Law and ethics in the modern EU 'surveillance society': Are the data protection principles 'dead' in the Area of Freedom Security and Justice? The case-study of the information systems of VIS and EURODAC.

Maria Tzanou

***** Preliminary draft. *****

***** Please do not cite or circulate without the author's permission. *****

"The problem with databases emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, resulting in a lack of meaningful participation in decisions about our information."[1]

I. Introduction

II. Defining the 'Surveillance society'

III. The EU as an emerging 'Surveillance society'

i. The New Age of Information exchange: From the Hague to the Stockholm Programme vision

ii. Some caveats: why should we be careful when characterizing the EU as an emerging 'Surveillance society'?

IV. The EU as an emerging 'Surveillance society' and Data Protection: Dangers

[1] Daniel Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy", *53 Stan. L. Rev.* (2001), 1393, 1422.

i. 'Function creep': the case studies of VIS and EURODAC

1. The case of VIS

a. The VIS legal framework

b. Counter-terrorism and access to VIS for law enforcement purposes: Challenges to fundamental rights

2. The case of EURODAC

a. Legal framework

b. EURODAC and counter-terrorism: Challenges to fundamental rights

V. Concluding remarks: The EU as an emerging 'Surveillance society': Risks to the rule of law

I. Introduction

The computer database has been eloquently described as 'the biggest change brought about by the information technology revolution'.[2] Indeed, multiple data can now be gathered, processed, tabulated and cross-referenced at speeds and with accuracy that would have been unthinkable in the past. In today's information society, where the collection, storage, use, collation and communication of vast amounts of personal data are central to the functioning of public services as well as private business, computer databases and computer networks are becoming almost ubiquitous.[3]

It goes without saying that databases are crucial for law enforcement. The storage and exchange of information through large-scale databases that interlink to each other is a very powerful apparatus for law enforcement authorities, in particular in the fight against terrorism. For this reason, a proliferation of cross-border information systems used for law enforcement purposes has been witnessed over the past few years. This 'security web'[4] is currently being spun at national, supranational and transatlantic levels alike.

However, despite the obvious benefits, large-scale databases raise many questions. What information is stored in them and for how long? How 'secure' are they? Who accesses them? Is there any accountability for the processors of personal information stored in databases? But above

[2] 'A report on the surveillance society: For the Information Commissioner by the Surveillance Studies network', September 2006, available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf, para 9.6.1.

[3] Surveillance society report, above n 1, para 9.6.1.

[4] F. Geyer, Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice' [2008] <http://shop.ceps.eu/BookDetail.php?item_id=1650> Centre for European Policy Studies, Research paper No. 9, retrieved 10 May 2009, 2.

all: what are their implications on the rights to privacy and data protection of the individuals? What rights has the individual to check and, if necessary, to correct data held about himself or herself?

Writing on computer databases, Daniel Solove argued that the Big Brother metaphor, that is often used by journalists, politicians, jurists, and legal academics to describe the privacy problem created by the collection and use of personal information through databases is the wrong paradigm, and the metaphor of Franz Kafka's The Trial should be used instead because it depicts in the correct terms the problems posed by databases to data privacy.[5] According to Professor Solove, the problems caused by the collection and storage of information in databases should not be couched on terms of surveillance, because databases do not 'uncover one's hidden world', nor they 'disclose concealed information'. On the contrary, the problem posed by databases "is the powerlessness, vulnerability, and dehumanization created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information."[6] While Professor Solove makes a strong point, I will all the same use the Big Brother paradigm for the present discussion. There are two reasons for that: First, the 'surveillance paradigm' does not ascribe to the databases that will be examined, but to the EU instead. In this context, I will explain why I consider the EU as an 'emerging surveillance society'. Secondly, and more importantly, I will argue that specifically in the law enforcement context, the Big Brother metaphor seems the most appropriate one.

The paper will proceed as follows: First, I will attempt to sketch out why the European Union (EU) can be considered as an emerging surveillance society and what implications this has on the right to personal data protection as protected within this legal order. I will start by defining the surveillance state or the surveillance society and by identifying its main characteristics (II). I will then examine to what extent the characteristics of the surveillance society can be applied to the EU (III). Subsequently, I will discuss the dangers posed to the right to data protection by the EU as an emerging surveillance society. For this reason, I will focus, in particular, on two case studies that pose the particular problem of 'function creep': the Visa Information System (VIS) database and EURODAC (IV). I will conclude with a critical note on the risks posed to fundamental rights and the rule of law when the EU is acting as a surveillance society (V).

II. Defining the 'Surveillance society'

In academic literature, has been used in a plethora of political science studies[7] already since the 1980s[8] in order to describe a computer-based society where information plays a crucial role within the bureaucratic control exercised by the national state.

Be that as it may, the notion of 'surveillance society' does not fit well in the legal discipline, as it is far from being a legal notion itself. Problems of definition in a legal text of a non-legal concept

5

6

7 Surveillance society report, above n 1, para 3.5 and references therein.

8 The first reference to surveillance society was made by Gary T. Marx in 1985.

hence arise. However, I will use the term 'surveillance society' merely *instrumentally*,[9] insofar as it is needed in order to demonstrate my main thesis which regards the privacy-intrusive measures adopted by the EU within the general context of the fight against terrorism.

In an article of 2006, Balkin and Levinson note that the 'National Surveillance State is characterized by a significant increase in government investments in technology and government bureaucracies devoted to promoting domestic security and (as its name implies) gathering intelligence and surveillance using all of the devices that the digital revolution allows.'[10] We can discern three parts in this definition: the first one concerns the increased engagement of the National Surveillance State in intelligence gathering and surveillance activities; the second regards the use of new technologies and technological devices to facilitate this process; finally, the third deals with the overall goal of the surveillance activities which is the safeguarding and promotion of national security.

For the purposes of the present analysis, this definition will be adopted but with the necessary clarification that I will not refer to the 'National Surveillance State', but rather to the 'surveillance society'.

III. The EU as an emerging 'Surveillance society'

The main thesis of the present contribution is that the European Union (EU) is acting after the 9/11 terrorist attacks and especially after the Madrid and London bombings, as an emerging 'Surveillance Society'. In particular, I argue that one can identify, with a number of *caveats* that will be analyzed later, the basic characteristics of the surveillance society in the EU. This assumption is based on the emphasis that the European Union has placed over the past years on the creation of an extensive toolbox for the collection, storage, and exchange of information between national authorities and other European players in the area of freedom, security, and justice.

As seen above, the surveillance society is characterized by 1) an increased engagement in intelligence gathering and surveillance activities 2) the use of new technologies and technological devices and 3) the overall goal of enhancing security. As will be demonstrated below, these characteristics can be found in the EU's actions and policies after 9/11. However, a further clarification is needed here. The surveillance-related activities of the EU are mainly pinned down in the exchange of information through large-scale centralised databases in the Area of Freedom, Security, and Justice (AFSJ). Below, the main characteristics of the EU's surveillance society-related policies, i.e 'information exchange' for the safeguarding of security is set out.

---

9 Emphasis added.

10 Balkin, Levinson, J. Balkin and S. Levinson, 'The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State', available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=930514, p. 131.

i. The New Age of Information exchange: From the Hague to the Stockholm Programme vision

Facilitating the exchange of and access to information for the fight against terrorism, but also more generally to ensure security has been high on the political agenda of the European institutions over the past few years.[11] This is because the exchange of data is becoming more and more essential for law enforcement in 'high profile' fields, such as counter terrorism. In its Communication of 10 June 2009 on an area of freedom, security and justice serving the citizen, the Commission notes that 'security in the EU depends on effective mechanisms for exchanging information between national authorities and other European players. To achieve this, the EU must develop a 'European Information model' based on a more powerful strategic analysis capacity and better gathering and processing of operational information.'[12]

Against this background, the exchange of personal data between the law enforcement authorities in the different Member States has become lately a common scenario in the area of Freedom, Security and Justice. In this regard, improving the exchange of information was one of the central elements of the 'Hague Programme', the EU's five year (2005-2010) Action Plan for Freedom, Justice and Security, adopted on 5 November 2004 by the European Council in response to the 'war on terrorism'.[13] Under the headline 'Strengthening Security', the 'Hague Programme' included the so-called 'principle of availability', which purported the governing standard for information flows throughout the Union. According to this principle, 'a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State'. This means that full use of new technologies should be made, in order to establish reciprocal access to national databases, interoperability as well as direct (online) access to existing central EU databases.[14]

Currently, a number of EU databases and systems of information exchange are already in place, while others are envisaged to become operational soon. However, as a scholar notes eloquently, it appears as if the EU is only at the beginning of a 'new age of information exchange'.[15] The EU's information exchange architecture in the area of Freedom, Security and Justice involves various different actors and is conducted for a number of different purposes. In particular, four actors can be

---

11 Hijmas and Scirocco, 'Shortcomings in EU Data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?', 2009 CMLR 46, 1485, 1489.

12 COM2009 (262) final, p. 16.

13 The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005, p. 1.

14 See Statewatch analysis of the 'principle of availability', available at <http://www.statewatch.org/analyses/no-59-p-of-a-art.pdf> , according to which 'the "principle of availability" and data protection… are absolutely irreconcilable… The principle of availability and the "free market" in access to all (present and future) national or EU databases is a classic example of how EU governments have used the "war on terrorism" to give the emerging EU state sweeping powers of surveillance and control'.

15 F. Geyer, Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice' [2008] <http://shop.ceps.eu/BookDetail.php?item_id=1650> Centre for European Policy Studies, Research paper No. 9, retrieved 10 May 2009.

identified: the EU, its Member States, private parties, and third countries (or international organisations). This leads to four different exchange possibilities: Firstly, reciprocal data transfers between Member States and EU institutions in the framework of centralized databases. These are the databases of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS) that store data input by the Member States, and provide access to them for law enforcement purposes.[16] The second possibility is the exchange of information between Member States and private actors (public/private partnership in combating crime). An example of this is the draft Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes.[17] This obliges air carriers to make available the PNR data of passengers on international flights to competent authorities for the purpose of preventing and combating terrorist offences and organized crime.[18] A third option is data transfer between private actors and third countries. Under this category falls for instance the transmission of PNR data to the US, or the SWIFT case.[19] Finally, the fourth possibility is the exchange of data between Member States themselves, based on intergovernmental agreements, such as the Prüm Treaty regulating enhanced cross-border cooperation, particularly in combating terrorism and cross-border crime, which was signed in May 2005 by seven EU Member States.[20]

The 'Stockholm Programme', which is the next EU's five year plan (2010-2014) for Justice and Home Affairs, endorses an even more powerful vision of surveillance society elements. In particular, it sets out a number of policies to be adopted and implemented in the area of freedom, security and justice that demonstrate quite clearly that the EU's surveillance-related aspirations are even more serious than before. In the Programme, the European Council calls for a definition of a comprehensive EU internal security strategy based, *inter alia*, on a proactive and intelligence-led approach, that requires stringent cooperation between EU agencies, including a further improvement of their information exchange.[21]

According to the Programme, security in the EU requires an integrated approach in which security professionals share a common culture, pool information as effectively as possible and have the right technological infrastructure to support them. For this reason, and while the European Council 'notes with satisfaction that developments over the past years in the EU have led to a wide choice and created an extensive toolbox for collecting, processing and sharing information between national authorities and other European players in the area of freedom, security and justice',[22] where

---

16 Geyer, above n 21.

17 Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM (2007) 654.

18 Another example of the public/private partnership is the Data Retention Directive adopted under the first pillar.

19 See Working Party 29 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

20 Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, Prüm, 27 May 2005. The Prüm Treaty has been incorporated in the EU legal order.

21 Stockholm Programme, p. 36.

22 Stockholm Programme, p. 38.

the principle of availability continues to give important impetus to this work, there is a need for a coherent and consolidated development of information management and exchange. In this respect, the European Council invites the Council and the Commission to adopt and implement an 'EU Information Management Strategy', and to consider the need for developing a 'European Information Exchange Model' based on current instruments, such as the Prüm framework and the so-called Swedish Framework Decision (Proposal for a Framework Decision on exchange of information under the principle of availability).

The Stockholm Programme stipulates that the EU information management strategy should be based among others on business-driven development (a development of information exchange and its tools that is driven by law enforcement needs), guiding principles for a policy on the exchange of information with third States for law enforcement purposes, interoperability of IT systems, a rationalisation of the different tools, including the adoption of a business plan for large IT systems, and overall coordination, convergence and coherence. The European Council also calls for the establishment of an administration having the competence and capacity to develop technically and manage large-scale IT-systems in the area of freedom, security and justice.

The European Council also takes into account and stresses the role of new technologies that need 'to keep pace with and promote the current trends towards mobility, while ensuring that people are safe, secure and free'.[23] In this respect, it invites the Council, the Commission, the European Parliament, and where appropriate the Member States to 'ensure that the priorities of the internal security strategy are tailored to the real needs of users and focus on improving interoperability'. Finally, it calls the EU institutions to reflect on how to further develop the use of existing databases for law enforcement purposes, while fully respecting data protection rules, so as to make full use of new technologies with a view to protecting the citizens.

ii. Some caveats: why should we be careful when characterizing the EU as an emerging 'Surveillance society'?

It has been argued that the EU is developing more and more elements of a surveillance society. However, the characterization of the EU as an emerging 'surveillance society' might be scientifically risky and thus requires several caveats. First of all, it is a known fact that the EU does not have police or public authorities with executive powers to ensure directly security. This means that its contribution to security is based on the adoption of measures that are intended to enable the competent authorities of the Member States to fight terrorism and crime themselves.[24] In this respect, the EU has laid down a number of legislative instruments aimed to harmonize, co-ordinate and facilitate the Member States' action against terrorism and crime.

Secondly, and within this context, its role as a 'Surveillance Society' comes *in principle* at a later stage: it is normally the national authorities of the Member States that will first collect the

23 Stockholm Programme, p. 40.

24 Buttarelli, 'Legal Restrictions- Surveillance and fundamental rights' in 'New Technical Means of Surveillance and the Protection of Fundamental Rights- Challenges for the European Judiciaries', Vienna July 19th 2009, p. 4.

information using surveillance technologies, and the EU will then make possible the exchange of this information with other Member States and its storage in centralized databases.

IV. The EU as an emerging 'Surveillance society' and Data Protection: Dangers

The protection of personal data is recognized in primary EU law as a dimension of the right to respect for private life[25] under Article 8 of the European Convention on Human Rights (ECHR), as reflected in Article 6 (2) of the TEU which provides that the Union respects fundamental rights, as guaranteed by the ECHR and the constitutional traditions common to the Member States, as general principles of Community law'.[26]

More importantly, the right to data protection, enjoys constitutional protection within the EU legal order enjoys as it is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (EUCFR). This elevation of the right to data protection to the level of a fundamental right is very important, because, for the first time, it has been recognized as a distinct right from the right to respect for private and family life, home and communications which is set out in Article 7 of the Charter.[27]

There is a particular danger posed to the fundamental right to data protection by the EU as an emerging 'surveillance society': the so-called 'function' or 'competence creep'. Within the EU legal context, this danger is linked to the EU's own particular nature that encompasses different competences in distinct areas. Most EU databases, such as VIS or EURODAC have nothing to do with the fight against terrorism or crime, since they have been created for different purposes. For instance, the Visa Information System was created to support the common visa policy, and EURODAC was established in order to enhance the common asylum policy. Yet, data contained in the former database can be accessed by designated authorities of Member States and by Europol to fight terrorism; the same - with even more serious consequences - has been proposed with respect to EURODAC. This raises many concerns: once the information has been collected and stored in centralized databases it can be very easily used for law enforcement purposes. This is required in the name of the 'surveillance society'. However, the fundamental question here is: Can information be used only because it exists and new technologies permit the storage of data and their interchange? In this respect, this article will take a closer look at the case studies of VIS and EURODAC.

---

[25] Skandamis, Sigalas and Stratakis, 'Rival Freedoms in Terms of Security: The Case of Data Protection and the Criterion of Connexity', Research Paper No.7, December 2007, available at http://www.ceps.eu, p. 6.

[26] The ECJ has repeatedly held with regard to fundamental rights that: 'fundamental rights form an integral part of the general principles of law whose observance the Court ensures. For that purpose, the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which they are signatories. In that regard, the ECHR has special significance'. See for instance Case 29/69 *Stauder* [1969] ECR 419, para 7.

[27] Rodota, 'The European Constitutional Model for Data Protection', paper presented at the Public Seminar of the European Parliament: PNR/SWIFT/Safe Harbour: Are transatlantic data protected? (Transatlantic relations and data protection), Monday 26 March 2007, available at http://www.europarl.europa.eu/hearings/20070326/libe/rodota_en.pdf, p. 2.

i. 'Function creep': the case studies of VIS and EURODAC

1. The case of VIS

a. The VIS legal framework

Despite the fact that the Visa Information System database (VIS) has no direct connection with the EU's counter-terrorism strategy being a database that supports the common visa policy, ironically enough, as an author points out, the decision to establish the Visa Information System (VIS) was 'a direct consequence of the terrorist attacks of 11 September'.[28] At the extraordinary Council meeting of 20 September 2001 that followed the attacks, the Home Affairs and Justice Ministers agreed that the procedures for the issue of visas should be tightened and that the Commission should make proposals for the establishment of a network for information exchanges concerning visas issued by Member States. The VIS would collect and store fingerprints and other biometric identifiers of all third-country nationals applying for short-term visas in any EU Member State. According to the relevant Council guidelines, the development of the VIS aimed, among others, to contribute towards improving internal security and combating terrorism.[29]

The Council Decision establishing a system of exchange of visa data between Member States, 'the Visa Information System' was adopted on 8 June 2004 on the basis of Article 66 EC.[30] The Decision gives the Commission the mandate to develop the VIS and constitutes the required legal basis to allow for the inclusion of the necessary appropriations for its development through EC financing. According to the Decision, the Visa Information System will be based on a centralised architecture and consist of a central information system, 'the Central Visa Information System' (CS-VIS), an interface in each Member State, 'the National Interface' (NI-VIS) which will provide the connection to the relevant central national authority of the respective Member State, and the communication infrastructure between the Central Visa Information System and the National Interfaces.[31] The Central VIS, the National Interface in each Member State, and the communication infrastructure between the Central VIS and the National Interfaces are to be developed by the Commission, while the national infrastructures are to be adapted and developed by the Member States.[32] The system will be designed to provide for the connection of at least 12,000 users in 27 Member States and at 3,500 consular posts.[33]

---

28 Baldaccini, 'Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases', (2008) *European Journal of Migration and Law* 10, 31, 39.

29 Council Conclusions on the development of the Visa Information System (VIS), Doc. 6535/04, 20 February 2004.

30 Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213/5.

31 Article 1 (2) of the VIS Decision.

32 Article 2 of the VIS Decision.

33 Communication from the Commission to the Council and the European Parliament – Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS), COM(2003) 771 final, 11 December 2003, p. 26.

Citizens from 134 countries require visas to enter the EU. This means that it had been possible for an applicant rejected by one country's consulate to continue applying to other consulates. Once the VIS is in place this will not be possible. Information on previous applications and reasons for rejection will be available through the new system. The inclusion of fingerprint data is intended to allow the exact verification of somebody's identity.

The VIS was due to become operational by spring 2009. On 24 June 2009, following the request of the Council and the European Parliament, the Commission introduced a legislative package proposing the setting up of an Agency for the long-term operational management of the SIS II, VIS, EURODAC and other large-scale IT systems in the area of freedom, security and justice. According to the proposals, the core mission of the Agency would be to fulfil the operational management tasks for SIS II, VIS and EURODAC, keeping the systems functioning 24 hours a day, seven days a week. In addition to these operational activities, the Agency will also be responsible for adopting the necessary security measures, reporting, publishing statistics, the monitoring of research, SIS II and VIS related training and information issues. It will ensure data security and integrity as well as compliance with data protection rules.

In order to implement the Decision, a Regulation defining the purpose, the functionalities and the responsibilities of the information system, and establishing the procedures and conditions for the exchange of data between Member States on short-stay visa applications was adopted on 9 July 2008.[34] According to it, the data to be recorded in the VIS include not only alphanumeric data (on the applicant and on the visas requested, issued, refused, annulled, revoked or extended), but also biometric identifiers such as photographs and applicants' fingerprint data. Links to previous visa applications and to the application files of persons travelling together are also included in the VIS.[35]

Access to the VIS for entering, amending or deleting data, will be reserved exclusively to duly authorised staff of the visa authorities; while access for consulting data, will be reserved to visa authorities and authorities competent for checks at the external border crossing points, immigration checks and asylum, and will be limited to the extent the data is required for the performance of their tasks.

b. Counter-terrorism and access to VIS for law enforcement purposes: Challenges to fundamental rights

As seen above, apart from improving the implementation of the common visa policy, one of the purposes of VIS was also to contribute towards internal security and to combating terrorism. In its meeting of 7 March 2005 the Council stated that 'in order to achieve fully the aim of improving internal security and the fight against terrorism', Member State authorities responsible for internal

[34] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218/60.

[35] Article 5 of the VIS Regulation.

security should be guaranteed access to the VIS, 'in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats'.

On 23 June 2008 the Council adopted a Decision allowing access for consultation of the Visa Information System by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.[36] The Decision was adopted on the basis that 'it is essential in the fight against terrorism and other serious crimes for the relevant services to have the fullest and most up-to-date information in their respective fields in order to perform their tasks. The Member States' competent national services need information if they are to perform their tasks'. In this respect, 'the information contained in the VIS *may be necessary* for the purposes of preventing and combating terrorism and serious crimes and should therefore be available for consultation' by the designated authorities,[37] and by Europol that has a key role in the field of cross-border crime investigation and in supporting Union-wide crime prevention, analyses and investigation.[38]

The Decision provides that VIS will be accessed by designated authorities of the Member States. For this purpose, every Member State must keep a list of the designated authorities and notify them to the Commission and the General Secretariat of the Council. The Commission will publish these declarations in the *Official Journal of the European Union*.[39] Access to the VIS for consultation can be exercised also by authorities responsible for internal security from Member States which are not part of the VIS.[40]

Access to VIS data is limited for the specific purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA on the European arrest warrant. The Decision stipulates that 'it is essential to ensure that the duly empowered staff with a right to access the VIS is limited to those who 'have a need to know' and possess appropriate knowledge about data security and data protection rules'.[41]

Article 5 of the Decision lays down clearly the conditions for the access to VIS data. In order to exclude routine access, this provision allows for the processing of VIS data only on a case-by-case basis. Such a specific case exists in particular when the access for consultation is connected to a specific event or to a danger associated with serious crime, or to a specific person in respect of whom there are serious grounds for believing that he will commit or has committed terrorist offences or other serious criminal offences or he has a relevant connection with such a person. In this regard, the designated Member States' authorities and Europol may search the data contained in

---

36 Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218/129.

37 See Recital 3 of the VIS Decision (emphasis added).

38 See Recital 4 of the VIS Decision.

39 Article 3 of the VIS Decision.

40 Article 6 of the VIS Decision. The VIS Regulation does not apply to the United Kingdom and Ireland. Denmark has decided to implement it.

41 Recital 6 of the VIS Decision.

the VIS when they have reasonable grounds to believe that such a search will provide information that will substantially assist them in preventing, detecting or investigating serious crime.[42]

It is true that the VIS Decision attempts to circumscribe with a number of data protection safeguards the access to VIS data by law enforcement authorities. However, it has been asserted that this measure is still very problematic from the point of view of the right to personal data protection. More precisely, there is a specific data protection principle that suffers particularly by the Decision granting access to VIS data: the purpose limitation principle.

The 'purpose limitation principle' – that is, according to the Data Protection Directive, the principle that establishes that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes[43]- is a fundamental principle of the EU data protection regime.[44] This is because an individual's informed consent to the collection and processing of his/her personal data is dependent on the information about the purpose and use of those data.[45]

With regard to the storage of personal information to centralized databases, the importance of the purpose limitation principle for safeguarding the transparency and the legality of the use of the data and consequently of the individuals' fundamental rights cannot be overemphasized. Within this context, the principle of purpose limitation prescribes that the scope and purpose of a database should strictly define the group of users who may lawfully access the database and process the data held on it. This principle commands that there be a strict nexus between the purpose of a data collection and the use that can be made of the data.

Given the importance of the purpose limitation principle, it is almost by definition that this principle should enjoy the highest level of protection within the context of the VIS information system. This fundamental principle, however, is rendered meaningless by the general trend to grant law enforcement authorities access to databases that have no law enforcement purposes whatsoever. With respect to VIS, it is unacceptable that it contains among its purposes stipulated in the Regulation itself a vague and open goal of contributing to the prevention of threats to Member States' internal security. The Visa Information System database cannot function by its nature as a 'multifunctional tool'. In this regard, it is very different from the SIS which pursues also law enforcement purposes, and includes alerts upon which certain executive action should be adopted. VIS on the other hand should be used only for the implementation of EU visa policy, and not for the fight against terrorism, or serious crime, or even illegal immigration. Once the purposes of a large-scale information system, where huge amounts of data are stored, are not clearly and restrictively

---

42 Article 5 of the VIS Decision. See also Recital 8.

43 Article 6 (1) (b) of the Data Protection Directive.

44 And of data protection law in general. As Gellman (Gellman, 'Privacy: Finding a Balanced Approach to Consumer Options', available at http://www.cdt.org/privacy/ccp/consentchoice4.pdf) notes a 'statement of purpose helps to strike a reasonable balance between the interests of record keepers and those of record subjects. It tells the record subject the consequences of disclosing data . . . A purpose statement provides the data subject with information about the purpose for data collection, so that he or she can assess the benefits and risks of disclosure and make an informed decision. It also prevents a record keeper from using or disclosing information in ways that are not in accordance with the stated purpose . . . The purpose specification principle has a self-balancing feature'.

45 Cannataci and Bonnici, 'The end of the purpose-specification principle in data protection?', (2010) *International Review of Law, Computers & Technology* Vol. 24, No. 1, 101, 101.

defined, then the system is opened up for any possible purpose. It goes without saying that this 'function' or 'competence creep', where personal data collected for one specific purpose and in order to fulfill one function, are used for completely different purposes, which are totally unrelated to the ones for which they were initially collected constitutes a breach to the purpose limitation principle.

The need for law enforcement authorities to benefit from the best possible tools to identify the perpetrators of terrorist acts or other serious crime cannot be disregarded. Furthermore, it seems that the Decision granting access to VIS for law enforcement purposes sets out a number of data protection safeguards and in particular envisages only access on a case-by-case basis and not routinely. However, it has been asserted that the adoption of the VIS Decision itself violates the purpose limitation principle. Granting access to VIS in order to combat terrorism and serious crime constitutes a disproportionate intrusion in the privacy of travelers who agreed to their data being processed in order to obtain a visa, and expect their data to be collected, consulted and transmitted, only for that purpose. What's more, since information systems are built for a specific purpose, with safeguards, security, conditions for access determined by this purpose, granting access for a purpose different from the original one would not only infringe the principle of purpose limitation, but could also render the above mentioned elements inadequate or insufficient.[46] It is very questionable to what extent measures that introduce exceptions to the purpose limitation principle, such as the VIS Decision which allows law enforcement authorities and Europol access and use of the VIS data for other purposes than for which these data were collected and processed, can be adopted in the context of the fight against terrorism.

Finally, the fact that law enforcement authorities are granted access to such a vast amount of data entails the risk of profiling individuals on the basis of the information held on them into VIS. This might lead to an infringement of other fundamental rights beyond the right to privacy of the individuals concerned.[47]

2. The case of EURODAC

a. Legal framework

EURODAC, which stands for *European Dactyloscopie*, is the European fingerprint database for identifying asylum seekers and irregular border-crossers established by Council Regulation 2725/2000 of 11 December 2000.[48] The objective of the creation of the EURODAC system was to facilitate the application of the Dublin Regulation, which makes it possible to determine the Member State responsible for examining an asylum application, by comparing the fingerprints of asylum seekers and illegal immigrants. EURODAC enables Member States to identify asylum applicants and persons who have been apprehended while unlawfully crossing an external frontier

[46] See in this respect Opinion of the EDPS on the VIS Decision, above n 216, 4.

[47] For instance violations of the principle of non-discrimination, of due process rights, of the freedom of movement.

[48] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316/1.

of the Community. The system is based on the assumption that asylum seekers must apply for asylum in the first EU country in which they arrive and may be returned to another Member State if it can be proven that they have either passed through the border of another Member State or already lodged an application for asylum in that Member State. Thus, by comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State, or whether an asylum applicant entered the Union territory unlawfully. EURODAC stores fingerprints of every applicant for asylum and of every alien who is apprehended in connection with the irregular crossing of an external border of a Member State, over the age of 14 years old.

EURODAC is a database aimed to support the implementation of the common asylum policy by preventing 'asylum shopping'. In particular, the computerised system allows for the identification of third-country nationals who may have already lodged asylum applications in the EU and whose data were already enrolled by one Member State, and thus when a Member State receives a hit reply, proving that an asylum seeker has applied for asylum before in another Member State, it will request the other Member State to take back the asylum applicant.

EURODAC consists of: (a) the Central Unit equipped with a computerised fingerprint recognition system; (b) a computerised central database in which the EURODAC data are processed for the purpose of comparing the fingerprint data of applicants for asylum and of illegal immigrants; and (c) means of data transmission between the Member States and the central database.

b. EURODAC and counter-terrorism: Challenges to fundamental rights

Following the general trend, started with VIS, the Member States have agreed that EURODAC should also be made accessible for law enforcement purposes in order to fight terrorism. A commitment to this effect had been made by the Interior Minister of the EU's six largest Member States at their G6 meeting in Heiligendamm, Germany, on 22-23 March 2006.[49] Furthermore, a paper discussed at the beginning of 2007 states the following concerning the use of EURODAC for enforcement purposes:

> 'Frequently, asylum-seekers and foreigners who are staying in the EU unlawfully are involved in the preparation of terrorist crimes, as was shown not least in the investigations of suspects in the Madrid bombings and those of terrorist organizations in Germany and other Member States (for instance, two of the five accused in German proceedings against the terrorist group "Al Tawhid", which prepared attacks against Jewish institutions in Berlin and Dusseldorf, were asylum-seekers)… Access to EURODAC can help provide the police and law enforcement authorities of the Member States with new investigative leads making an essential contribution to preventing or clearing up crimes.'[50]

---

[49] See House of Lords European Union Committee, 40th Report of Session 2005–06, *Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm*, HL Paper 221, 19 July 2006.

[50] Common 18-months Presidency Programme on Police and Customs Co-operation, Council Doc. 5291/07 of 12 January 2007, 6.

Along the same line, the conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 considered that, in order to fully achieve the aim of improving security and to enhance the fight against terrorism, access under certain conditions to EURODAC should be granted to Member States' police and law enforcement authorities, as well as Europol. The Ministers therefore invited the Commission to present 'as soon as possible' an amendment to the EURODAC Regulation in order to allow for police access to the database.[51]

On 10 September 2009 the Commission adopted a proposal concerning access to EURODAC data by Member States law enforcement authorities and Europol for law enforcement purposes.[52] The proposal was justified by the Commission on the basis that fingerprint data is especially useful information for law enforcement purposes, as it constitutes an important element in establishing the exact identity of a person. 'The usefulness of fingerprint databases in fighting crime is a fact that has been repeatedly acknowledged'.[53] Fingerprint data of asylum seekers are collected and stored in the Member State in which the asylum application was filed, as well as in EURODAC. In fact, the Commission points out that in most Member States the law enforcement authorities have direct or indirect access to their national databases that contain the fingerprints of asylum seekers for the purpose of fighting crime.[54]

According to the Commission though, while Member States successfully access asylum seekers fingerprints on a national level, access to asylum seekers fingerprint databases of other Member States is more problematic. This is because there is a structural information and verification gap since there exists no single system which enables law enforcement authorities to determine the Member State that has information on an asylum seeker. If a query of a national Automated Fingerprint Identification Systems (AFIS) using the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and crossborder crime (Prüm Decision) does not result in a 'hit', it is not certain that no information is available in a Member State. In this respect, according always to the Commission's proposal, law enforcement authorities may not only remain ignorant about whether or not information is available at all and in which Member State, but often also whether this information relates to the same person. This means, pursuant to the proposal, that without any action at EU level, the action of law enforcement authorities may become prohibitively expensive or may seriously jeopardise the application of the law because no further efficient and reasonable action to determine a person's identity can be taken. Moreover, the absence of the possibility for law enforcement authorities to access EURODAC to combat terrorism and other serious crime was reported as a shortcoming by the Commission in one of its Communications to the Council and the European Parliament.[55]

---

51 Access to Eurodac by Member State police and law enforcement authorities – Council Conclusions. Available at: http://register.consilium.europa.eu/pdf/en/07/st10/st10002.en07.pdf.

52 Proposal of 10 September 2009 for a Council decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes , COM(2009) 342 final.

53 Proposal for a Decision on EURODAC, above n 237, 2.

54 Proposal for a Decision on EURODAC, above n 237, 2.

55 Commission Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 24 November 2005.

I will not comment on the Commission's justification concerning access to EURODAC by law enforcement authorities, which nevertheless is, at best, extremely weak. Turning to the substance of the proposal itself, this follows in most points the VIS Decision, examined above. In particular, it establishes a case-by case access to EURODAC and lays down a number of data protection safeguards, among which are the proportionality and purpose limitation principles.

A number of points should be advanced on the EURODAC proposal. First of all, here again we are dealing with a function creep case. When adopted, the Regulation establishing EURODAC did not contemplate police access to EURODAC; the fingerprints were collected for the very specific purpose of determining which Member State is responsible for examining an asylum application, and in any case for facilitating the application of the Dublin Convention. To be used for a completely different purpose, that is by law enforcement authorities to fight terrorism and crime, goes clearly against the purpose limitation principle and the legitimacy of the processing.

There are however wider concerns about access to EURODAC data for law enforcement purposes. The proposal for a Council Decision not only concerns individuals in principle not suspected of any crime, but what is more important, it concerns a particularly vulnerable group in society, i.e. asylum seekers, who are in need of higher protection because they flee from persecution.[56] Furthermore, granting access to EURODAC data to law enforcement authorities might have a discriminatory impact on asylum seekers, or other illegal border-crossers whose data are stored in the EURODAC database, in that they might be subject to 'a greater level of surveillance' than others in the population,[57] particularly as there is a general presumption that a disproportionate criminal activity might result from this group. This assumption is very dangerous to be translated into legal texts, since, besides reinforcing widespread prejudices, it also increases the risk of discrimination.

Finally, as the EDPS highlights in his Opinion, the Commission's proposal raises questions with regard to its necessity since there already exist a number of legal instruments,[58] concerning access to centralized databases by law enforcement authorities that have not yet been fully implemented.

V. Concluding remarks: The EU as an emerging 'Surveillance society': Risks to the rule of law

---

[56] See Opinion of the European Data Protection Supervisor on the Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, para 17.

[57] Baldaccini, above n 29, 44.

[58] For instance, the Prüm Decision, provides that Member States shall grant each other an automated access *inter alia* to national Automated Fingerprint Identification Systems (AFIS). Also, Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ 2008, L 386/89) facilitates the exchange of information (fingerprints and supplementary information) which is held by or is available to law enforcement authorities in the Member States.

It has been argued that one can identify, with a number of caveats, three elements of the surveillance society, i.e. 1) the increased engagement in intelligence gathering and surveillance activities 2) the use of new technologies and technological devices, and 3) the overall goal of enhancing security in the EU's actions after 9/11 and especially after the Madrid and London terrorist attacks. Starting from this premise, the present article has focussed on the examination of the so-called 'function creep' paradigm.

For this reason, the selected case studies have been the databases of VIS and EURODAC and in particular the access to them envisaged for law enforcement purposes. As analyzed above, this goes against the purpose limitation principle, which constitutes a fundamental principle of the EU data protection regime. Information cannot be used for different purposes from the ones that it was initially selected only because it exists and new technologies permit data interchange. This principle applies even if the information is further used for security purposes in order to fight terrorism.

Also, it seems that both in the cases of VIS and EURODAC, the boundaries between migration and asylum issues, border control, criminal law and counter-terrorism are becoming increasingly blurred in the emerging EU 'surveillance society'. This entails the risk that the movement of people across borders is conceived and treated more and more as a security issue and a potential criminal activity and that certain parts of the population, such as asylum-seekers or illegal border-crossers , or more in general third-country nationals are regarded as potential threats to security. In addition, fishing expeditions, profiling and discrimination practices can very easily arise with regard to the two databases examined.

In this respect, the present contribution demands that first of all, access to EURODAC data should not be granted to law enforcement authorities not even for the purpose of the fight against terrorism. There are already numerous possibilities for gathering information through SIS II and VIS (not to mention directly between Member States), that have not become fully operational yet, hence there is no reason to rush in this field. There are serious concerns about the respect on fundamental rights in the Area of Freedom Security and Justice. Unfortunately, it seems that this is becoming all the more an area focused mainly on security.