Profiling Technologies in Practice
Applications and Impact on Fundamental Rights and Values

Edited by Niklas Creemers, Daniel Guagnin and Bert-Jaap Koops
With contributions by Francesca Bosco, Niklas Creemers, Elena D'Angelo, Valeria Ferraris, Daniel Guagnin, Mireille Hildebrandt, Bert-Jaap Koops, Bogdan Manolea, Arnold Roosendaal and Elise Vermeersch

Profiling Technologies in Practice

Applications and Impact on Fundamental Rights and Values

Edited by Niklas Creemers, Daniel Guagnin and Bert-Jaap Koops
With contributions by Francesca Bosco, Niklas Creemers, Elena D'Angelo, Valeria Ferraris, Daniel Guagnin, Mireille Hildebrandt, Bert-Jaap Koops, Bogdan Manolea, Arnold Roosendaal and Elise Vermeersch

ISBN: 9789462402416

Published by:
Wolf Legal Publishers (WLP)
PO Box 313
5060 AH Oisterwijk
The Netherlands
E-Mail: info@wolfpublishers.nl
www.wolfpublishers.com

All URLs have been valid in time of printing, and no guarantee can be given that they will stay.

Table of Contents

IV. Border control: a new frontier for automated decision making and profiling?

Valeria Ferraris

Introduction: Borders, Bodies and Databases

Borders seemed to lose most of their significance after 1989, but then, after 9/11, all of a sudden – they were back on the agenda. Borders were once again performing the role they first acquired in the 20th century: as barriers against terrorism and to prevent other violations of security.

In Europe, this new centrality of borders was accompanied by an increasing harmonisation of the European migration policy framework and the growing relevance of risk-based approaches in many policy fields e.g., policing, justice, welfare and immigration (see Feeley and Simon 1992, Ericson and Haggerty 1997).

Borders are one of the privileged arenas for implementing risk-based strategies. They have increasingly become a tool of classification aimed at sorting individuals into deserving and undeserving foreigners (see Bosworth 2008, 200). Technology adds a new complexity to this action of sorting, as it enables automated profiling. It means that in the future the classification between different categories of foreigners could be left to algorithms and automatic procedures rather than to the reasoning of border agents. This could decrease the opportunity for the person being profiled of contesting the decision. In addition to this future development, the nature of borders has also changed, as they have become gradually more mobile, in a way that was unforeseeable just a few years ago. The concept of mobile borders (see Weber 2006) focuses on the different strategies developed by receiving countries to prevent and deter unwelcome arrivals of migrants. They are not new border control measures but strategies of manipulation of the "location and meaning of borders themselves" (Weber 2006, 22). These include, according to Weber, three different ways of border-shifting – functionally, spatially and temporally – plus a fourth one, the personalised border, when the foreigner embodies the border.

The functional shift occurs when the border is not the sole location where border functions are performed. Migration control is not confined to the border as a geographical site but is a combination of checks implemented inside and outside a country. The spatial shift refers to the removal of a part of a country's

territory,[1] whereas the temporal shift underlines that for a specific period of time the border is moved somewhere else. The personalised border has been conceptualised as "fragmented and fully portable, its location defined, not by sites of enforcement action by state officials, but in terms of the current whereabouts of certain intending visitors" (Weber 2006, 36), in other words, as a border that would-be migrants incorporate and carry around, regardless of where the functional or spatial boundary lies.

Technology plays a significant part in personalising borders. Border control is a challenging task because of the mobility of its targets. As effectively underlined by Koslowski (2011, 7), "border control officers often compare their task to squeezing a balloon: if you squeeze one end, it expands at the other". Technology is often presented as a solution to this problem, especially by policy makers and the security industry. Databases are promoted as efficient tools to track migrants and by that persistently make them accessible for border control functions. Thus the exchange of information via databases has been one of the frontiers for migration control over the last 15 years (see Zolberg 1997). This paper seeks to draw attention to one specific aspect of this subject, namely the issue of automated decision making and profiling, in order to understand whether and to what extent the new strategies of immigration control involve such measures. In particular, this study focuses on the newly developed Schengen Information System II and on Eurodac, examining how these databases are implemented and used in Italy for immigration control. The databases, especially the SIS II, will not be entirely explored. The discussion will focus on aspects concerning the control of Third Country Nationals (TCNs). The choice of Italy is due to its centrality as a gateway to Europe from the South. This role has expanded with the Italian border being placed under increasing pressure as a consequence of the crisis in Northern Africa and the Middle East.

Sections one and two draw attention to the main features of SIS II and Eurodac, examining their implementation in Italy and their daily use by immigration offices. Section three explores further developments at EU level in the so-called smart borders package and other initiatives aimed at increasing surveillance in the Mediterranean area. The last section provides some reflections on profiling and automated decision making in border control.

This research is exploratory in nature. The issue of automated decision making and profiling is fairly new and has not been described in depth in relation to immigration databases, in particular not in terms of how they are applied in

---

[1] Australia is the land of experimentation in this extreme practice. Since 2001 Australia has excised some northern islands from the so-called migration zone (area where people landing by boat, have the possibility to apply for asylum and have access to the Australian judicial system) declaring them 'excised offshore places' and, as a consequence, putting the migrants who land there in a legal no man's land. (see Coombs 2004; Ferraris 2014).

practice. Some contributions (Broeders and Hampshire 2013, Bigo et al. 2012) have pointed out, but not explored in detail, that the logic of profiling and data mining pertains to these EU databases and represents a risk for fundamental rights infringements. Other scholars (Brouwer 2007, 2008a, 2008b; Karanja 2008) have focused their attention on the risks of infringements of fundamental rights and remedies analysing the implementation of the SIS databases in some EU countries (France, Germany, The Netherlands). Also worth mentioning is the research carried out by the National Ombudsman of the Netherlands, the only public body to have conducted an assessment of the implementation of the SIS database in the Netherlands (De Nationale Ombudsman 2010).

The research was conducted through fieldwork and desk research. Before starting the fieldwork, legal texts at EU and country level together with the relevant literature were reviewed. The empirical research relies mainly on individual or group interviews with MEPs (3), the European Data Protection Supervisor (EDPS) assistant supervisor, lawyers (4), the head of the EU Commission - DG Home Affairs - Unit A3 - Police cooperation and relations with EUROPOL and the European Police College (CEPOL) (1), the Italian Data Protection Authority (DPA), police authorities at a central and local level (Italian National SIS Division, Immigration office of two cities in Italy). The Italian SIRENE Office refused the interview.

It is worth mentioning that we encountered some difficulties with gaining access to the information and obtaining authorisation to perform the interviews. Most likely, these difficulties were due to the fact that the topic concerns police databases and so specific authorisations or additional checks were necessary. Although this does not limit the generalisability of the findings, it does mean we were only able to draw a partial picture of the situation. As already underlined, this study is exploratory in nature. The issues raised certainly require further in-depth analysis.

1. The Schengen Information System (SIS)

The Schengen Information System (SIS)[2] is the oldest and most comprehensive large-scale database in the European Union. It was originally created as a compensatory measure to allow for the free movement of persons in the Schengen area. Furthermore it enhances cooperation and coordination between the police and the judicial authorities in order to safeguard internal security by countering illegal migration and fighting crime, namely organized crime.

It was operational from the entry into force in 1995 of the Convention Implementing the Schengen Agreement - hereafter Schengen Convention or CISA - until its replacement (on 9 April 2013) by the new information system

[2] For an overview of border control systems see Peers 2011.

SIS II,[3] which has more functions and allows the expansion of the original SIS to the new Member States.

The switch to SIS II occurred in response to two main issues: the inclusion of new Member States, which required a new IT infrastructure, and the need for new functionalities. The new system also involves changes in the supervision and management of the database. A coordinated structure of the national DPAs and the EDPS now supervises SIS II and has replaced the Schengen Joint Supervisory Authority (JSA), which supervised the Schengen Information System up to 2013.

The new European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) assumed the operational management of SIS II on 9 May 2013.

SIS II has a dual legal basis, formerly falling under the first and third EU pillars: a Decision (2007/533/JHA), which focuses on the use of the system for policing and criminal law purposes, and a Regulation (No. 1987/2006) that implements the rules on immigration matters.[4]

Its purpose "shall be to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the Treaty relating to the movement of persons in their territories" (Article 1, Regulation No. 1987/2006; Decision 2007/533/JHA). Compared to the purpose laid down in the Schengen Convention[5] the objective appears wider and more ambitious, moving forward from a largely administrative purpose for which the Schengen Information System had been established to one of a more general policy.

1.1 The data stored and the alerts

The SIS contains entries (called alerts) on objects or persons, according to the dual legal basis (Decision 2007/533/JHA and Regulation No. 1987/2006). Objects include: motor vehicles, boats, aircraft; firearms; stolen, misappropriated

---

3 For a critical view on the development of SIS II and the actors involved see Parkin 2011.

4 Another regulation is on the use of SIS II by vehicle registration authorities.

5 The general purpose of the Schengen Information System is described in Article 92 as: "the SIS shall enable the authorities (…) by means of an automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks". In the case of the specific category of alerts referred to in Article 96, the purpose is the issuing of visas, residence permits and the administration of legislation on aliens.

or lost official documents, identity papers, residence permits, travel documents, banknotes etc. (see Article 100, CISA; Article 38, Decision 2007/533/GAI).

Persons include:

- persons wanted for arrest for surrender or extradition purposes (Article 95, CISA; Article 26, Decision 2007/533/GAI);
- unwanted Third Country Nationals (Article 96, CISA; Article 24, Regulation No. 1987/2006);
- missing persons (Article 97, CISA; Article 32, Decision/2007/533/GAI);
- persons sought to assist with a judicial procedure (Article 98, CISA; Article 34 of Decision 2007/533/GAI);
- persons for discreet surveillance or specific checks (Article 99, CISA; Article 36, Decision 2007/533/GAI).

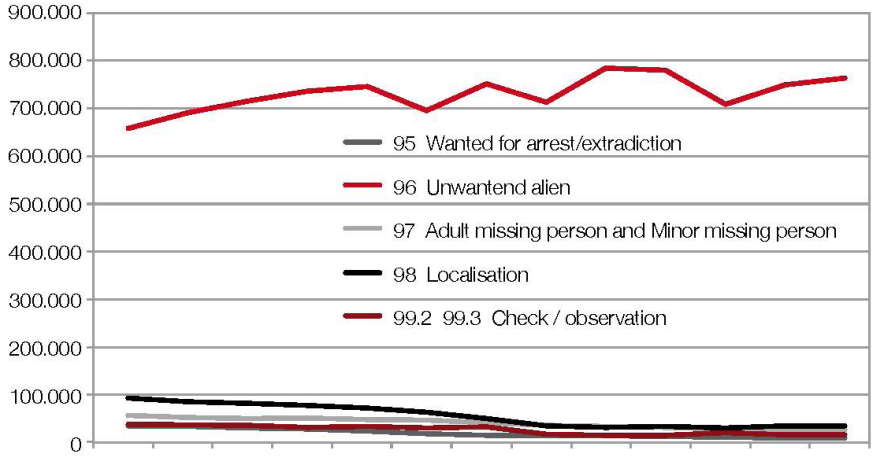
Over the last five years the number of alerts entered for persons has been about 900,000 per year (and more than 10 million for objects). The overwhelming majority of alerts on persons are in respect of unwanted Third Country Nationals. However, compared to 1999, the number of alerts issued under Article 24 of the Regulation has decreased and all those related to police investigation or judicial proceedings have increased.

Table No. 1 – Alerts issued according to type

Type of alert	01/01/13		01/01/10		01/01/07		01/01/03		1/1/1999	
	N.	%	N.	%	N.	%	N.	%	N.	%
Wanted for arrest/ extradition	35,919	4.05	28,666	3.08	16,047	1.79	14,023	1.60	10,491	1.23
Unwanted TCNs	659,347	74.43	736,868	79.27	752,338	84.08	780,992	88.99	764,851	89.36
Missing persons	57,302	6.47	52,319	5.63	42,500	4.75	32,211	3.67	27,436	3.21
Arrest in view of a judicial procedure	94,292	10.64	78,869	8.48	50,616	5.66	34,413	3.92	35,806	4.18
Discreet or specific checks	38,947	4.40	32,824	3.53	33,275	3.72	16,016	1.82	17,365	2.03
Total	885,807		929,546		894,776		877,655		855,949	

Source: own elaboration of EU Council data

Graph No. 1 – Issued alerts according to type



Source: own elaboration of EU Council data

In contrast to the original SIS, SIS II also contains biometric data (see table No. 2. below). The legal basis requires a specific quality check of biometrics to be determined according to an identified procedure. However, there are no common obligations or requirements related to biometric data.

Biometric data are currently only used to confirm the identity of a Third Country National who has been located as a result of an alphanumeric search in SIS II. As soon as this becomes technically possible, fingerprints may also be used to identify a person on the basis of the biometric identifier.

Before this functionality is implemented, the Commission shall present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted. But there will be no further vote on this new functionality. As soon as it becomes technically possible to compare the biometric data of an unidentified person with all the biometric data in the database (the so called "one to many" search), it will also be in compliance with the law (see Article 22 of the Regulation and of the Decision listed below).

Table No. 2 Data stored: evolution from the CISA to the present rules

CISA	Article 22 Regulation No. 1987/2006	Article 20 Decision 2007/533/GAI
(a) surname and forenames, any aliases possibly entered separately; (b) any specific objective physical characteristics not subject to change; (c) first letter of second forename; (d) date and place of birth; (e) sex; (f) nationality; (g) whether the persons concerned are armed; (h) whether the persons concerned are violent; (i) reason for the alert; (j) action to be taken.	a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately; (b) any specific, objective, physical characteristics not subject to change; (c) place and date of birth; (d) sex; *(e) photographs;* *(f) fingerprints;* (g) nationality(ies); (h) whether the person concerned is armed, violent or has escaped; (i) reason for the alert; (j) authority issuing the alert; *(k) a reference to the decision giving rise to the alert;* (l) action to be taken; *(m) link(s) to other alerts issued in SIS II in accordance with Article 37.*	(a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately; (b) any specific, objective, physical characteristics not subject to change; (c) place and date of birth; (d) sex; *(e) photographs;* *(f) fingerprints;* (g) nationality(ies); (h) whether the person concerned is armed, violent or has escaped; (i) reason for the alert; (j) authority issuing the alert; *(k) a reference to the decision giving rise to the alert;* (l) action to be taken; *(m) link(s) to other alerts issued in SIS II pursuant to Article 52; (n) the type of offence.*

* In Italics the new data included under the Regulation and under the Decision that were not included under the CISA.

As shown in the table, the two other new pieces of data included in the SIS II system, besides biometric data, are a reference to the decision giving rise to the alert and links between alerts.

The reference to the legal basis of the alert should make it possible to check its legitimacy more quickly. But the links between alerts are the most relevant and sensitive novelty. This functionality allows one alert to be associated with another. The sensitiveness of such links was well stressed in the EDPS opinion on SIS II: "Interlinking of alerts can have a major impact on the rights of the person concerned, since the person is no longer 'assessed' on the basis of data relating only to him/her, but on the basis of his/her possible association with other persons. Individuals whose data are linked to those of criminals or wanted persons are likely to be treated with more suspicion than others. Interlinking of alerts furthermore represents an extension of the investigative powers of the original SIS because it will make possible the registration of alleged gangs or networks (if, for instance, data on illegal immigrants are linked with data of traffickers)" (EDPS 2005). To give an example: an alert for an unwanted TCN could be linked to an alert for a stolen vehicle where the person was found. If there was another person in the car, these two persons would be linked by the alert on the vehicle.

The eu-LISA statistical report presents the composition of the SIS II database[6] on 31 December 2013. Italy is the country with the highest number of alerts entered into the system, followed by Germany (with less than ½ of the Italian alerts) and the Netherlands and Spain (with less than ¼ of the alerts). As regards persons, Italy and France have the highest numbers, followed by Germany and Greece.

Table No. 3 – Numbers of alerts by country

COUNTRY	Persons	Documents (issued and blank)	Vehicles	Licence plates	Firearms	Others*	Total
Italy	294,101	13,819,029	1,143,745	471,905	51,511	387,539	16,167,830
France	125,058	2,263,170	326,824	1	32,557	35,319	2,782,929
Germany	76,302	6,230,209	234,818	626,111	148,227	204,133	7,519,800
Spain	71,454	3,187,767	632,581	380	45,848	764	3,938,794
Greece	65,885	396,640	165,303	119,017	14,433	28,301	789,579
Poland	29,953	679,061	210,721	144,712	17,121	3,247	1,084,815
Switzerland	29,386	828,930	21,175		9,780	1,460	890,731
Austria	27,043	317,438	24,999	13,833	5,658	548	389,519
Netherlands	24,393	3,872,084	89,331	194	1,517	420	3,987,939
Portugal	20,147	87,385	57,204	1	9,369	10	174,116
Hungary	16,888	767,931	32,518	28,615	397	213	846,562
Czech Republic	14,462	2,443,655	81,988	113,524	16,989	153	2,670,771
Norway	14,161	129,777	7,009	6,669	1,493	746	159,855
Sweden	11,002	242,286	34,406	19	17,819	27	305,559
Belgium	10,450	2,494,023	56,863	184,119	36,234	4,229	2,785,918
Slovakia	7,370	718,799	20,657	12,510	4,424	44	763,804
Romania	6,587	1,329,120	7,343		537	17	1,343,604
Denmark	3,061	556,732	26,487	182	4,563	115	591,140
Finland	2,789	125,491	4,391	174	8,070	77	140,992
Malta	2,451	87,197	836	8	174	14	90,680
Lithuania	2,339	799,157	27,298	276,719	3,255	44	1,108,812
Estonia	1,574	339,518	2,442	2	254	0	343,790
Latvia	1,414	72,817	1,756	1,068	10	4	77,069
Bulgaria	1,247	955,647	22,302	121,554	61	0	1,100,811
Luxembourg	1,220	19,318	1,085	107	156	169	22,055
Slovenia	896	138,103	7,652	35,819	645	273	183,388
Liechtenstein	231	2,311	72	84	8	34	2,740
Iceland	36	15,736	3	1	11	0	15,787
Total	861,900	42,919,331	3,241,809	2,157,328	431,121	667,900	50,279,389

* The category "others" includes: aircraft, banknotes, boats, boat engines, containers, industrial equipment, licence plates, securities, vehicle registration documents.
Source: own elaboration of eu-LISA (2014b).

[6] Twenty-eight countries are connected to SIS II. Member States of the EU connected to SIS II are Austria, Belgium, Bulgaria, Czech, Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. Associated Countries connected to SIS II are Iceland, Norway, Switzerland and Liechtenstein. Moreover, the authorities of the United Kingdom, Ireland and Croatia are in the process of making preparations for their technical connection to SIS II.

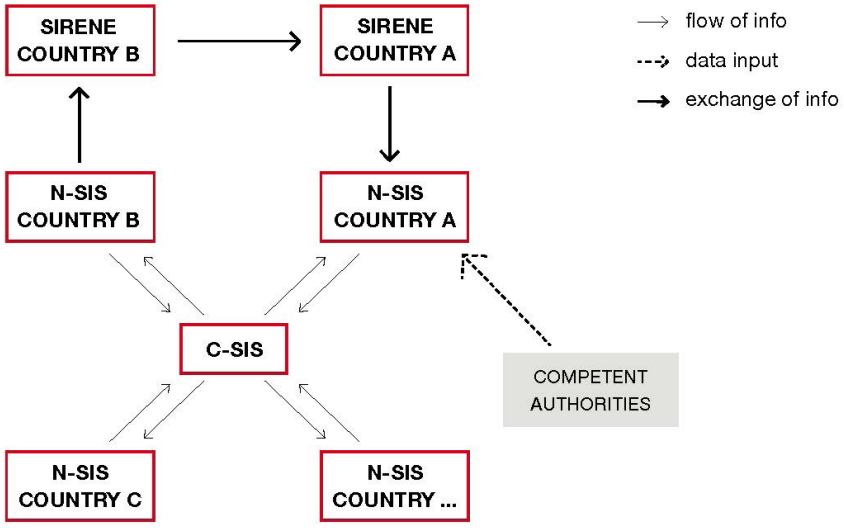
1.2 The architecture of the system and information searches

The system is an interconnection of a national database (N-SIS), via a secure communication infrastructure, with a central server in Strasbourg (C–SIS) that sends and receives data to and from the Member States (radial shape). Each Member State accesses the system through a common interface. The national database may contain a national copy of the data (Article 9 of the Regulation). However, this is not necessary. Access is guaranteed by the central system. During the interview, the SIS office clarified that in actual fact the biggest countries have a national copy for their own purposes.

When an alert needs to be entered, the N-SIS of a Member State sends the request to the central server. After checking the alert to verify its compliance with technical requirements, the C-SIS validates it and then enters it into both the national system and the C-SIS. Consequently the permanent updating of the central database and the uniformity of the national system are guaranteed. Each Member State adopts a security plan to guarantee the security of the system and if it has a copy of the data, the copy is under its own responsibility.

Information searches in each Member State only take place within that country's N–SIS. The authorities of a country cannot search the N-SIS of another one. An N-SIS Office in each Member State is responsible for the operational management of the N-SIS. In addition, an office (called SIRENE, Supplementary Information Request at the National Entry) is established to provide additional information. Member States exchange information through the respective national SIRENE offices.

Figure No. 1 – The circulation of information in the system



Source: own elaboration based on collected information

1.3 Right to access and retention period

Having outlined the architecture of the system and the types of data it contains, a subsequent important aspect is to define who is authorised to access the system and under which conditions. Access to the system refers to "a query – regardless of whether a hit is achieved or not – or to a transaction intended to create/update/delete (CUD) an alert. Every access is counted, even if an access resulted in an error and an error message was returned from the system (e.g. if the operator commits an error)" (eu-LISA 2014a). Access is granted on a "hit/no-hit" basis. The searched object or person can be entered as a search query in order to obtain a yes/no answer. If the response is positive and the alert has been issued by the country performing the search, additional information can be searched through national databases. If the alert has been issued by another country, the SIRENE office of the country that did the search will contact the SIRENE office of the country that issued the alert to ask for additional information (see figure No.1 above).

According to the rules set forth in Article 27 of Regulation No. 1987/2006 and in Article 40 of Council Decision 2007/533/JHA, the authorities that have access to the information entered in the SIS II must be identified by each Member State. As regards Third Country Nationals (TCNs), Article 27 of the Regulation gives the right to search data to the authorities responsible for the identification of TCNs for the purpose of border control and for other police and customs checks. In addition, the right to access data entered in SIS II is given to judicial authorities and to those issuing visas. In both cases access by these authorities is governed by national legislation.

The statistical report (eu-LISA 2014b) provides figures on the numbers of accesses from April to December 2013, distinguishing between manual and automated processes. As shown in the following table, few countries were able to provide separate figures for the number of manual and automated accesses. Belgium, Hungary, Malta, the Netherlands, Poland and Sweden reported not using any automated data processing systems. Some countries (Estonia, Spain, Italy, Austria, Romania, Slovenia, Norway, and Switzerland) reported that they use automated data processing systems to a certain extent but that they cannot separate the data. The table also reveals notable differences between the various countries. It is hard to entirely understand these differences. Several countries that do not insert many alerts appear to use the system a lot. Other countries, especially Italy, enter a large number of alerts but do not access the system as frequently as others. It is also reasonable to suppose that not all countries understand the meaning of automated processes in the same way as no common definition is provided at EU level. Moreover a high number of automated processes could be related to the use of automatic licence plate readers. This could explain the high figure in countries with intense road traffic, such as Germany.

Table No. 4 – Numbers of accesses to SIS II from April to December 2013

	Country	Manual processes	Automated processes	Total
1	SPAIN			**343,655,015**
2	GERMANY*	2,148,704	237,047,720	**239,196,424**
3	POLAND	128,744,291	0	**128,744,291**
4	ROMANIA			**64,593,255**
5	CZECH REPUBLIC	30,522,148	19,485,451	**50,007,599**
6	BULGARIA	3,038,194	45,266,498	**48,304,692**
7	SWITZERLAND			**43,028,560**
8	FRANCE	38,869,603		**38,869,603**
9	FINLAND	23,532,727	14,604,394	**38,137,121**
10	AUSTRIA			**37,623,689**
11	HUNGARY	36,161,651	0	**36,161,651**
12	NETHERLANDS	33,286,351	0	**33,286,351**
13	ESTONIA			**28,477,900**
14	ITALY			**25,229,296**
15	SLOVENIA			**23,897,408**
16	GREECE	21,982,593	1,473,291	**23,455,884**
17	LITHUANIA	22,559,080		**22,559,080**
18	LATVIA	14,681,460		**14,681,460**
19	SWEDEN	13,887,614	0	**13,887,614**
20	PORTUGAL**	6,988,878		**6,988,878**
21	BELGIUM	6,968,088	0	**6,968,088**
22	SLOVAKIA	3,903,002	1,449,740	**5,352,742**
23	NORWAY			**4,728,876**
24	DENMARK	2,727,000	1,500,000	**4,227,000**
25	MALTA	1,053,529	0	**1,053,529**
26	LUXEMBOURG	241,116	269,914	**511,030**
27	ICELAND	292,192	179,121	**471,313**
28	LIECHTENSTEIN	106,801	307,320	**414,121**

*Partial data, for CUDs only alerts and flags are counted ** Figures only for the second semester 2013

Source: eu-LISA (2004b)

The retention period is limited to the time required to achieve the purposes for which the alert was entered. In addition, the Member State has a duty to review the need to keep the alert after three years. A Member State "shall, where appropriate, set shorter review periods in accordance with its national law" (Article 29, Regulation No. 1987/2006).

1.4 Implementation in Italy[7]

The authorities in charge of the Schengen Information System are the SIS Office and the SIRENE Office. In Italy these two offices are located at two different branches of the Public Security Department of the Ministry of the Interior.

The N-SIS Division is a branch of the *Ufficio Coordinamento e Pianificazione delle Forze di Polizia* (Coordination and Planning Office of the Police Forces). This Office performs several tasks, aimed at increasing the efficiency of the police forces and improving cooperation between them in Italy and between the Italian law enforcement offices and those of foreign countries.

The SIRENE Office is located at the *Direzione Centrale per la Polizia criminale* (Central Directorate of the Criminal Police). This Central Directorate coordinates police investigations at the national level, collects and analyses data on criminal phenomena and is in charge of the international cooperation with foreign countries aimed at fighting organised crime.

1.4.1 The interface

The police forces may access the SIS II database through the native interface or the SDI (*Sistema Di Indagine*) interface, which is the national police information system. Access is more frequent through the SDI because this is the commonly used police information system and offers more functionality than SIS II. The two databases are hosted on different servers but users can access the data in SIS II through the SDI interface, provided they have the appropriate privileges. Accessing the SDI and SIS II involves different authorisation procedures, and the authorisation of users to access SIS II is an exclusive competence of the N-SIS office. When law enforcement officers access the SDI interface, either to process or consult an alert, they enter or search the relevant information in the SDI and the system is able to link the information that has been entered or the search queries to the SIS II database. Thus, if the information entered in the SDI is relevant for the Schengen Information System, it is automatically copied in the SIS II databases. If the person or object searched in the SDI is also present in the SIS II, a link to the SIS II alert appears. This happens if the officers searching the system have the required level of authorisation, otherwise no information appears. SDI and SIS II are interoperable as described in case of queries. For the operations of creation, update or deletion of an alert the two databases are interoperable only for objects and not for people.

---

[7] The main sources of this part are the interviews carried out during the fieldwork.

The flow of information is different if the alert has been issued by another country. When the officers need more information besides that included in the alert, they must contact the SIRENE Office of their own country and request an exchange of information.

1.4.2 The issuing of alerts under Article 24 of the Regulation

The reasons for issuing an alert differ from one Member State to another. Reports by the JSA[8] and the 2013 eu-LISA report show a high level of discretion among Member States in issuing alerts. This is because Article 24 of the Regulation (and previously Article 96 of the CISA) provides the general framework but also allows National States considerable discretion.

Article 24 provides for the issuing of an alert in two situations: when a TCN has been subject to a measure involving expulsion, refusal of entry or removal that is accompanied by a re-entry ban and when a TCN could represent a threat based on the fact that s/he has been convicted in a Member State of an offence carrying a custodial sentence of at least one year or there are serious grounds for believing that s/he has committed (or intends to commit) a serious criminal offence.

National immigration laws regulate several aspects of expulsion and refusal of entry. Moreover, penalties for crimes or the reasons why a person could be defined as a threat to public policy or public security are a matter of State sovereignty. This results in different methods of enforcement across Member States. In Italy, the local Police authorities we interviewed affirmed that the alerts envisaged under Article 24(2) had never been implemented and that they had only ever issued alerts based on Article 24(3) (see table below).

---

[8] Over the years, the JSA has carried out several inspections on the implementation of The Schengen Convention. See http://schengen.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

Table No. 5 – Rules on the issuing of the alert for unwanted TCNs.

Article 96 Schengen Convention	Article 24 Regulation No. 1987/2006	Article 10 Legislative Decree No. 286/1998[9]
1. Data relating to aliens who are reported for the purposes of being refused entry shall be included on the basis of a national report resulting from decisions taken, in compliance with the rules of procedure laid down by national legislation, by the administrative authorities or courts responsible. 2. Decisions may be based on a threat to public order or national security and safety which the presence of an alien in national territory may pose. Such may in particular be the case with: (a) an alien who has been convicted of an offence carrying a custodial sentence of at least one year; (b) an alien who, there are serious grounds for believing, has committed serious offences, including those referred to in Article 71, or against whom there is genuine evidence of an intention to commit such offences in the territory of a Contracting Party. 3. Decisions may also be based on the fact that the alien has been the subject of a deportation, removal or expulsion measure which has not been rescinded or suspended, including or accompanied by a prohibition on entry or, where appropriate, residence, based on non-compliance with national regulations on the entry or residence of aliens.	1. Data on third-country nationals in respect of whom an alert has been issued for the purposes of refusing entry or stay shall be entered on the basis of a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law taken on the basis of an individual assessment. Appeals against these decisions shall lie in accordance with national legislation. 2. An alert shall be entered where the decision referred to in paragraph 1 is based on a threat to public policy or public security or to national security which the presence of the third-country national in question in the territory of a Member State may pose. This situation shall arise in particular in the case of: (a) a third-country national who has been convicted in a Member State of an offence carrying a penalty involving deprivation of liberty of at least one year; (b) a third-country national in respect of whom there are serious grounds for believing that he has committed a serious criminal offence or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a Member State. 3. An alert may also be entered when the decision referred to in paragraph 1 is based on the fact that the third-country national has been subject to a measure involving expulsion, refusal of entry or removal which has not been rescinded or suspended, that includes or is accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of third-country nationals.	1. The border police may refuse entry to foreigners who arrive at border posts without the legal requirements foreseen by this law. 2. The refusal of entry is also ordered by the police authority for foreigners: a) who are stopped at an entry point or immediately after entering the territory of the State while avoiding border controls; b) who while being in the circumstance provided for under paragraph No.1, have been temporarily admitted on the grounds of public assistance needs. 3. Should a carrier transport a foreigner to the national border without the required documents to enter the country, or a foreigner who must in any case be rejected, that carrier shall assume responsibility for immediately accompanying the foreigner back to the country that he or she came from. 4. The measures provided for by article 10 commas 1,2,3 and article 4 commas 3 and 6 do not apply in those cases envisaged by the existing provisions regulating political asylum, recognition of refugee status or the adoption of measures of temporary protection for humanitarian reasons. 5. The rejected foreigner shall be granted due assistance at national borders. 6. All rejections shall be recorded by the border police.

[9] Decreto legislativo no. 286/1998 Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero. Legislative Decree No. 286/1998 Cosulated text of provisions on immigration legislation and norms on the foreigner status . Translation is by the author.

In Italy, the only authority that can issue alerts in accordance with Article 24 of Regulation No. 1987/2006 is the Immigration Office of the local Police Headquarters.[10] This office is responsible for issuing the alert, and for its subsequent deletion or any amendments as required.

In Italy the reasons for issuing an alert ensue from the implementation of the rules set forth under EU Regulation No. 1987/2007, the Return Directive 2008/115/EC as transposed into Italian law and Italian immigration laws. There is no national legal text that clarifies the reasons for issuing a SIS II alert. This complex legal framework made up of different European instruments and Italian legal rules is therefore subject to the interpretation of the local offices.

As regards alerts based on a removal measure (Article 24(3) Regulation), Italian immigration law does not provide for the issue of an alert as a consequence of a refusal of entry (Article 10 Legislative Decree No. 286/1998). This is because in the Italian legislation there is no ban on re-entry following a refusal of entry measure. In contrast, expulsion decisions are always accompanied by a ban on re-entry and consequently an alert is always issued. This difference in the rules is problematic, since Italian Immigration law envisages a specific type of refusal of entry, namely delayed refusal of entry, which is difficult to distinguish from expulsion.

Article 10 Legislative Decree No. 286/1998 provides for refusal of entry to migrants who are not entitled to stay within the territory of the Italian State. Delayed refusal of entry applies when migrants have avoided border controls and have been stopped upon entry or immediately after entering the country or are entitled to enter temporarily in order to be rescued. This is often the case with people entering Italy via Lampedusa or other areas of Sicily.[11] This last reason for delayed refusal of entry overlaps with one of the reasons for expulsion — envisaged under Article 13(1)(a) Legislative Decree No. 286/1998 — in cases where migrants have entered avoiding border controls and have not been removed.

In actual fact, regardless of whether the persons were rescued or landed on their own, the authority has full discretionary power to choose between expulsion and delayed refusal of entry. The two procedures differ significantly; for the purposes of this discussion, expulsion implies the issue of a Schengen Information system alert whereas delayed rejection at the border does not.

---

[10] Each province in Italy (there are 110 in all) has a police headquarters ("*Questura*"). Every Immigration office is responsible for the administrative decisions taken in respect of Third Country Nationals resident or present within the territory of the province.

[11] Since the insurgence of the political crisis in the regions of North Africa, Italy has experienced a significant rise in the number of undocumented immigrants arriving from the coasts of North Africa by boat. Lampedusa and other areas in Sicily are the main places of arrival.

If a case requires the issuing of an alert, Article 24(1) of the Regulation states that the decision to issue the alert has to be taken "on the basis of an individual assessment" (see table No. 5 above). This means that the authorities must always assess the concrete circumstances and evaluate whether or not the case warrants the issuing of a Schengen Information System alert (see Brouwer 2008b, Peers 2011). On the other hand, this could be interpreted as meaning that the issuing of one alert for a group of people based on a collective decision (e.g., a collective expulsion order) is prohibited.

According to the lawyers interviewed, alerts are, however, issued automatically after an expulsion order. The authorities interviewed confirmed this. The existence of an expulsion order is a necessary and sufficient condition for issuing an alert.

In addition, Article 21 of the Regulation states: "Before issuing an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant entry of the alert in SIS II". In practice, this proportionality assessment does not take place, since there is no discretionary power to issue an alert as a consequence of an expulsion order.

Both the individual assessment requirement and the proportionality clause therefore do not work as limitations for entering alerts in respect of TCNs. The issuing of the alert appears to be the consequence of a highly routinized procedure.

The retention period of alerts based on a removal measure (Article 24(3) of the Regulation) is calculated according to the length of the entry ban. In the interview the SIS office underlined that the retention period is calculated from the day on which the TCN leaves the Schengen territory (not just that of Italy). Thus, if there is no proof that the migrant has left the territory, the alert is maintained and renewed. This could partially explain the high number of alerts on persons in Italy.

1.4.3 Access to the database by the authorities

Access to the database depends on the type of alert and level of authorisation of the respective authority. All five Italian law enforcement bodies have access.[12]

---

[12] In Italy there are five national police forces under gouvernment control. Two are military police (Carabinieri and Guardia di Finanza) and three are civilian police (Polizia di Stato, Polizia Penitenziaria and Corpo Forestale dello Stato). The Polizia di Stato (State Police) is under the authority of the Ministry of Interior – Department of Public Safety, whereas the Carabinieri is under the authority of the Ministry of Defence. Both are organised on a territorial basis and they have patrolling, investigative and law enforcement duties. The other three police forces have specific duties: the Guardia di Finanza (under

The city police only have access to vehicle registration data. The Foreign Affairs Ministry has access with the restriction described in Article 27(3) of the Regulation.

There is no national legislation regulating access to the databases. Decrees of the Chief of the Police establish who has access to the database. These are administrative acts, circulated internally. The list of authorities that have access to the database is not published but, in accordance with Article 31 of Regulation 1987/2006, it must be sent to the eu-LISA, which will ensure its annual publication in the Official Journal of the EU[13].

According to the authorities interviewed, there are 140,000 accounts with access to the Schengen Information System. Each access account refers to a name but not to a specific IP address; this means that the same person can have access from different computers. Data are not downloadable.

1.4.4 The right to information and the right of access, correction and deletion

According to Article 42 of the Regulation, Articles 10 and 11 of the Directive 95/46/EC regulate the right to be informed when an alert has been issued in respect of Third Country Nationals for the purpose of refusing entry and stay, but there are some specific exceptions. The information must not be provided if the personal data have not been obtained from the TCNs or when provision of the information would involve a disproportionate effort or proves impossible. Moreover there is no right to information when the Third Country National already has the information or where "national law allows for the right of information to be restricted, in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offence". This leaves the doors open to a wide interpretation of these exceptions by the Member States. All the lawyers interviewed agree that most TCNs do not know anything about the alert, but they usually understand the meaning of the re-entry ban. Moreover, the

---

the authority of the Ministry of Economy and Finance) deals with prevention and prosecution of currency, financial and tax related offences; the Polizia Penitenziaria (under the authority of the Ministry of Justice) is responsible of the management of penal facilities and correctional programs; the Corpo Forestale dello Stato (under the authority of the Ministry of Agriculture) has some specific competences for the environmental management of open spaces and national heritage. The Ministry of Interior, which is the branch of the government in charge of public security control, has authority over all the police forces.

13 The list of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information has been published in the Official Journal 2014 C 278, pp. 1-144, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2014:278:FULL&from=EN.

information "shall be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert" (Article 42(1) Regulation). According to the lawyers and the immigration officers interviewed, Third Country Nationals receive a copy of the decision that states the length of the re-entry ban but provides no specific information about the Schengen Information System alert.

Both Article 109 of the CISA and Article 41 of the Regulation provide for the right of access, correction and deletion. The Italian Data Protection Act (Legislative Decree No. 196 of 30 June 2003) also establishes the rules for exercising these rights. The procedure is explained on the websites of the Ministry of the Interior and of the DPA.[14]

Since 1 January 2004 the right of access, correction and deletion has been exercised directly through the Ministry for Home Affairs – Public Security Department – SIS Office. Prior to that date, the data subject could exercise these rights through the Data Protection Authority, which had the duty to request information from the Ministry for Home Affairs. According to the lawyers interviewed, lawyers exercise the right of access when they need to know if the existence of an alert is hampering the possibility for the Third Country Nationals involved to receive a visa or a residence permit. Immigration lawyers seem not to consider data protection as a right that needs to be protected in itself. If the answer provided is unsatisfactory, data subjects may lodge a complaint with the Data Protection Authority. No complaint has ever been processed by the DPA.

According to the authority interviewed, the duty of information is the responsibility of the local authorities that issue the alert. The information is not centralised. The interviewees revealed that information about data protection aspects is almost never given. Expulsion orders always include information on the length of the ban on entry but nothing is written on the issue of a Schengen alert.

In the experience of the lawyers, foreign nationals are rarely aware of the issued alert. It is difficult to say whether this is due to their not being informed, or whether they were informed but did not realise the content of the information they were given or perhaps simply forgot it.

In addition, the lawyers reported a lack of information when an alert is deleted. When they ask for an alert to be deleted they are not always informed that it has been erased. In practice, what happens is that the foreign national receives the residence permit that could not previously be issued because of the alert.

---

[14] The websites are available in Italian and English. See http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/servizi/come_fare/banca_dati_delle_forze_di_polizia/dati_schengen.html; http://www.garanteprivacy.it/home/attivita-e-documenti/attivita-comunitarie-e-internazionali/cooperazione-in-ambito-ue/schengen.

Consequently it is clear that the alert must have been cancelled or expired, although the lawyers did not receive any official communication in that respect.

1.4.5 The interlinking of alerts

The interlinking of alerts is a useful tool for policing purposes because it permits the identification of associations between persons or persons and objects, such as documents or vehicles. Consequently, the authorities can take action based not only on single persons but on their link to alerts issued for other people or objects. This appears to be a particularly sensitive issue for a database such SIS, which has a broad scope and a large number of alerts related to different reasons.

The purpose of an alert of a TCN as provided for under Article 24 should be limited to immigration control and the fight against illegal migration. In practice, linking two alerts adds a new and different purpose to the alert, compared to that for which it was originally issued: TCNs involved are now also targeted as "persons of interest" for investigative reasons. This appears to go beyond the scope of the alert *ex* Article 24. According to Article 37 of the Regulation, the link is based on national law and it should be used "when there is a clear operational need".

The authorities at the central level underlined that this new functionality represents an investigative lead, but this does not in itself imply that there is "a clear operational need" to use SIS II in this way also as a database for policing purposes. There is a grain of truth in the statement, but this does not alter the fact that the data of thousands of undocumented migrants are in the database and can be used for other purposes, completely unrelated to that for which they were originally included, and thus affecting many people for whom there is no particular suspicion that they are involved in crimes.

Moreover, there are no legal rules on the criteria for issuing a link. The N-SIS only provides an operational manual that explains the meaning and the technical aspects of the alerts. This gives wide discretionary powers to the police authorities.

One of the two local immigration officers interviewed affirmed that they do not implement links or enter fingerprints into the database. However, this does not mean that the law enforcement officers do not collect these data. Fingerprints are included in other national databases. For example, the national AFIS database (Automated Fingerprint Identification System) stores fingerprints of all TCNs who apply for a residence permit, who are expelled and who are convicted of a crime. Moreover, the SDI database, which allows the addition of links and has more functionalities than SIS II, is used by the Italian police on a daily basis. It could therefore be argued that the full enforcement of a database that is more relevant at the international than at the domestic level is not yet regarded as a priority by some local police authorities.

2. Eurodac

Eurodac is the oldest EU biometric database. It was established in 2000 (Regulation No. 2725/2000) and became operational in 2003. Since then several proposals have been enacted by the Commission to comply with modifications in the common European asylum system and to extend access to new authorities. The present Regulation (No. 603/2013) is a revised version that takes these changes into account. It will come into force on 20 July 2015.

The original purpose was to help to establish which Member State is responsible, in accordance with the Dublin Convention, for the reception of asylum applications. Eurodac was introduced to avoid so-called "asylum shopping", i.e. the risk that applicants submit several applications or travel across Europe in order to choose the Member State they prefer.

The 2013 Regulation adds a new purpose, described as follows: "This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the Central System for law enforcement purposes" (Article 1(2), Regulation No. 603/2013)". This will be discussed later on.

As for SIS II, the new European Agency eu-LISA is now in charge of the operational management of the database. Changes have also been made to the supervisory authority, which will bring it in line with the structure envisaged for SIS II. When the new Regulation comes into force, the Eurodac Supervision Coordination Group (composed of representatives from the DPAs of each of the participating states and the EDPS) will be replaced by the EDPS that will supervise all the data processing activities concerning the Eurodac. National DPAs will supervise the processing of data within the Member States.

2.1 The architecture of the system

The system consists of a computerised central fingerprint database ("Central System") and a communication infrastructure between the Central System and Member States, which provide an encrypted virtual network dedicated to Eurodac data. Each Member State has a single national access point. In Italy the authority in charge of Eurodac is the *Direzione Centrale Anticrime – Servizio di Polizia scientifica* (Central Department of the Forensic Police). At the sub-national level there are fourteen branches (*Gabinetti Regionali di Polizia Scientifica* – regional offices of the Forensic Police) which are the Eurodac focal points.

Data are entered into the system by the 14 focal points within the Italian territory through the national AFIS interface. This means that communicating with the central system is possible only from the central unit in Rome. In the

local branches, the fingerprints inserted locally are sent to the national AFIS system for searches, and then AFIS gets back in real time with a list of possible matches. In the case of a hit, the central office in Rome enters the new data in Eurodac. And if there is no hit, a new file is created in AFIS. Then, the central office in Rome inserts the new fingerprints in the Eurodac system.

When hits occur (i.e. the fingerprints are already in the system because the person has already asked for asylum in another Member State), the Member States involved are likely to exchange additional data via a system called 'DubliNet'. The data that are exchanged include the individual's name, date of birth, nationality, photos, and even information about his/her family and address.

2.2. Types of data stored and retention period

The new Regulation, like the previous one, defines three categories of people whose data can be stored in the system:

- Category 1: applicants for international protection over 14 years old;
- Category 2: TCNs or stateless persons over 14 years old apprehended in connection with the irregular crossing of an external border;
- Category 3: TCNs or stateless persons over 14 years old found illegally staying in a Member State, with the aim of checking whether the data subject has previously lodged an application for asylum in another Member State.

The data stored are specific for each category and the retention period varies. The table below summarises the new provisions, which contain just a few changes compared to the previous Regulation.

Table No. 6 – Data stored in Eurodac

	Category 1	Category 2	Category 3
Data stored	- fingerprint data (all ten fingers) - MS of origin, place and date of the application for international protection - sex - reference number used by MS of origin - date on which the fingerprints were taken - date on which the data were transmitted to the Central System - *operator user ID* - *dates related to transfers, removals or other specific movements of the persons according to Article 10**	- fingerprint data (all ten fingers) - MS of origin, place and date of the application for international protection - sex - reference number used by MS of origin - date on which the fingerprints were taken - date on which the data were transmitted to the Central System - *operator user ID**	No data storage. Fingerprint data may be transmitted to the Central system in order to check whether a person has previously lodged an application for international protection
Transmission of data to the Central System	Within 72 hours + additional 48 hours in specific cases *(under the previous Regulation there were no rules)*		Within 72 hours + additional 48 hours in specific cases (under the previous Regulation there were no rules)
Retention period	10 years from the date the fingerprints were taken	18 months *(under the previous Regulation it was 2 years)*	data shall not be recorded
Erasure of data	As soon as the State becomes aware of: - acquisition of citizenship;	As soon as the State becomes aware of : - acquisition of citizenship; - issuing of a residence permit; - departure from the MS	N.A.
Marking of data	*When a MS grants international protection, the applicant's record will be marked. The marked data will be available for three years for law enforcement purposes, as laid down in Article 1(2). Upon the expiry of the three year period the data will be blocked and then erased, when the retention period expires.*		

* Info in italics was not included in the previous Regulation.

Source: Own elaboration of legal texts.

As the table above shows, under the new Regulation, when TCNs receive international protection,[15] their data are not erased but marked so that they can be used for law enforcement purposes for three more years. Under the previous regulation, data of persons recognised as refugees[16] were blocked and hits concerning them were not transmitted. As soon as the retention period expired, the data were erased. The regulation made no provision for asylum seekers who were recognised as beneficiaries of subsidiary protection.

Allready stated, data are entered in the system by the 14 focal points within the Italian territory through the national AFIS-interface (Automated Fingerprint Identification System). Due to the specificity of recent immigration flows, this activity is most extensively performed by the focal points in the South of Italy, mainly in Sicily, where the number of people apprehended while unlawfully crossing the country's border is highest. Since the beginning of the recent operation called Mare nostrum[17] migrants' fingerprints have also been taken immediately on board of the search and rescue ships. Live scan fingerprints is the technology used in the offices and on board of ships.

As shown in the table below, at the end of 2013 2,378,008 data sets were stored in the Eurodac Central System. Data differ between countries due to geographic or geopolitical reasons (see the high number of Category 2 data in Italy and Greece) and rules on granting residence permits and citizenship that allow erasure. Moreover, as underlined in the 2013 Eurodac annual report, levels of blocked data vary among Member States, several of which are working in order to comply with the Regulation[18] (eu-LISA 2014a, 11). In fact the number of data sets that were blocked increased from 16,573 in 2012 to 56,013 in 2013.

---

15 Under the new Regulation this rule applies to any type of international protection (from refugee to subsidiary protection).

16 There were no rules for other types of international protection. Consequently the data remained in the system.

17 See http://www.marina.difesa.it/EN/operations/Pagine/MareNostrum.aspx.

18 The report underlines: "In several cases (in Cyprus, Denmark, France, Greece, Iceland, Latvia, Malta, Norway and Slovakia) fewer than 10 data sets had ever been blocked since Eurodac became operational in 2003, whilst in Germany, Sweden and the UK the figure was in the tens of thousands. In most cases where very few data sets had been blocked, the Member States informed the Commission that they intended to undertake projects to apply the Eurodac Regulation correctly in future as well as to conduct retrospective corrections. France informed the Commission that they would need to block around 110,000 cases, which would require a fifteen-month project to complete. Having each blocked 0 cases in 2012, in 2013 Belgium blocked 8,072 data sets, Cyprus blocked 15, France blocked 4,417, Greece blocked 76 and Norway blocked 16,640 (which, they explained to the Commission, included historic cases that had previously not been blocked). Slovenia blocked 91 and Slovakia blocked 59 – both appearing to have resolved their previous problems concerning the blocking of data" (eu-Lisa 2014a, 11).

Table No. 7 - Numbers of data sets in Eurodac on 31.12.2013

	Category 1	Category 2	Blocked Category 1
FRANCE	359,742	796	4,247
GERMANY	334,535	122	19,405
UNITED KINGDOM	256,692	456	29,712
SWEDEN	219,594	0	23,408
ITALY	189,400	33,883	3,208
BELGIUM	152,615	16	7,972
GREECE	121,315	28,888	76
AUSTRIA	118,177	197	7,463
NETHERLANDS	90,384	30	4,714
SWITZERLAND	82,625	4	5,897
NORWAY	76,601	89	16,558
POLAND	52,128	48	556
SPAIN	32,895	7,645	489
HUNGARY	32,659	1,688	302
CYPRUS	30,272	52	14
FINLAND	24,687	7	1,062
DENMARK	22,953	0	0
IRELAND	21,666	8	966
SLOVAKIA	16,187	64	59
CZECH REPUBLIC	14,935	0	434
BULGARIA	10,217	9,856	12
ROMANIA	8,419	52	622
MALTA	8,096	58	70
LUXEMBOURG	7,652	2	9
SLOVENIA	3,793	48	98
LITHUANIA	2,122	5	57
PORTUGAL	1,632	1	29
LATVIA	784	0	0
ICELAND	478	0	0
CROATIA	335	38	0
ESTONIA	283	1	32
LIECHTENSTEIN	81	0	0
TOTAL	**2.293.954**	**84.054**	**127.471**

Source: eu-LISA 2014a

Besides the above-mentioned changes, there are some relevant new provisions regarding the rights of data subjects and the rights of law enforcement authorities to access data.

2.3 The rights of law enforcement authorities to access data

For the new purposes that have been added under the 2013 Regulation, in 2015 Europol and the law enforcement authorities of the Member States will have access to the database for comparing fingerprint data with the data stored in the Central System. According to Article 20, Member States' law enforcement authorities can only gain access if the search in other databases did not lead to the establishment of the identity of the data subject. The mentioned databases are national fingerprint databases, other Member States' databases, accessible through the network of national DNA databases established by the Prüm Decision (2008/614/JHA) and the Visa Information System (VIS) database.

In addition, access has to be:

1) "necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences" which means that there is "an overriding public security concern which makes the searching of the database proportionate";

2) "necessary in a specific case", which means that systematic comparisons are not allowed;

3) based on reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.

As outlined in the table above, this right of access includes the right to access the fingerprints of people granted recognition as asylum seekers for three years.

The law enforcement authorities with power to access such data are designated at Member State level and, according to Article 5 of the 2013 Regulation, must be authorities that are "responsible for the prevention, detection or investigation of terrorist offences or other serious criminal offences".

2.4 The rights of the data subject

Article 29 of the 2013 Regulation establishes the rules governing the rights of the data subject. It replaces Article 18 of the 2725/2000 Regulation, adding some new obligations for data controllers. This is a consequence of the findings of the inspection carried out by the Eurodac Supervision Coordination Group in 2009. The inspection identified a need for a general improvement in the

quality of information given to the data subject. In particular, it reported that asylum seekers (Category 1) are provided with better information than illegal border crossers (Category 2). Some Member States give information in writing, others only orally. Information on data protection is generally included in the information regarding the whole asylum procedure, and no attention is paid to providing this information in an accessible and understandable language. Finally the moment the information is given differs among Member States (see Eurodac Supervision Coordination Group 2009).

In Italy, the leaflet refers to the provisions under Article 18 of Council Regulation (EC) No. 2725/2000, and specifies the data controller, the purpose for which his/her data will be processed in Eurodac, and the right of access to data. Moreover, the authority responsible for the information to be given to the person whose fingerprints are taken is the Central Directorate for Immigration and Border Police, Border and Immigration Police Service, and to be more precise, the Police Headquarters (Questura) at local level. It is not the Forensic Police to be responsible for these aspects. However, it is worth noticing that none of the interviewed lawyers have ever seen the leaflet, not even once.

The 2000 Regulation did not set out any rules on the form of information, whereas the 2013 Regulation stipulates that a person must be informed "in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand". Moreover a common leaflet, clear and simple, written in a language that the person concerned can understand (or is reasonably supposed to understand) has to be drawn up in such a manner as to enable Member States to complete it with additional Member State-specific information.

The content of the information given and the right to access, correct and delete data are the same as those envisaged under the 2000 Regulation. It is worth underlining that the above-mentioned inspection report refers to very few requests to access data submitted by data subjects. Moreover it stated that "in general the countries where such requests are being presented are the same ones in which the information which is being provided to data subjects is deemed to be complete, adequate and in compliance with Eurodac Regulation" (Eurodac Supervision Coordination Group 2009, 15). During the interview, the Italian DPA stated that they have never received any requests.

2.5 Successful transactions and hits

The annual report on the activities of Eurodac shows the number of so-called successful transactions, namely data transactions, which have been correctly processed, without rejection due to a data validation issue, fingerprint errors or insufficient quality.

This number represents the times a Member State has sent fingerprint data to the system and the data were successfully processed by the system. As the table clearly shows, the use of Eurodac increases, albeit not steadily. However, in the last 3 years the number of transactions has grown significantly.

Table No. 8– Successful transactions from 2003 to 2013

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Cat. 1	246,902	232,205	187,223	165,958	197,284	219,557	236,936	215,463	275,587	285,959	354,276
Cat. 2	7,857	16,183	25,162	41,312	38,173	61,945	31,071	11,156	57,693	39,300	48,276
Cat. 3	16,814	39,550	46,299	63,341	64,561	75,919	85,554	72,840	78,753	85,976	106,013
Total	**271,573**	**287,938**	**258,684**	**270,611**	**300,018**	**357,421**	**353,561**	**299,459**	**412,033**	**411,235**	**508,565**

Hits indicate matches. When a hit occurs it means that the searched fingerprints were already in the system. There are three categories of hits:

- Cat. 1 against cat. 1, asylum seekers' fingerprints against asylum seekers' fingerprints. This shows how many migrants have repeatedly applied for asylum in the same country (local hits) or in another one (foreign hits);

- Cat. 1 against cat. 2, asylum seekers' fingerprints against those of persons apprehended while irregularly crossing an external border. This shows how many persons who irregularly crossed the border later lodged an asylum application and where they did so;

- Cat. 3 against cat. 1, fingerprints of irregular migrants found in a Member State against asylum seekers' fingerprints. This shows how many irregular migrants previously requested asylum and where.

According to the data published by eu-LISA (2014a), Italy is the country with the highest number of hits. This means that when other countries enter fingerprints and find a match, the data are already in the system because the same fingerprints have already been entered by Italy.[19]

[19] 10 % of the hits on cat. 1 against cat. 1 and on cat. 3 against cat. 1 and about 50% of hits on cat. 1 against cat. 2 are Italian.

3. Current and forthcoming developments

Several databases and information-sharing schemes are currently under implementation or discussion, besides SIS II and Eurodac. All of these instruments have a twofold objective: to improve border management and counter serious crime. None of them have the exclusive aim of border control (with the sole exception of API, the Advanced Passenger Information system). Almost all of them have multiple purposes, either from the outset or having acquired more purposes during their development or implementation, and are aimed at managing borders, fighting serious crimes and enhancing judicial cooperation. Some of the schemes involve exchange of data with third countries, others explicitly forbid this exchange.

It is beyond the scope of this research to provide an overview of all of these, but it is worth underlining the main features of some of them, as they have many characteristics in common with SIS II or Eurodac or are closely linked to the Italian context.

The first database, already in an advanced phase of implementation, is the Visa Information System (VIS),[20] which allows the exchange of data between Member States on short-stay visas. Like SIS II and Eurodac, the architecture of this system is composed of a central database, a national interface and a communication infrastructure between the Central VIS and the national interfaces. In particular SIS II and VIS share the same communication system and system for processing biometric data. Operational management is performed by eu-LISA. The EDPS and the respective national DPAs supervise the system.

The VIS has a very broad purpose. It aims to improve the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and decisions, in order to:

(a) facilitate the visa application procedure;

(b) prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application (i.e. asylum shopping);

(c) facilitate the fight against fraud;

(d) facilitate checks at external border crossing points and within the territory of the Member States;

---

[20] VIS has a dual legal basis, formerly falling under the first and third pillars: Regulation No. 767/2008, concerning the exchange of data between Member States on short-stay visas and Council Decision 2008/663/JHA concerning access by several authorities for the purposes of preventing, detecting and investigating terrorist and other criminal offences.

(e) assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or reside in the territory of the Member States;

(f) facilitate the determination of the Member State responsible for an asylum application lodged in one of the Member States;

(g) contribute to the prevention of threats to the internal security of any of the Member States (see Article 2, Regulation No. 767/2008).

It clearly links the implementation of the common visa policy with security interests of the EU and its Member States.

The database contains ten fingerprints,[21] as does Eurodac, and a digital photograph of the visa applicant along with data provided in the visa application form.[22]

Visa authorities are the only authorities allowed to enter the relevant information but a wide range of authorities can have access for consultation (from the border control authorities and those performing checks within the country to the designated authorities of the Member State for the purposes of the prevention, detection and investigation of terrorist offences or other serious offences). Searches may be performed for the purposes of verification and identification. Verification consists of checking that the fingerprints scanned at the border crossing point correspond to those associated with the biometric record attached to the visa. Identification consists of comparing the fingerprints taken at the border crossing post with the contents of the entire database.

Similarly to SIS II and Eurodac, the VIS envisages the rights of data subjects to information, access and deletion.

Similar to the VIS are the databases proposed in the Smart Border Package.[23] This package was proposed by the Commission in February 2013 with the

---

[21] Article 9, Regulation No. 767/2008 refers to the Common Consular Instructions that require the fingerprints of all ten fingers to be taken.

[22] These data include: surname, name, sex, date, place and country of birth, current nationality and nationality at birth, type and number of the travel document, the authority which issued it and the date of issue and of expiry, place and date of the application, type of visa requested, details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, main destination and duration of the intended stay, purpose of travel, intended date of arrival and departure, intended border of first entry or transit route, residence, current occupation and employer; for students: name of school, in the case of minors, surname and first name(s) of the applicant's father and mother (Articles 9, 10, Regulation No. 767/2008). When the visa is issued further data concerning the visa will be added.

[23] http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228_01_en.htm

aim of introducing a higher level of automation of border control. The package contains three proposals: one establishing an Entry-Exit System (EES), another implementing a Registered Traveller Programme (RTP) and a third one introducing the consequently needed modification in the Schengen Border Code.

The EES, modelled on the US-VISIT system,[24] registers the time and place of entry and exit of all TCNs who travel to the European Union for a short stay. Its aims are:

- to calculate the authorised stay of TCNs admitted for a short stay;
- to assist in the identification of any person who does not fulfil the conditions for entry or stay on the EU territory;
- to enable authorities of the Member States to identify overstayers[25] and take the appropriate measures (The proposal does not specify the measures to be taken. They could amount to a fine or the issuing of an expulsion order);
- to gather statistics on the entries and exits of TCN for analysis.

The total amount of border crossings has been identified in 887 million by 2025 (see EC 2014). The aim of the RTP is to speed up border crossing for frequent, pre-vetted, pre-screened TCNs, who are estimated to about 9 million by 2025 (see EC 2014). This registered traveller programme would be voluntary and under the payment of a fee. The successful applicants will receive a token (a machine readable card with a unique identifier) that allows entering and exiting the border through the Automatic Border Control (ABC) gates.

Both of these proposed new systems will collect alphanumeric and biometric data. Like SIS II, they will be under the operational management of eu-LISA and they will share the same communication and biometric data processing systems.

Specifically relevant for the Mediterranean area is EUROSUR (European Border Surveillance System), which became operational in December 2013. Its aim is to facilitate the exchange of information and cooperation between Member States and Frontex[26] and - in certain cases and on the basis of bilateral and

---

[24] The US-VISIT system is rather controversial, in particular because it does not seem to succeed in collecting biometric exit data (for details see Koslowski 2005, Koslowski 2007, Jeandesboz et al. 2013).

[25] Those who enter the EU with a valid travel document but then become unlawful migrants because they do not leave the EU territory when their authorisation to stay expires.

[26] Frontex is the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. It was established by

multilateral agreements – with third countries. The purpose of the exchange of information is the empowerment of the "ability to monitor, detect, identify, track and understand illegal cross-border activities in order to find reasoned grounds for reaction measures on the basis of combining new information with existing knowledge, and to be better able to reduce the loss of lives of migrants at, along or in the proximity of, the external borders" and the "ability to perform actions aimed at countering illegal cross-border activities at, along or in the proximity of, the external borders" (Article 3, Regulation No. 1052/2013). Information is obtained from several sources (national border surveillance systems, sensors, patrol activities, drones, etc.) and is collected and analysed in order to obtain pictures of the situation organised in three different layers:

- an events layer, which contains events such as unauthorised border crossings, detected cross-border crimes, suspect objects or persons, crisis situations;

- an operational layer, which contains information on the authorities involved in border activities and on weather conditions;

- an analysis layer, which contains information such as indicators, risk analysis and maps. In the proposed version of the regulation it also includes migrant profiles.

The purpose of EUROSUR is not to collect personal data but it could result in more collection and processing of personal data than originally foreseen, given the wide range of information collection activities and the use of advanced technologies such as drones and smart cameras. Moreover EUROSUR is one of the surveillance systems that will be interoperable within the Common Information Sharing Environment (CISE)[27] in the EU maritime domain. The aim of the CISE system, which is currently under development, is to enhance the exchange of information between national authorities and EU agencies on maritime surveillance. Flows of migrants to the Schengen Area via the Mediterranean Sea are one of the areas of interest (for details see the recent COM 2014 451 final[28]).

Regulation No. 2007/2004.

[27] See http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm.

[28] Communication from the Commission to the European Parliament and the Council. Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain.

4. Discussion: some reflections on profiling and automated decision making in the context of Italian border control

The EU databases and in general the use of technology in border control have been analysed from several points of view. In particular, the lack of transparency in the decision making process and the lack of democratic control over these information systems have been underlined by several authors (Parkin 2011, Brouwer 2008a, Petermann et al. 2006). Although this fieldwork did not analyse these aspects, its findings do confirm a lack of information and understanding among the experts, in particular lawyers, who work in the field of immigration. The lawyers interviewed seem to take data protection issues into consideration when problems arise which affect the possibility of their clients to stay in the country. None of them ever consider data protection as a right in itself that needs to be enforced. This may be due to the disciplinary segmentation of these professionals. Lawyers that deal with data protection issues do not deal with immigration and vice versa.

Besides this lack of awareness among experts, the results of this fieldwork revealed that data protection rights are clearly established on paper but not fully enforced in practice. TCNs are often unaware that their data are being collected, even when this is done according to the law; they are not properly informed about the fact that they are being registered, what this registration implies and how they can dispute it. Moreover, data are collected lawfully but the purpose of their collection and use changes over time. New authorities have access to the data, the retention of data is extended and new purposes are added that justify the use of previously collected data. In conclusion, it would not appear to be an exaggeration to say that the essence of data protection principles is undermined by these databases.

In general, these databases allow the storage of a huge amount of information about a growing number of people or objects and aim to make it easier for countries to exchange information. However, the findings of this fieldwork have underlined that the effective implementation of all of their functions (such as the addition of fingerprints and links between alerts) has not yet been achieved. Bureaucracies need time to implement new functions and this appears to be one of the biggest obstacles to their effectiveness. Somehow the delays of the State bureaucracy in adapting to the new functionalities involuntarily protect the rights of the persons whose data are stored in these databases.

Notwithstanding this, the addition of new functions (in the case of SIS II) and new purposes (both for SIS II and Eurodac), and the features of forthcoming databases (EES and RTP), have blurred the distinction between border control, counter terrorism, the fight against transnational crimes and migration management.

This trend is strictly related to the power of the law enforcement authorities at

EU (Europol) and Member States level to access data.

The original collection of data for a well-defined and narrow purpose has been combined with further storage for new purposes. The clear-cut example is Eurodac. This database, originally created to better implement asylum policy, will store data about persons who have been granted refugee status and grant access to law enforcement agencies. It appears clear that these data will not serve the original purpose (to identify the competent State for the asylum procedure) but rather plant a seed of suspicion as to the motives of people asking for international protection (innocent and even vulnerable people) whose data are stored with a view to fighting future crimes, even though there is no indication that those people whose data have been withheld will ever commit a criminal offence.

The original nature of SIS II has also changed. From being a tool to guarantee the enforcement of the Schengen Agreement, it is slowly moving towards becoming a tool for investigative purposes. This transformation is now at the embryo stage. But an extensive interlinking of alerts and the collection of fingerprint data in a format that allows comparison will modify the present – certainly limited – use of the database. The VIS, RTP and EES clearly have a multi-purpose nature and this clearly indicates that the trend is towards multi-purpose databases.

Moving closer to the specific issue of this chapter, all the EU databases (existing and forthcoming) share the common feature of being tools aimed at classifying people (i.e. TCNs and travellers) into various categories, whose access to rights is differentiated. The aim of this classification is to make it easier to control borders, or better to say, control mobility of the target population.

Those identified as trusted travellers (and who will be included in RTP databases in the future) will be granted the highest degree of mobility and given the green light, thanks to previous checks, which will allow them to be included in the databases.

Those with criminal records or bans on entry to EU territory will be given the red light. They are the Third Country Nationals included in SIS II.

Those whose motives are questionable, whose data are requested and held for future use, get the amber light. This is the case for those whose data are entered in the EURODAC database and those who apply for a visa. All such TCNs are looked upon as possible troublemakers, and their data are kept well beyond the time needed for the administrative and purely migration-management purposes for which they were collected. Amber is also the colour assigned to potential overstayers who will be included in the forthcoming EES.

As already suggested in the introduction, owing to this differentiation, these databases are the perfect tool for regulating personalised borders, where controls can be performed at multiple sites because the border is embodied in the traveller.

In order to be efficient, this personalisation certainly finds a good ally in automated decision making and profiling systems.

The databases in their current forms contain some traces of automated decision making. In the daily use of SIS II it appears clear that law enforcement officers enter the alert without any individual assessment. The alert is the automatic consequence of the administrative act of expulsion.

Moreover the new function of the interlinking of alerts represents a fruitful tool for profiling purposes. It allows the assessment of the person to be performed on the basis of the links between that person and other people and/or objects.

The evolution of border control databases over the last ten years has shown the information stored in these databases to be of a rather dynamic character. Information that might have been gathered for a very limited purpose can be turned into valuable knowledge when combined with other data or when used for different purposes. This is clearly the case for the extension of access to law enforcement officers.

Moreover, the EUROSUR system and the CISE, currently under development, are clearly directed towards the exchange of information with the aim of building new knowledge from the available information.[29]

Automated profiling is certainly not a common practice in the present use of databases but the classification of the population according to different risk levels through the creation of new databases and the development of new information exchange schemes makes border control an area of increasing interest for profiling and automated decision making.

References

Besters, Michiel and Frans W.A. Brom. 2010. "'Greedy' information technology: the digitalization of European migration policy." *European Journal of Migration and Law* 12(4): 45-70.

Bigo, Didier, Sergio Carrera, Ben Hayes, Nicholas Hernanz and Julien Jeandesboz. 2012. *Evaluating current and forthcoming proposals on JHA databases and a smart borders system at EU external borders.* Accessed December 1, 2014. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462513/IPOL-LIBE_ET(2012)462513_EN.pdf.

[29] EUROSUR and CISE regard maritime borders. However, other EU proposals, such as the Directive on PNR (Passenger Name Record), have made it clear that land and air borders are also increasingly reliant on the exchange of information for border control.

Boehm, Franziska. 2012. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. Berlin and Heidelberg: Springer.

Bosworth, Mary. 2008. "Border control and the limits of sovereign state." *Social & Legal Studies* 17(2): 199-215.

Broeders, Dennis and James Hampshire. 2013. "Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe." *Journal of Ethnic and Migration Studies* 39(8): 1201 – 1218.

Brouwer, Evelien. 2007. "The use of biometrics in EU data bases and identity documents. Keeping track of foreigners' movements and rights." In *Are you who you say you are? The EU and Biometric Borders*, edited by Juliet Lodge, 45-66. Nijmegen: Wolf Legal Publishers.

Brouwer, Evelien. 2008a. *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*. Leiden and Boston: Martinus Nijhoff.

Brouwer, Evelien. 2008b. *The Other Side of the Moon: The Schengen Information System and Human Rights – A Task for National Courts.* Accessed 1 December, 2014. http://www.libertysecurity.org/article1997.html.

Coombs, Mira. 2004. *Excisions from the Migration Zone. Policy and Practice.* Accessed 1 December, 2014. http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/J4TB6/upload_binary/j4tb66.pdf;fileType=application%2Fpdf#search=%22library/prspub/J4TB6%22>.

Council Decision 2007/533/JHA of 12 June 2007 on the establishment operation and use of the second generation Schengen Information System (SISII), *Official Journal L205, 8/7/2007*, 63–84. Accessed December 1, 2014. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1420717799293&uri=CELEX:32007D0533.

Council Decision 2008/663/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, *Official Journal L 218, 8/13/2008*, 129–136. Accessed 29 January, 2015, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008D0633.

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, *Official Journal L 316 , 12/15/2000*, 1 -10. Accessed 29 January, 2015, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000R2725:EN:HTML.

De Nationale Ombudsman. 2010. *No entry. Investigation of the registration of foreign nationals in the Schengen Information System and the provision of information in this connection*. Accessed 1 December, 2014. http://www.nationaleombudsman.nl/sites/default/files/report_2010-115_no_entry.pdf.

EDPS Opinion of 19 October 2005, *2006/C 91/11*. Accessed 1 December, 2014. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2005/05-10-19_SISII_EN.pdf.

Ericson, Richard and Kevin Haggerty. 1997. *Policing the Risk Society*. Oxford: Oxford University Press.

European Commission. 2011. "Proposal for a Regulation of the European Parliament and of the Council COM (2011) 873: Establishing the European Border Surveillance System (EUROSUR)." *2011/0427 (COD),* Accessed 18 May, 2015, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/eurosur_final.pdf.

eu-LISA. 2014a. *Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000*, Accessed 1 December, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/docs/eulisa_report_eurodac_en.pdf.

eu-LISA. 2014b. *SIS II – 2013 Statistics*. Accessed 1 December, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/docs/20140709_sis_ii_stats_2013_public_en.pdf.

EU Regulation No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *Official Journal L 381, 12/28/2006*, 4–23. Accessed 29 January, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1420717394124&uri=CELEX:32006R1987.

EU Regulation 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). *Official Journal L 218, 8/13/2008*, 60–81. Accessed 29 January, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1420717261919&uri=CELEX:32008R0767.

EU Regulation No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 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 requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and

amending Regulation. (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems, *Official Journal L 180, 6/29/2013*, 1–30. Accessed 15 January, 2015 http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1420717461649&uri=CELEX:32013R0603.

Eurodac Supervision Coordination Group. 2009. *Second inspection report*. Accessed 1 December, 2014. https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac.

Feeley, Malcolm M. and Jonathan Simon. 1992. "The new penology: notes on the emerging strategy of corrections and its implications." *Criminology* 30 (4): 449-474.

Ferraris, Valeria. 2014. "Trapped by stand-by borders." *International Journal of Migration and Border Studies* 1: 27-28.

Karanja, Stephen K. 2008. *Transparency and Proportionality in the Schengen Information System and Border Control Cooperation*. Leiden: Martinus Nijhoff.

Koslowski, Rey. 2005. "Real challenges for virtual borders: the implementation of US-VISIT." Accessed 1 December, 2014. http://www.migrationpolicy.org/pubs/Koslowski_Report.pdf.

Koslowski, Rey. 2007. *Testimony before the Senate Judiciary Committee Subcommittee on Terrorism, Technology and Homeland Security, US-VISIT: Challenges and Strategies for securing the U.S. Border.* Accessed 1 December, 2014. http://www.gpo.gov/fdsys/pkg/CHRG-110shrg34148/pdf/CHRG-110shrg34148.pdf.

Koslowski, Rey. 2011. "The evolution of Border Controls as a Mechanism to Prevent Illegal Immigration." Accessed 1 December, 2014. http://www.migrationpolicy.org/research/evolution-US-border-controls-illegal-immigration.

Lyon, David. 2007. "Surveillance, Security and Social Sorting: Emerging Research Priorities." *International Criminal Justice Review* 17(3): 161-170.

Lyon, David. 2009. I*dentifying Citizens: ID Cards and Surveillance*. Cambridge: Polity.

Parkin, Joanna. 2011 "The difficult road to the Schengen Information System II: the legacy of laboratories and the cost for fundamental rights and the rule of law." Accessed 1 December, 2014. http://www.ceps.eu/book/difficult-road-schengen-information-system-ii.

Peers, Steve. 2011. *EU Justice and Home Affairs Law*. Oxford: Oxford University Press

Petermann, Thomas; Arnold Sauter and Constanze Scherz. 2006. "Biometrics at the borders. The challenges of a political technology." *International Review of Law, Computers & Technology* 20 (1-2): 149-166.

Valverde, Mariana and Michal S. Mopas. 2004. "Insecurity and the Dream of Targeted Governance." In *Global Governmentality: Governing International Spaces*, edited by Wendy Larner and William Walters, 233-250. London: Routledge.

Weber, Leanne. 2006. "The shifting frontiers of control." In *Borders, mobility and technologies of control*, edited by Sharon Pickering and Leanne Weber, 21-43. Dordrecht: Springer.

Zolberg, Aristide R. 1999. "The Great Wall Against China: Responses to the first Immigration crisis, 1885- 1925." In *Migration, Migration History, History. Old Paradigms and New Perspectives*, edited by Jao Lucassen and Leo Lucassen, 291-315. Berlin and Wien: Peter Lang.