threats to their citizens, threats such as the potential misuse of forensic data or inaccurate information. Such threats have led EU Member States to create different policies specifying the criteria for DNA data exchange via the Prüm system. That said, exploring the NCPs narratives makes it possible to map national sociotechnical imaginaries about the Prüm system, as well as its potential threats to civil liberties.

4. Methodology

This article is based on a broader project[10] that explores the societal, cultural, ethical, regulatory and political impacts of the use of forensic DNA technologies in the European Union. The paper is anchored in a qualitative methodology in order to capture the multidimensionality of this object of study and to privilege the socially constructed perspectives of the different social actors that are related to the empirical subject. The conditionality of only being able to subtract pre-existing sensitizing concepts[37(p34)] and not theoretical frameworks and general working hypotheses, implies adopting research strategies that make it possible to associate the construction of hypotheses and the elaboration of theoretical concepts to the specific circumstances of locally situated empirical reality. This research is guided by a systematic comparison between analysis, empiricism and theory[38] following some assumptions of grounded theory.[38] This study thus values the sociological representativeness of each case, and these seem to be generalizable to theoretical statements and not to populations or universes[39(p10)],[40(p248)].

Interviews were conducted with professionals involved in international police cooperation who have acted as Prüm National Contact Points or were directly involved in the process of joining the Prüm system. NCPs are central actors in the Prüm system. Generally, they are responsible for conducting daily activities that allow the transnational exchange of personal data and occupy a crucial position in decision-making processes. In particular, NCPs are responsible for: organizing and implementing the connections necessary to perform the automatic data exchange with other databases (sending and receiving information), testing the exchange with other partner countries, and managing/reporting DNA matches. Nevertheless, the NCPs responsibilities may vary between countries according to different organizational structures and national legislation. Therefore, individuals operating as NCPs may have differentiated professional and educational backgrounds and may work in forensic laboratories as well as in police forces.

The interviews were conducted under the protocols and procedures of the European Research Council's ethics regulations. The participants were identified first from the public contact list provided by the 'Working Party on Information Exchange and Data Protection' documents,[41] and then by contacting privileged informants in the area. The participants were recruited by email, letter and telephone calls. Prior to the interviews, all interviewees signed a written informed consent form and agreed to be audio recorded. The data on which the analysis is based includes 37 semi-structured interviews conducted in 22 EU member states with 47 professionals operating in the Prüm system. The interviews took place at the participants' workplaces or a location of their choice and they had an average duration of 90 min. All interviews were digitally recorded, transcribed verbatim and anonymised. Editing of the quotes was carried out whenever necessary to assure clarity of language, while fully respecting the meaning manifested by the participants' words.[42] To protect the anonymity of the interviewees, the country in which each interviewee was based was identified using a letter and a number was attributed to each participant. This form of anonymisation will be used in the interview quotes analysed in the following sections.

The interviews included the collection of the following information: views and experience with the implementation of Prüm at the levels of Member States and the EU as a whole, opinions about the Prüm' purpose and contribution, ethical issues raised by the transnational exchange of DNA data, expectations about DNA technology development and innovation, and perceptions related to communication with the public. For the present article, we analyse the interviewees' perspectives related to ethical issues that refer to notions of privacy and data protection in the Prüm system.

Relevant quotes revealing the participants' narratives about the relevance of the procedures adopted for the exchange of personal data through the Prüm system were coded and subjected to multiple readings, in order to develop an in-depth understanding of the sociotechnical imaginaries regarding privacy and data protection articulated by the N CPs. These quotes were systematically compared, contrasted, synthesised and coded by theme and thematic category using the principles of grounded theory[43] and interpreted using a qualitative content analysis approach.[44] In this paper, I analyse the replies that were considered by the authors as illustrative of each thematic category that emerged from the content analysis.

[10] Exchange project (http://exchange.ics.uminho.pt/).

5. National Contact Points: views on the databases custody and follow-up procedures

The Prüm System attempts to create minimum standards for data protection in a forensic context using the two-step approach.[10] At the national level, the institution that has custody of the national forensic DNA database is also responsible for different socio-technical imaginaries concerning privacy and data protection. National forensic DNA databases may be under the jurisdiction of the Ministry of Justice or the Ministry of Internal Affairs and the custodian can influence the flow and fluidity of communication between the authorities of different Member-States.

5.1. Judicial process vs police process - time-consuming vs quickness

Interviewees emphasised that the models of cooperation are dependent on the custody of the respective country's database,[45] wherein the procedures involving the exchange of DNA information via the judicial authorities are slower than exchange via police institutions.[45] The following extract clearly indicates this contrast, in terms of the tardiness of procedures, characteristic of judicial authorities, which, according to the interviewee, contributes to the inefficiency of cooperation in step 2 of the Prüm system:

> In my country DNA is not police information. So, now what happens [is that] if another country would like to have more information about a person, they have to send a rogatory commission to my country. It's very complicated, because, [if] it's in the police department, [they] phone and [asks] 'Could you give me the name?' and it's done. (Interview I01)

Different practices of transnational cooperation between the police and judicial authorities may thus present an obstacle to the exchange of information for criminal investigation purposes.[45] Police institutions operate on the principle of the maximum degree of access to available information with the aim of advancing a criminal investigation (*intelligence*).[46] On the other hand, the mode of action of judicial authorities is seen to be more restrictive because it is a slower process and, usually, results in less exchange of information.[45] The scarce experience on transnational cooperation attributed to the judicial authorities by the police forces is, according to interviewees from the police forces, one of the obstacles for the fluidity of the communication.[45] This happens partly because the judicial authorities are not involved in the investigative phase. Therefore, the *rationale* and *modus operandi* of the two institutions are different due to their different objectives in the criminal justice system. Police forces searches for people who have committed crimes. Judiciary systems other judges those who have (or haven't) committed such crimes. As Machado and Granja (2019) stated:

"The clash between these different working methods (…) therefore undermines the principle of reciprocity and trust that police professionals claim is needed within transnational cooperation and prevents the construction of relationships based on trust with their judicial counterparts."[45(p14)]The differences between Member-States in terms of the custody of forensic DNA databases reveals different imaginaries of privacy and data protection as well as tensions in transnational cooperation between police and judicial institutions. The first extract was explicit about the difficulty in obtaining information from judicial authorities. The following excerpts contain illustrative participants' views of cooperation. The first participant refers to the bureaucracy that is required to request information in the judicial sphere. The second interviewee identifies the frustration that can arise from failure to exchange information. Both excerpts express critical views about the functioning of judicial institutions in relation to transnational cooperation, namely, that it requires too much work to obtain information, and frustration because of the refusal to grant information:

> They send us the name of the guy, they send very few information: name, the offence … Not automatically. So, we have a name, but if we want to have more than that, we need to send another request. Judicial request. (Interview H02)

> I would say, sometimes it leads to more frustration. I mean, [Country A] is so pissed at [Country B] right now. They have the identity of a murderer, but they are refusing to give [Country A] the information because they are under the Ministry of the Interior. (Interview U01)

5.2. Follow-up criteria for the exchange of information

The sociotechnical imaginaries related to data protection and privacy can also be found in the criteria decided by Member-States for the follow-up of DNA hits/matches. As is outlined in the participants' narratives, the criteria for following-up DNA hits differ between countries. In the following excerpts, interviewees explain that there are countries that only exchange information in specific situations, for instance, of the crime typology and seriousness in terms of the penal framework. Some countries opt not to exchange information if they consider the crime does not justify the sending of private information about someone in their database. In this situation, the information held by a Member-State is protected regardless of whether or not it may help solve a case in a third country.

> If you have a minor case, most of the time people don't make any follow-up. (Interview H02)

> So even if there is a hit, there is [still] also the option that the local police unit decides not to start a case, because maybe it's a too old case (…) and maybe the prosecutor [already] closed the case and there is nothing to do. So, they have information from the laboratory that there is a hit, but nobody will send us a request to make a further inquiry in the Second step. (Interview G06)

5.3. Trust between Member-States in transnational cooperation

There was one topic that was emphasised by participants, namely, the trust between Member-States. The lack of trust that could characterize countries relationships is one of the obstacles to the implementation of the exchange of personal data in the Prüm system.[47(pp2−3)], [48] The different custodians of databases have placed a strain on trust relations between countries. Historically, police cooperation is permeated by informal information-exchange networks, which do not require the presence of political negotiations between countries.[7] Judicial cooperation is characterized by a more formal and politicized character, which is often dependent on interpersonal relations of trust between people from different countries.[7] The formalization of the Prüm system has merged the traditional dynamics of data exchange by allowing judicial entities to exchange data with law enforcement agencies and *vice versa*.[49] That said, step 2 give countries some manoeuvre to decide which data should be exchanged. In that sense, some countries opted to legally formalize these dispositions while in other nations decisions over the type of data exchanged are under the responsibility of the NCP.[7]

As the following quote demonstrates, the interviewee is in favour of forcing countries to carry out step 2 of the Prüm system. The participant argued that the police and judicial cooperation should be based on trust and solidarity between EU Member-States.[9,50]

> Now we have to force people to do a step 2 application. (…) Do not ask what ministry they are from, we are cooperating within Europe, if they ask a Prüm question and they are fully agreeable, then you get the information. I have information, of course I want to help the other countries. If you just filled in the paperwork correctly, we trust you. (Interview U01)

The interviewee's narratives showed that different options for the databases custody and the follow-up procedures for step 2 of the Prüm can conditionate the transnational exchange of genetic information. On the one hand, the Member-States with judicial custody of the database tends to negatively constraint the fluidity of the information. On the other hand, countries with database custody under the Ministry of Internal Affairs are more willingly to exchange DNA profiles data. Also, the follow-up procedures explained by the participants allow the identification of the different sociotechnical imaginaries regarding privacy and data protection. As one interviewee said, in minor cases, some countries opt for not exchange the information of its own citizen. The option of do not proceed with step 2 of the Prüm system can be seen as a measure of privacy protection. Also, through the participants' narratives, this section highlighted some tensions on transnational co-operation between the Member-States regarding their governance modes of the second step of the Prüm system.

6. National Contact Points: views on restrictive and expansive modes of forensic data exchange

Another relevant aspect of data protection and privacy imaginaries in the context of transnational exchange is related to the restrictions placed upon the use of the data that is sent. The categorization that will be presented in this section is inspired by the work of Santos, Machado and Silva.[51] The authors use the categories of "restrictive countries" and "expansive countries" to classify the insertion criteria of individuals into national forensic DNA databases. On the one hand, the restrictive countries instead of inserting all population that passed in the criminal system, usually opt for a set of conditions that will determine or not the insertion of the DNA profile on the database. Santos, Machado and Silva classify the following countries as the restrictive ones: Belgium, France, Germany, Hungary, Ireland, Italy, Luxemburg, the Netherlands, Poland, Portugal, Romania, Spain and Sweden. On the other hand, there are the expansive countries that, generally, are much more inclusive in terms of the rules to the insertion of DNA profiles on the database[51(p6)]. In this group are the following countries: Austria, Denmark, Estonia, Finland, Latvia, Lithuania, Scotland Slovakia and the United Kingdom. In this paper, I propose to expand their categorization to the type and amount of information that is exchanged between the Member-States that are in the Prüm system. That said, several Member-States choose to specify on the document sent to the requesting State that the submitted data cannot be used in their courts as such. They thereby limit their use to the investigative stage of the criminal process. However, this option generates different perspectives on the reciprocity implicit in international cooperation,[52] and in particular in the Prüm system, as well as the practice of the analysis of DNA profiles. In the following quote, is illustrated the statement that is added to the document before exchanging data, which means that for further information the requesting country should send an international letter rogatory. This procedure could, again, slow the process of transnational cooperation and also reveals the lack of trust concerning the protection of the data by third countries.

> The following statement is always included: 'The above information including the personal data related to the mentioned individuals may be released for the operational internal police use only and cannot be used as an evidence in your respective countries. In order to acquire evidence which can be used in legal proceedings, your authorities should apply to the competent authorities via an international letter rogatory.' (Interview G06)

The two-step approach aims to place more safeguards on transnational data exchange.[10] However, there are different modes of conceiving what personal information about their own citizens should be exchanged between Member-States. The different socio-technical imaginaries regarding privacy and data protection are expressed in the following extracts in which the interviewees explained the national modalities about the personal data that is exchanged for criminal investigation purposes. On the one hand, there are countries that decided to have an expansive[51] approach to exchanging personal information. In the following quote, the interviewee referred to his/her country's expansive exchange of data to third countries:

> It is of course a question of how easily countries give up those persons, give up their information. If the country does not protect their people, it is a problem. I am not proud to say it, but our government does not protect our people very well. So, they give them up quite easily. Once they get these Prüm matches they are given up. I think it might not be only our country's problem. (Interview B01)

On the other hand, there are Member-States that take greater consideration of the kind and amount of personal information that is exchanged in transnational cooperation, so-called 'restrictive' countries.[51] In the following extract, the participant explains that in his/her country they do not exchange all the personal information that they keep. In that national context the authorities opt for the selection of information and only send to third countries the data that is considered to be strictly necessary:

> We don't want to send everything. We want to select the more efficient information, waiting for the country to send us an additional request. Otherwise, if we need to have some coercion to get the information, that will be dealt with by the judicial channel. (Interview H02)

The differences between restrictive and expansive countries are mainly related to the type and quantity of information exchanged via the Prüm system. It is important to emphasise that the categories of restrictive and expansive approaches to cooperation are not rigid. The flow of personal information for criminal investigation purposes may vary according to the Member-States that are involved in the data exchange. For instance, one country may choose to exchange more or less information about a person in function of the requesting country, precisely because of different levels of trust between Member-States. Generally, on the one hand, the Member-States that have attributed the custody of the national forensic DNA database to policial authorities are characterized for a more expansive mode of information exchange.[45] On the other hand, the restrictive way of data exchange between countries is associated with Member-States whose custody is under the judicial entities.[45] That said, the majority of the countries in the Prüm system have their national DNA database under the Ministry of the Interior (or Internal Affairs or Home Affairs). Only Belgium, Portugal, the Netherlands and Sweden have their national DNA database under the Ministry of Justice. However, it is important to emphasize that the listed categories are flexible. Nevertheless, a country can decide for policial custody of the national DNA database and still have a restrictive mode of transnational information exchange.

7. Conclusion

The sociotechnical imaginaries about privacy and data protection have shaped the trajectories of implementation of the Prüm system, as well as the processes put in place and the application of policies regarding the exchange of data. At the same time, these policies have simultaneously reinforced the specific imaginary of the risks and benefits of the Prüm system. Scientific and technological practices comprise expectations of future possibilities,[53] which will consequently shape decision-making and also the trajectories of science and technology.[20] The co-construction of scientific trajectories, such as the Prüm system, are made via understandings about the notions of the 'common good'. The formulation of policies regarding Prüm is permeable to several sociotechnical imaginaries about privacy and data protection at the national level. However, the State, in the social environment, is the figure that has more resources and more power to define the

sociotechnical imaginaries that will be adopted in a certain society.[20]

The Prüm system appeared as a response to the security concerns at a transnational level posed to the European Union by the mobility of persons in the wake of the Schengen Agreement.[11] This system aimed to harmonise procedures for transnational cooperation, but such harmonisation is limited by social, cultural, technological and political differences among Member-States. The automation and standardisation of Prüm Step 1 procedures dilute differences. Nevertheless, these reappear at the second step, due to the existence of highly heterogeneous practices at the local and global level regarding privacy and data protection in sociotechnical imaginaries. The projection of the infrastructures of the Prüm System is the result of a set of scientific, ethical, and political options: scientific - because they need to fulfil their design remit, for example, the comparison/evaluation of DNA profiles is a consolidated scientific technique; ethical - because the infrastructures equate the potential risks or errors of one technology, for instance, false positives, privacy, abuse of power, data misuse; and political - because it was originally intended as a voluntary cooperation mechanism, but the Prüm system later became mandatory for the entire European Union.

The expansion of surveillance activities, such as the operation of forensic DNA databases, demands debate, which involves the need to find a balance between the use of surveillance for international security and the guarantee of fundamental human rights.[54] It is crucial to reflect on the proportionality and intensity of surveillance systems that in some circumstances could lead to the vulnerability and the stigmatisation of certain populations and/or individuals.[12–19] Although there is a general recognition of potential threats to the security of the European Union, namely terrorist attacks and trans-border criminality, not all the interviewed professionals of the Prüm system – the NCPs – have the same sociotechnical imaginaries concerning privacy and data protection.

The research data that was explored in the paper challenge the notion of a unified European Union in terms of policial and judicial cooperation. The tensions highlighted can be the result of different national sociotechnical imaginaries regarding the privacy and data protection of the personal information of their own citizens. However, due to the lack of official reports and statistics, it is not feasible to deeply analyze some subjects, for example, regarding the type and amount of information that is exchanged between the Prüm system members.

Declaration of interest

None.

Conflict of interest statement

I declare no conflicting interests.

Acknowledgements

This work has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. [648608]), within the project “EXCHANGE – Forensic geneticists and the transnational exchange of DNA data in the EU: Engaging science with social control, citizenship and democracy” led by Helena Machado and hosted at the Communication and Society Research Centre, Institute for Social Sciences of University of Minho (Portugal). I am also immensely grateful to Dr. Carole McCartney (Northumbria University) for her comments on an earlier version of the manuscript, although any errors are my own and should not tarnish her reputation.

[11] Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:l33020, January 23, 2019.

References

1. Cole S, Lynch M. The social and legal construction of suspects. *Annu Rev Law Soc Sci.* 2006;2:39–60. https://doi.org/10.1146/annurev.lawsocsci.2.081805.110001.
2. Haggerty KD, Ericson RV. The surveillant assemblage. *Br J Sociol.* 2000;51(4):605–622. https://doi.org/10.1080/00071310020015280.
3. Maciel D, Machado H. Biovigilância e governabilidade nas sociedades da informação. In: Machado H, Moniz H, eds. *Bases de Dados Genéticos Forenses: Tecnologias de Controlo e Ordem Social. Coimbra.* Coimbra Editora; 2014:141–166.
4. Datafication Dijck J van. Dataism and dataveillance: big Data between scientific paradigm and ideology. *Surveill Soc.* 2014;12(2):197–208.
5. Wright D, Kreissl R. European responses to the Snowden revelations. In: Wright D, Kreissl R, eds. *Surveillance in Europe.* London: Routledge; 2015:6–50.
6. Wright D, Kreissl R, eds. *Surveillance in Europe.* Oxon and New York: Routledge; 2015.
7. McCartney C, Wilson T, Williams R. Transnational exchange of forensic DNA: viability, legitimacy, and acceptability. *Eur J Crim Policy Res.* 2011;17(4):305–322. https://doi.org/10.1007/s10610-011-9154-y.
8. McCartney C. Opting in and opting out: doing the hokey cokey with EU policing and judicial cooperation. *J Crim Law.* 2013;77:543–561. https://doi.org/10.1350/jcla.2013.77.6.879.
9. McCartney C. Forensic data exchange: ensuring integrity. *Aust J Forensic Sci.* 2014;47(1):36–48. https://doi.org/10.1080/00450618.2014.906654.
10. Prainsack B, Toom V. The Prum regime. Situated dis/empowerment in transnational DNA profile exchange. *Br J Criminol.* 2010;50(6):1117–1135. https://doi.org/10.1093/bjc/azq055.
11. Prainsack B, Toom V. Performing the union: the prum decision and the european dream. *Stud Hist Philos Sci C Stud Hist Philos Biol Biomed Sci.* 2013;44(1):71–79. https://doi.org/10.1016/j.shpsc.2012.09.009.
12. Chow-White P, Duster T. Do health and forensic DNA databases increase racial disparities? *PLoS Med.* 2011;8(10) https://doi.org/10.1371/journal.pmed.1001100 e1001100.
13. Duster T. The molecular reinscription of race: unanticipated issues in biotechnology and forensic science. *Patterns Prejudice.* 2006;40(4-5):427–441. https://doi.org/10.1080/00313220601020148.
14. Duster T. Selective arrests, an ever-expanding DNA forensic database, and the specter of an early-twenty-first-century equivalent of phrenology. In: Lazer D, ed. *The Technology of Justice: DNA and the Criminal Justice System.* Cambridge: MIT Press; 2004:315–334.
15. Machado H, Silva S, Amorim A. Políticas de identidade: perfil de DNA e a identidade genético-criminal. *Análise Soc.* 2010;XLV(196):537–553http://analisesocial.ics.ul.pt/documentos/1283950470C0xRF9bo4Yl23YJ7.pdf, Accessed date: 19 November 2010.
16. Aas KF. “Crimmigrant” bodies and bona fide travelers: surveillance, citizenship and global governance. *Theor Criminol.* 2011;15(3):331–346. https://doi.org/10.1177/1362480610396643.
17. Ball K, Di Domenico M, Nunan D. Big data surveillance and the body-subject. *Body Soc.* 2016;22(2):58–81. https://doi.org/10.1177/1357034X15624973.
18. Williams R, Johnson P. Circuits of surveillance. *Surveill Soc.* 2004;2(1):1–14. https://doi.org/10.1901/jaba.2004.2-1.
19. Williams R, Johnson P. “Wonderment and dread”: representations of DNA in ethical disputes about forensic DNA databases. *New Genet Soc.* 2004;23(2):205–223. https://doi.org/10.1080/1463677042000237035.
20. Jasanoff S, Kim SH. Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva.* 2009;47(2):119–146. https://doi.org/10.1007/s11024-009-9124-4.
21. Kierkegaard S. The Prum decision - an uncontrolled fishing expedition in “Big Brother” Europe. *Comput Law Secur Rep.* 2008;24(3):243–252. https://doi.org/10.1016/j.clsr.2008.03.002.
22. O'Neill M. The issue of data protection and data security in the (Pre-Lisbon) EU Third Pillar. *J Contemp Eur Res.* 2010;6(2):211–235http://www.jcer.net/index.php/jcer/article/view/264.
23. Machado H, Silva S. Portuguese forensic DNA database: political enthusiasm, public trust and probable issues in future practice. In: Hindmarsh R, Prainsack B, eds. *Genetic Suspects: Global Governance of DNA Profiling and Databasing.* Cambridge: Cambridge University Press; 2010:218–239.
24. Prainsack B. Key issues in DNA profiling and databasing: implications for governance. In: Hindmarsh R, Prainsack B, eds. *Genetic Suspects: Global Governance of Forensic DNA Profiling and Databasing.* Cambridge: Cambridge University Press; 2010:153–174.
25. Lampland M, Star SL, eds. *Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life.* Ithaca: Cornell University Press; 2009.
26. Bigo D. EU police cooperation: national sovereignty framed by european security? In: Guild E, Geyer F, eds. *Security versus Justice? Police and Judicial Cooperation in the EU.* Farnham, UK: Ashgate; 2008:91–108.
27. de Hert P, Gutwirth S. Interoperability of police databases within the EU: an accountable political choice? *Int Rev Law Comput Technol.* 2006;20(1-2):21–35. https://doi.org/10.1080/13600860600818227.
28. McCartney C. Transnational exchange of forensic evidence. In: Bruinsma G, Weisburd D, eds. *Encyclopedia of Criminology and Criminal Justice.* New York: Springer; 2014:5302–5313. https://doi.org/10.1007/978-1-4614-5690-2.
29. Gonçalves ME, Jesus IA. Security and personal data protection in the European Union: challenging trends from a Human Rights' perspective. *Hum Secur Perspect.* 2012;9(1):117–144.
30. Kruse C. *The Social Life of Forensic Evidence.* Oakland, CA: University of California Press; 2016.

31. Cole S. *Suspect Identities: A History of Fingerprinting and Criminal Identification.* Harvard: Harvard University Press; 2001.
32. Jasanoff S. Just evidence: the limits of science in the legal process. *J Law Med Ethics.* 2006;34(2):328–341. https://doi.org/10.1111/j.1748-720X.2006.00038.x.
33. Lawless C. The low template DNA profiling controversy: biolegality and boundary work among forensic scientists. *Soc Stud Sci.* 2012;43(2):191–214. https://doi.org/10.1177/0306312712465665.
34. Williams R, Johnson P. *Forensic DNA Databasing: A European Perspective. Durham.* 2005; 2005http://www.dur.ac.uk/resources/sass/WilliamsandJohnsonInterimReport2005-1.pdf, Accessed date: 21 July 2017.
35. Lynch M. God's signature: DNA profiling, the new gold standard in forensic science. *Endeavour.* 2003;27(2):93–97.
36. Sarewitz D. *Frontiers of Illusion: Science, Technology, and the Politics of Progress.* Philadelphia: Temple University Press; 1996.
37. Charmaz K. *A Construção Da Teoria Fundamentada: Guia Prático Para Análise Qualitativa.* Porto Alegre: Artmed; 2009.
38. Strauss AL, Corbin J. *Basics of Qualitative Research. Grounded Theory Procedures and Techniques.* Newbury Park, CA: Sage Publications; 1990.
39. Yin RK. *Case Study Research: Design and Methods.* London: Sage Publications; 1994.
40. Nunes JA. *As teias da família: A construção interaccional das solidariedades primárias.* 1992; 1992.
41. EU Council. Implementation of the provisions on information exchange of the "Prüm Decisions" - 5010/3/15. Presented at the http://data.consilium.europa.eu/doc/document/ST-5010-2015-REV-3/en/pdf; 2015.
42. Bertaux D. *Les Récits de Vie: Perspective Ethnosociologique.* Paris: Editions Nathan; 1997.
43. Charmaz K. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis.* London: Sage Publications; 2006.
44. Mayring P. Qualitative content analysis. In: Flick U, Kardorff E von, Steinke I, eds. *A Companion to Qualitative Research.* London: Sage; 2004:266–269.
45. Machado H, Granja R. Police epistemic culture and boundary work with judicial authorities and forensic scientists: the case of transnational DNA data exchange in the EU. *New Genet Soc.* May 2019:1–19. https://doi.org/10.1080/14636778.2019.1609350.
46. Innes M, Fielding N, Cope N. "The appliance of science?": the theory and practice of crime intelligence analysis. *Br J Criminol.* 2005;45(1):39–57. https://doi.org/10.1093/bjc/azh053.
47. Hijmans H. The Third Pillar in practice: coping with inadequacies-information sharing between Member States. *Discussion Paper for the Meeting of the Netherlands Association for European Law.* Nederlandse Vereniging voor Europees Recht, NVER; 2006.
48. McCartney C. Trust and the international exchange of forensic information. In: Hufnagel S, McCartney C, eds. *Trust in International Police and Justice Cooperation.* Oxford and Portland, Oregon: Bloomsbury; 2017:169–189.
49. Perras C. Transnational policing and its contexts: flexibility and (dis)trust. In: Hufnagel S, McCartney C, eds. *Trust in International Police and Justice Cooperation.* Oxford and Portland, Oregon: Bloomsbury; 2017:221–240.
50. Balzacq T, Hadfield A. Differentiation and trust: prüm and the institutional design of EU internal security. *Co-op Conflict.* 2012;47(4):539–561. https://doi.org/10.1177/0010836712462781.
51. Santos F, Machado H, Silva S. Forensic DNA databases in European countries: is size linked to performance ? *Life Sci Soc Policy.* 2013;9(12):1–13. https://doi.org/10.1186/2195-7819-9-12.
52. Hufnagel S, McCartney C, eds. *Trust in International Police and Justice Cooperation.* Oxford: Hart Publishing; 2017.
53. Fujimura J. Future imaginaries: genome scientists as sociocultural entrepreneurs. In: Goodman AH, Heath D, Lindee MS, eds. *Genetic Nature/Culture: Anthropology and Science between the Two-Culture Divide.* Berkeley: University of California Press; 2003:176–199.
54. Craig P, Búrca G de. *EU Law. Text, Cases, and Materials.* Oxford: Oxford University Press; 2008.