prof[l]ng

PROTECTING CITIZENS' RIGHTS FIGHTING ILLICIT PROFILING

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

Valeria Ferraris

(Amapola - Projects on security and safety of cities and citizens)

With financial support from the
"Fundamental Rights and Citizenship Programme" of the European Union

Borders and Profiling

Unexplored field.

Borders are a tool of classification and are increasingly mobile

Technology is pictured as a great help to control the borders.

Databases are pictured as the efficient and effective way to exercise remote control.

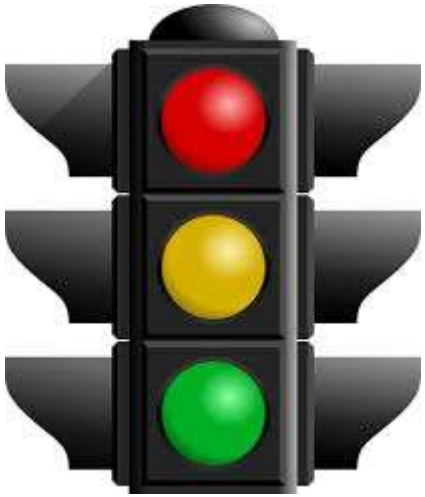
Methodology

- Literature review
- Semi- structured Interviews

The access to information has encountered some difficulties.

Databases

- SIS II – Schengen Information System
- EURODAC
- VIS – Visa Information System
- EES – Entry-Exit System
- TRP – Registered Traveller Programme



and surveillance programmes

- EUROSUR
- CISE

Databases

- They are biometric databases
- under the operational management of a new European Agency for the operational management of large-scale IT databases
- sharing the same communication system and handling system for biometrics.

SIS II

The Schengen Information System (SIS) is the oldest and one of the most important large-scale databases in the European Union. It was originally created as a compensatory measure to allow for the free movement of persons in the Schengen area.

SIS II has a **dual legal basis**, formerly divided between the first and third EU pillars.

The system is an **interconnection of a national system (N-SIS), via a secured 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 **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.

Access to the SIS from the police forces can be through the SIS II native interface or the SDI (Sistema Di Indagine) interface, which is the national police information system. The access to SDI and SIS has different authorisation procedures, and the authorisation of users for the SIS is an exclusive competence of the N-SIS office.

It contains alerts on persons and objects for several reasons.

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 (art. 97 CISA; article 32 Decision/2007/533/GAI);
- Persons sought to assist with a judicial procedure (art. 98 CISA; article 34 Decision 2007/533/GAI);
- Persons for discreet checks or specific checks (art. 99 CISA; article 36 Decision 2007/533/GAI).

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

Type of alert (%)	1999	2003	2007	2010	2013
Wanted for arrest/ extradition	1,23	1,6	1,79	3,08	4,05
Unwanted TCNs	89,36	88,99	84,08	79,27	74,43
Missing persons	3,21	3,67	4,75	5,63	6,47
Arrest in view of a judicial procedure	4,18	3,92	5,66	8,48	10,64
Discreet or specific checks	2,03	1,82	3,72	3,53	4,4

There are great differences among countries on the number of alerts inserted and on the number of access.

Numbers of alerts divided by countries

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

Numbers of access to the 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**

The reasons for creating an alert differ from one Member States to another. Article 24 of the Regulation gives the general framework but also allows a high degree of discretion by the National States.
Article 24 foresees the issue of an alert in two situations:
1.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
2.when a TCN could represent a threat inferable by the fact that a TCN has been convicted in a MS of an offence carrying a penalty of at least one year of detention or there are serious grounds for believing that s/he has committed (or intend to commit) a serious criminal offence.

In Italy, alerts are issued only by the **Immigration Office** of the local Police Headquarters. This office is responsible for issuing the alert, for deletion and for any changes related to this alert.
In the Italian law the alert is not foreseen in case of refusal of entry.
The local Police authorities interviewed affirmed that **the alerts foreseen in point 2 have not been implemented.**
The issuing of the alert appears to be the consequence of a **highly routinized procedure.**

Data Stored

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.

Biometric data are currently used only to confirm the identity of a Third Country National who has been located as a result of an alphanumeric search in SIS II.

The **links between alerts** are the most relevant and sensitive novelty. This functionality allows connecting an alert to another one.
To give an example: an alert for an unwanted TCN can be connected with an alert for a stolen vehicle where the person was founded. If in the car there was another person, these two persons are connected by the alert on the vehicle.

This is a useful tool for policing purposes and it adds new purposes to the alert.

But the local Police authorities interviewed affirmed that the links are not implemented yet.

The access to the database is given on a hit/no-hit basis.

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 visa. In both cases the national legislation governs the access of these authorities.

The access is profiled for typologies of alert and level of authorization. All the five Italian law enforcement agencies (Carabinieri, Police, Guardia di Finanza, Polizia Penitenziaria e Corpo Forestale dello Stato) have access. The city police have access only to registration regarding vehicles.

There is no national legislation regulating access to the databases. Decrees of the Chief of the Police establish who have access to the database. These are administrative acts, circulated internally. The list of authorities who have access to the database is unpublished but, according to article 31 Regulation 1987/2006 the list is sent to the EU-Lisa, which will ensure the annual publication in the Official Journal of the EU.

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.

The retention period is calculated from the day the TCNs left the Schengen territory (not just the Italian one). This means that if there is no proof that the migrants left the territory, the alert is maintained and renewed. This could partially explain the high figures on alerts on persons in Italy.

The right to information appears not to be enforced in practice.

A clear and well established procedure is foreseen for **the right of access, correction and deletion.**

EURODAC

Eurodac is the oldest EU biometric database. It was established in 2000 (Regulation no. 2725/2000) and became operational in 2003.

The original purpose was to help 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.

In 2013 law enforcement purposes have been added.

The system consists of a computerised central fingerprint database (so called "Central system") and a communication infrastructure between the Central System and Member States.

In Italy the authority in charge is the Forensic Police.

There are 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 to check whether the data subject has previously lodged an application for asylum in another Member State.

Data stored are specific for each category and the retention period varies.

	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 in which the fingerprints were taken - date in 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 in which the fingerprints were taken - date in 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
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 become aware of: - acquisition of citizenship;	As soon as the State become 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 purpose, as laid down in Article 1.2. Upon the expiry of the three years period the data will be blocked and then erased, when the retention period expires.*		

Data are inserted in the system by the fourteen focal point in the Italian territory through the national AFIS (Automated Fingerprint Identification System) interface.

Due to the specificity of the recent immigration flows, this activity take places more extensively in the focal point in the South of Italy, mainly in Sicily, where greater is the number of people who are apprehended while irregularly crossing the borders. Since the beginning of the recent operation called Mare nostrum fingerprints are also immediately taken on the ship that search and rescue the migrants.

Information exchange and surveillance programmes

EUROSUR (the European Border Surveillance System), which became operational in December 2013.

Its aim is to facilitate the exchange of information and the cooperation between Member States and Frontex and 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 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 1052/2013).

Information exchange and surveillance programmes

The sources of information are many (national border surveillance system, sensors, patrol activities, drones, etc.) and collection and analysis of information aims at producing pictures of the situation organized in three different layers:

1. an events layer, which contains events such as unauthorized border crossing, detected cross-border crimes, suspects objects or persons, crisis situations;
2. an operational layer, which contains information on the authorities involved in border activities and on weather conditions;
3. an analysis layer, which contains information such as indicators, risk analysis, maps. In the proposal version of the regulation it also included migrant profiles.

Information exchange and surveillance programmes

Moreover Eurosur is one of the surveillance systems that will be interoperable within the **Common Information Sharing Environment (CISE)** in EU maritime domain. CISE is a under development system that aims to enhance the information exchange between national authorities and EU agencies on maritime surveillance. The flows of migrants to the Schengen Area through the Mediterranean Sea are one of the area of interest.

Main findings

1. Databases classify travellers according to degrees of suspicion.
2. Some of the new functions of SIS II, in particular the interlinking between alerts, are elements of profiling.
3. Eurosur and the maritime surveillance programmes contains elements of profiling.
4. There is a hiatus between the design of the database and its implementation.
5. There is a clear trend to multi-purpose databases.
6. There is a clear trend to grant access to new authorities, unrelated with the original scope of the data collection.
7. Data protection rights are clearly established on paper but not fully enforced in practice.
8. Profiling is not a common practice in the present use of databases for migration control but there are all the elements for profiling practices in the future.

What we need most

Transparency

Proportionality

Data protection for TCNs

Awareness

Thank you for your attention!

Valeria Ferraris
valeria.ferraris@amapolaprogetti.org
valeria.ferraris@unito.it
Amapola Progetti
Law Department – University of Turin
http://profiling-project.eu