in:ex

Converging and conflicting ethical values in the internal/external security continuum in Europe

European Commission, 7th Framework Programme

# D.1.3. Documentation and analysis of the impact of new security technologies on European citizens

**Deliverable submitted March 2010 (M24) in fulfillment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the Internal/External Security Continuum in Europe (INEX)**


| PRIO | International Peace Research Institute, Oslo | PO Box 9229 Grønland NO-0134 Oslo, Norway | T: +47 22 54 77 00 F: +47 22 54 77 01 | www.inexproject.eu |
|---|---|---|---|---|

# Documentation and analysis of the impact of new security technologies on European citizens

INEX Deliverable D.1.3.

Centre d'études sur les Conflits

**Contributors:**

Didier Bigo

Julien Jeandesboz

Francesco Ragazzi

## TABLE OF CONTENTS



## List of tables:

## ACRONYMS

| | |
|---|---|
| **AFIS** | Automated Fingerprint Identification System |
| **AFSJ** | Area of freedom, security and justice |
| **API** | Advanced Passenger Information |
| **ATS** | Automated Targeting System |
| **CAPPS** | Computer Advanced Passenger Prescreening System |
| **CBP** | Customs and Border Protection |
| **CCI** | Common Consular Instructions |
| **CCV** | Community Code on Visas |
| **CRS** | Computer Reservation System |
| **DHS** | Department of Homeland Security |
| **DPA** | Data Protection Authority |
| **EDPS** | European Data Protection Supervisor |
| **GDS** | Global Distribution Service |
| **INES** | Carte nationale d'identité électronique et sécurisée |
| **PNR** | Passenger Name Record |
| **RFID** | Radio-frequency identification |
| **SIS** | Schengen Information System |
| **TCN** | Third Country National |
| **TSA** | Transport Security Authority |
| **VIS** | Visa Information System |

## INTRODUCTION[1]

1. European border control and surveillance practices are based on the key premise that the EU constitutes an 'area of freedom', where EU citizens enjoy the right to come and go at their will. As the recently adopted Stockholm programme argues:

> The right to free movement of citizens and their family members within the European Union is one of the fundamental principles on which the Union is based and one of the fundamental freedoms of European citizenship. Citizens of the Union have the right to move and reside freely within the territory of the Member States, the right to vote and stand as candidates in elections to the European Parliament and municipal elections in their Member State of residence, protection of diplomatic and consular authorities of other Member States, etc. When exercising their rights, citizens are ensured equal treatment to nationals under the conditions set by Union law.
>
> (Council of the European Union, 2009b: 13)

This premise, however, is complemented by the notion that with free movement come a series of challenges that need to be addressed, if one is to protect this very freedom. This is made very clear in the recent draft of the EU's Internal Security Strategy that was discussed at the meeting of the EU's Interior Minister in Toledo on 21 January 2010:

> The European Union (EU) in the 21st century consists of 500 million people across the 27 countries which make up the Union. Economic growth, together with the opportunities provided by a free and democratic society based on the rule of law, generate prosperity amongst people in Europe – but with such opportunities also come risks, as terrorists and other types of criminals seek to abuse these freedoms to destructive and malicious ends. Furthermore, increased mobility of people increases our common responsibility for protecting the freedoms all citizens of the Union cherish.
>
> (Spanish Presidency, 2010: 3)

This extract highlights the current evolution in the framing of EU citizenship, as being constituted jointly by the right to free movement and a right to security and protection. As we have highlighted in our previous deliverables, the inclusion of security as a fundamental right to be enjoyed by European citizens raises a certain number of questions. Protection, in this respect, is also a problematic notion (e.g. Bigo, 2006), particularly when protection, as suggested also in the Stockholm programme, is to be supported by a growing range of technical systems:

> Security in the EU requires an integrated approach where security professionals share a common culture, pool information as effectively as possible and have the right technological infrastructure to support them.
>
> (Council of the European Union, 2009b: 37)

This element is particularly emphasised with regard border control and surveillance. Referring again to the Stockholm programme:

[1] The authors want to thank Philippe Bonditti for his comments on earlier drafts of this paper, as well as the staff from the Centre d'études sur les conflits (C&C) for their invaluable assistance in research and bibliography.

> [t]he European Council considers that technology can play a key role in improving and reinforcing the system of external border controls […] The possibilities of new and interoperable technologies hold great potential for rendering border management more efficient as well as more secure but should not lead to discrimination or unequal treatment of passengers.
>
> (Council of the European Union, 2009b: 57)

European citizens, however, are not the only ones concerned by this issue. The Stockholm programme, in this respect, emphasises the issue of access to the EU as a core concern – although the document's framing of the question is worth mentioning:

> Access to Europe for businessmen, tourists, students, scientists, workers, persons in need of international protection and others having a legitimate interest to access EU territory has to be made more effective and efficient. At the same time, the Union and its Member States have to guarantee security for its citizens. Integrated border management and visa policies should be construed to serve these goals.
>
> (Council of the European Union, 2009b: 4)

Border control and surveillance practices, in this perspective, are not only about the control of the geo-political border: they involve, more fundamentally, the regulation of the relations between two categories of persons, EU citizens and 'non-citizens', of which geo-political demarcations are but one aspect. It is important to highlight, however, that these categories – EU citizens and 'non-citizens' – are constructed through a series of administrative, legal and political techniques that 'objectivise' this distinction.

2. These elements highlight the pertinence of proposing a reflection on the current impact of security technologies on movers across borders and within the EU. They also raise a number of questions regarding the relevance of focusing the analysis on EU citizens only. Empirically, the work conducted so far by WP1 researchers has pointed out that a number of the 'new' security technologies and technical systems put in place over the past decade have initially been designed for the purpose of governing the movements of so-called 'third-country nationals' (TCNs) – persons travelling to, or residing in the EU who do not hold formal citizenship of a Union Member State. The use of these technical systems, however, has simultaneously been expanded and applied to EU citizens. In recent years, a number of Member States have for instance sought to introduce biometric identity documents. Biometrics are also currently in the process of being introduced in all EU passports[2]. Another example in this respect is the proposed 'Registered Traveller Programme' evoked by the European Commission in its 2008 'Next Steps in Border Management' communication (European Commission, 2008): the programme would involve the deployment of automated gates for border crossing, which would be available both for 'cleared' non-EU citizens and EU citizens holding biometric travel documents, on a voluntary basis. Another proposal that is currently being considered, in this respect, is the possible establishment of an EU Passenger Name Record (PNR) system, which would process data of all passengers travelling, to, from and within the EU, regardless of their nationality.
3. In this perspective, a survey of the impact of security technologies on persons, particularly in the context of EU border control and surveillance practices, would be more pertinent if it took into account this movement, which sees technologies initially developed in the name of

[2] See Council Regulation (EC) No 2252/2004.

the protection of EU citizens progressively redeployed and used on them. We thus propose to structure the present deliverable as follows:

- In the first section, we develop a certain number of considerations regarding citizenship *qua* European citizenship, particularly in the perspective of contemporary European security practices. We argue that citizenship, rather than being interpreted in the classical view of social contract thinkers as a bundle of rights and obligations conferred onto individuals by the nation-state, can be problematised as a specific technology of differentiation, operating through the delineating and classifying of populations, for the purpose of organising relations between them. This angle opens up the possibility to envisage European citizenship and the correlated right to free movement not as an unchanging given, but as a shifting system for governing populations, susceptible of alterations and transformations. Similarly, it offers the possibility to consider so-called TCNs not as a homogeneous category of European 'non-citizens', but rather as a category of population constructed through, and divided into, a series of practices of demarcation and categorisation. We further suggest, in this perspective, that security constitutes one of the techniques of government (Huysmans, 2006) that effectuates this categorisation and demarcation, with technology standing as a specific modality thereof.
- In the second section, we document the ways in which security technologies operate within the practices of mobility of persons crossing the borders of, or travelling within, the EU. Our argument, in this respect, is that while EU citizenship constitutes an important marker for differentiating between populations, the difference is of degree, not of nature. Through a survey of some of the systems we have examined in our previous instalments, we show how 'new' security technologies actually encompass both EU citizens and non-citizens, *albeit* differentially, in the same technical systems (e.g. the SIS or the envisaged EU-PNR system) or through the same modalities (e.g. biometrics), and how the reliance on technical systems, by allowing an individualisation of controls, is making this distinction, if not irrelevant, at least more fluid and heterogeneous: the categories of EU citizens and non-citizens are re-engineered through the categories of trusted/distrusted, wanted/unwanted, known/unknown travellers.
- In the conclusions, we bring together some elements of analysis of these practices. Clearly, the European 'smart border' in the making has implications in terms of fundamental rights and freedoms – regarding the right to private life and data-protection, but also, more broadly, civil rights, procedural rights for detainees or the right of *non-refoulement* for persons seeking international protection. More broadly, however, it organises a blurring of the notion of freedom.

## 1. Government, populations and European citizenship

### *1.1. Citizenship*

4. Most of our contemporary political imagination remains shaped by a theory of citizenship that is deeply embedded in a tradition of the modern nation-state. Through the different thinkers of the social contract (Rousseau, Locke and others), it is citizens which are the sole subjects of sovereignty. Citizenship thus marks a paradigmatic border between those who are inside and those who are outside. Throughout the constitution of the modern state as the progressive monopolization and bureaucratization of administration, and later, with the emergence of parliamentary regimes, citizenship has played a central role in marking the different modes of inclusion in the polity. As T.H. Marshall has demonstrated in his socio-

history of citizenship in Great Britain, citizenship has been the tool through which, not without struggles, populations have acquired civil, political and social rights. (Marshall 1950).

5. Yet the sociological and historical reality of practices of citizenship are not so clear cut as contractual theory - and the folk democratic philosophy which derives from it would like to put it. This is not to say that contractual theory of citizenship is completely oblivious to socio-historical developments. In some cases, such perspectives reflect an attachment to a more 'parsimonious' analysis of citizenship:

> Like relations between spouses, between co-authors, between workers and employers, citizenship has the character of a contract: variable in range, never completely specifiable, always depending on unstated assumptions about context, modified by practice, constrained by collective memory, yet ineluctably involving rights and obligations sufficiently defined that either party is likely to express indignation and take corrective action when the other fails to meet expectations built into the relationship. As observers, we actually witness transactions between governmental agents and members of broadly-defined categories, *but we abstract from those transactions a cultural bundle: a set of mutual rights and obligations.*
>
> (Tilly, 1997: 600. Emphasis added)

6. Already, in classical Greece - the foundational model for our thinkers of the social contract - the short historical period which saw the emergence of citizenship as a principle of common political life was marked by porous and undefined borders between citizens and non-citizens, showing a wide variety of nuances and arrangements rather that a clear cut demarcation (Isin 2002:56-58). In a similar vein, as Gérard Noiriel showed for the case of post-revolutionary France, it is only progressively, and mostly in the early 19th century, that the techniques of documentation and identification were employed to mark the differences between citizens and foreigners (Noiriel 2001). There again, it was mostly as a secondary effect of the process through which the professionalized administration needed to attribute a "civil identity" to the different members of the population it was in charge of governing. The distinction between citizens and non-citizens, and the means to enforce this distinction, have historically been characterised by a constant circulation of practices, with different poles: how to 'protect' society and identify within national populations the 'abnormals' – deviants, criminals – and the foreigners? How to regulate access of 'foreign elements' to the territory? How to control, within the territory, the movements of 'nomads', of 'subversives', but also of individuals with economically valuable skills? As Pierre Piazza (2004) shows in his history of the French national identity card, these various problematisations all contributed to the progressive carding of the whole French population, drawing technical elements from the field of criminology and policing (involving, at the end of the 19th century the competition between the anthropometric approach of Alphonse Bertillon – the famous 'bertillonnage' – and the fingerprint identification approach of Francis Galton)[3] but also relying on the further refinement of administrative methods such as the holding of population registers and the conduct of censuses.

[3] Alphonse Bertillon, an official in the Paris *préfecture de police*, introduced the first systematic approach to judicial identification and forensics, through a method involving the measurement of certain bodily features – anthropometrics, also called 'bertillonnage'. 'Bertillonnage' was in fact a twofold process: it involved, on the one hand, the collect of specific bodily information, and on the other, its classification and storage so that descriptions could be retrieved at any time. Francis Galton, cousin to Charles Darwin and head of the London anthropological laboratory, introduced the use of fingerprints for criminal investigations purposes. While highly sceptical of this method, Bertillon, who was running a correspondence with Galton, eventually introduced fingerprints in the practices of the French police in the early years of the 20th century. See Kaluszynski, 1987, for a more detailed analysis.

7. More broadly, therefore, it can be argued, building on the work of Barry Hindess, that in its heterogeneous and discontinuous historical occurrences, citizenship has mostly been a technology of government through which the progressively centralized institutions of the state have separated populations to be subjected to different practices of power and surveillance (Hindess 2002). Citizenship provides for the classification and distribution of populations, and subjects them to differentiated techniques of control. In this perspective, the distinction between citizens and non-citizens, while central in the narratives of professionals of politics and in mainstream social contract theory, should be re-examined, as a difference in the degree to which certain practices of government can be applied to a given population, rather than as a difference in essence.

### *1.2. European citizenship*

8. European citizenship was formally established in the 1992 Treaty on European Union[4]. Article 8.1 stipulates that '[e]very person holding the nationality of a Member State shall be a citizen of the Union', while Article 8.2 indicates that '[c]itizens of the Union shall enjoy the rights conferred by this Treaty and shall be subject to the duties imposed thereby'. Articles 8a to 8d then proceed to specify some of these rights, the first of which (Article 8a) being that '[e]very citizen of the Union shall have the right to move freely within the territory of the Member State'.

9. The first thesis on European citizenship is based on the dispositions contained in the Treaties. It is the thesis of 'additionality', whereby European citizenship constitutes an expansion on nation-state citizenship, an enlargement of the bundle of rights and obligations concerning citizens of EU Member States, but with the relation between the individual and the state still firmly at the centre.

10. A second perspective has been defended under a variety of angles: the formal recognition of European citizenship in the Maastricht treaty hails the advent of a new form of citizenship, which would not derive from the relation between the individual and the state. Through the processes of European construction emerges a 'multiple' (Meehan, 1993) or 'fragmented' (Weiner, 1997) form of citizenship. At the theoretical level, for many, the promotion of European citizenship was inspired by the desire to supersede the exclusionary aspects of national citizenship and move towards "post-national" or cosmopolitan citizenship (Soysal 1994, Benhabib 2006). In fact, looking back to the 1990s when the question first emerged, most debates both in the public sphere and in academia, were organized around these notions of "Souverainisme" against Federalism as well as the the "National" against the "European". At stake were the borders between who should be included and excluded: what was disturbed was not only the traditional distinction between citizens of neighbouring European countries, but also and mainly the one between European citizens and third country nationals present in Europe.

11. The events of 11/9, 11/3 and 7/7 have, if not fundamentally changed the world in which we live in, certainly provided a strong ground for the most securitarian discourses to prevail in the wider European public sphere and administration. More particularly, they have allowed, in the local, national and European institutions that compose the European field of (in)security professionals, to advocate for an ever increasing use of technologies of control and surveillance, it is argued, to protect European citizens. In doing so, it could appear that the distinction between European and non-European citizens is a widening gap: while European citizens are supposedly ever freer to circulate, live and work within the Schengen/European space, non-EU citizens who reside or would like to reside in Europe are

[4] Following references are drawn from the original text of the Treaty as published in the Official Journal of the European Communities, C191 of 29 July 1992.

facing ever harsher and tougher checks, controls and coercive measures. This picture has been framed alternatively as an unfortunate but necessary model in the narratives of government officials, particularly from Member State ministries of interior and justice, or as the advent of a scandalous and unjust "fortress Europe" in the narratives of NGOs and civil liberties groups.

12. Our point, however, differs from these two sets of narratives. We argue that the strongly marked dichotomy between citizen and non-citizen is not representative of the practices of surveillance and control as they are deployed through new security technologies. While the difference of status does form a differentiated set of practices, the difference is of degree, not of nature. Our aim, therefore, is to highlight the multiple lines through which populations on the move are segmented, sorted, channelled – and in the process, governed– and how these lines are both effectuated and shifted by the use of the technical systems analysed in our previous paper. More specifically, profiling practices in the context of EU border control and surveillance play on three correlated lines: rather than focalising on the categories of citizens and non-citizens, they concentrate on the distinctions between trusted/distrusted, wanted/unwanted and known/unknown travellers. These lines, we argue, do not espouse the formal contours of the EU's external borders, nor do they draw a clear demarcation between European citizens and non-citizens.

13. As we have showed previously, border control and surveillance practices are increasingly moving away from the formally defined external borders of the European Union. They are redeployed and 'diffused' (Côté-Boucher, 2008) beyond the geopolitical locus of EU external borders, concentrating in specific points such as major transportation hubs. They also move beyond the bureaucratic hold of border agencies and services as they increasingly involve other public actors such as consular authorities (in the case of visa deliveries) or private actors such as air carriers.

14. European citizenship, on the other hand, remains a strong marker, particularly in its operation as a legal border (Basaran, 2009) for freedoms and rights: by law, EU citizens enjoy specific conditions of mobility into and within the Union (e.g. Guild, 2005), but this does not imply that they fall outside of the scope of border control and surveillance practices. As mentioned above, some of the techniques developed initially in the name of migration control are now being expanded to operate across EU populations. In the meantime, some practices of surveillance contribute to shrink the legal borders of freedoms and rights. This is the case, for example, of the exchanges of Passenger Name Records (PNR) data between the EU and the United States with regard to data protection rights of EU citizens travelling between Europe and the United States. Existing and upcoming security technologies might participate from a regime of visibility that is of another order compared to border checkpoints within the EU, but this does not amount to the disappearance of controls. The distinction between citizens and non-citizens, in this respect, intersects with (at least) another line of demarcation, which organises the distinction between *bona fide* and *mala fide* movers, thus determining the conditions of mobility enjoyed by given individuals and groups, not so much on the basis of their citizenship (although it definitely constitutes one element) but on the basis of profiling practices. In this respect, there is a need to interrogate the kind of freedom which is supposed to be promoted by European border control and surveillance practices. Do 'smart borders' enhance freedom, as they are claimed to? And whose freedom are we speaking about?

### *1.3. Citizens and 'non-citizens' as governmental categories*

15. So far, we have suggested that there was room, and need for, rethinking the notion of citizenship as a technique of government, participating from a technology of differentiation between populations. Citizenship and non-citizenship constitute, in this respect, a dynamic

system of categorisations and relations, and the intensity of the distinction between the two is subject to variations. In addition, these two categories are far from homogeneous.

*1.3.1. Mobility and the fluctuating categorisation of 'non-citizens'*

16. The work conducted so far by WP1 researchers, and in particular the 'cataloguing' of technical systems used for border control and surveillance in Europe (Amicelle et al., 2009), has pointed to the fact that a wide range of recent security technologies and technical systems have initially been developed for the purpose of governing the movements of non-citizens – persons travelling or residing within the EU who do not hold citizenship of a Union Member State, and are thus not EU citizens. EU-wide databases such as Eurodac or the SIS, for instance, are mainly populated by so-called 'third country nationals' (TCNs). By the same token, applications to a Schengen visa are currently a major source of collection of biometric data – again, from persons wishing to travel to the EU but who are not citizens of a Member State. As a population, however, TCNs are not homogeneously 'embraced' by security technologies in their travelling to and within the EU. The usage, surface of application and effects of security technologies, in this respect, is mediated by other elements, particularly the rules and procedures governing the delivery of authorisations to access the EU. Those persons most intensively subjected to the operations of security-related technical systems are persons seeking to apply for asylum in an EU Member State as well as nationals of countries placed on the 'negative' Schengen visa list[5]. Within the latter category, furthermore, some variations can be observed regarding in particular the very concrete effects that have been tied to the use of security technologies – e.g. the increase in the price of the Schengen visa allegedly due to the introduction of biometrics – according to the social position of travellers as well as to the possible existence of a 'facilitation' agreement between the EU and their country of origins.

17. The degree to which security technologies are used to monitor persons travelling to and within the EU without holding EU citizenship varies strongly according to these persons' nationalities, but also their professional status or their place of residence. Since the incorporation of the Schengen corpus into the Treaties, a significant body of decisions, directives and regulations, as well as a variety of agreements with specific third countries, has been adopted, establishing new rules or modifying previous ones. For example, Council Regulation 539/2001 listing the countries whose nationals must hold a visa for short term entry/stay into the EU (Schengen visa) has been amended five times since its entry into force[6]. Specific modalities have also been established regarding the regulation of local border traffic[7], as well as concerning the facilitation of transit for Russian nationals living in Kaliningrad[8]. In some cases, furthermore, nationals of the same country may or may not travel visa-free to the EU, depending on the type of travel document they hold[9].

18. In addition to these elements, one must also take into account the procedures characterising the delivery of travel authorisations to third-country nationals. European practices in this

[5] See Annex I of Council Regulation (EC) No 539/2001.

[6] Council Regulation (EC) No 539/2001 of 15 March 2001, modified by Council Regulation (EC) No 2414/2001, Council Regulation (EC) No 453/2003, Council Regulation (EC) No 851/2005, Council Regulation (EC) No 1932/2006 and Council Regulation (EC) No 1244/2009.

[7] Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 December 2006.

[8] Council Regulation (EC) No 693/2003 and No 694/2003 of 14 April 2003.

[9] Citizens of the former Yugoslav Republic of Macedonia, Montenegro and Serbia holding biometric passports may travel without a visa for stays not exceeding three months. Holders of non-biometric passports will need to apply for a visa, under the conditions established by the visa facilitation agreement concluded between the EU and their respective countries. See Council Regulation (EC) 1244/2009.

domain are far from homogeneous. The only so-called 'uniform' modality in this domain is the delivery of short stay visas, which are currently framed by the Common Consular Instructions[10] (CCI, Council of the European Union, 2005b) as well as by the future 'Visa Handbook' (European Commission, 2010) and the Schengen Border Code (established by Regulation (EC) No 562/2006). As Didier Bigo and Elspeth Guild (2003) have shown, it is in the context of the delivery of Schengen visas that an important part of the controls operated on persons wishing to travel to the EU takes place – and, more crucially for our purpose, where security technologies are put to use, mainly the recourse to computerised databases (the SIS and in the future the VIS) as well as biometrics (in relation to the VIS).

19. While formalising the procedures for delivering the Schengen visa, however, the CCI leave a wide room for manoeuvre to Member State consular posts as far as the decision to grant visas is concerned. Hence, the CCI note:

> The diplomatic mission or consular post shall assume full responsibility in assessing whether there is an immigration risk. The purpose of examining applications is to detect those applicants who are seeking to immigrate to the Member States and set themselves up, using grounds such as tourism, business, study, work or family visits as a pretext.
>
> (Council of the European Union, 2005b: 10)

20. The CCI thus authorise Member State consular posts to request other documents in addition to the mandatory requirements laid down in common procedures in order to limit 'immigration risk'. In fact, the CCI are merely countersigning the actual practice of visa delivery by Member State representations. There are now a growing number of studies that highlight the shear arbitrariness of the process, with document requirements varying not only from country to country, but also from consular post to consular post in the same country (e.g. for Bulgaria pre-accession, see Jileva, 2003), and a 'politics of front desks' (*'politique des guichets'*, see Spire, 2008) that is characterised by an extreme defiance of consular officers towards visa applicants who are *a priori* considered – and depicted - as potential abusers. Arbitrariness and defiance towards would-be travellers is not mitigated by the reliance on technical systems, despite the pervasive notion that technology as such is 'neutral'.

### *1.3.2. EU citizens: free movement for all?*

21. As suggested in the introduction, European border control and surveillance practices rest on the narrative that the EU constitutes an area where European citizens can move unhindered. This narrative, more precisely, rests on three tenets.

22. The first one is that movement has been 'freed' through the processes of European construction. However, if one examines the substantial regulatory body constituted over time around the issue of freedom of movement for persons, it seems more pertinent to argue that

[10] As of 15 April 2010, the CCI will be replaced by the Community Code on Visas (CCV, see Regulation (EC) No 810/2009 of 13 July 2009). At the time of writing, however, the CCI still apply, hence our use of this document in the following pages. Furthermore, the CCV introduces little change in the logic already laid out in the CCI – although the language in use is more polished. Hence, Art.21(1) of the CCV Regulation states that "[i]n the examination of an application for a uniform visa […] particular consideration should be given to assessing whether the applicant presents a risk of illegal immigration or a risk to the security of the Member States", while Art.21(8) establishes that "[d]uring the examination of an application, consulates may in justified cases call the applicant for an interview and request additional documents".

mobilities have been reorganised, rather than liberated. This is in fact quite obvious from EU legislation in this respect – see for instance Recital (1) of Directive 2004/38/EC[11]:

> Citizenship of the Union confers on every citizen of the Union a primary and individual right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaty and to the measures adopted to give it effect.

In analytical terms, European construction can be read as a process of 'de-monopolisation' of the means of movement previously claimed by European states (Torpey, 1998, 2000) which has seen this monopoly progressively redeployed through the European governmental arenas (Jeandesboz, 2009).

23. The second tenet is that this process of 'liberation' of mobility has been a linear and cumulative process, undoubtedly difficult at some times, but culminating in the current European 'area of freedom, security and justice'. It is important, however, to highlight that the processes that have led to the constitution of the European common, and later on, single, market, backed against the legal and normative framework of the so-called 'four freedoms' of circulation (for capitals, goods, services and most crucially, persons), the establishment of a 'passport-free zone' through the Schengen arrangements, and the concatenation of both dynamics within the current European 'area of freedom, security and justice' can be read as a series of competing operations, rather than as linear process. As students of the free movement of persons in Europe have noted, mobility in the TEC was closely associated to the question of economic activity. Free movement of persons was then initially restricted to those individuals considered as economically active – *i.e.* workers, and so-called 'service providers':

> In the view of those drafting the original EEC Treaty free movement rights would only be granted in order to facilitate the free pursuit of economic activities across inter-State borders. The right to move and reside freely were preserved for employed and self-employed persons and the right to equal treatment would, in principle, be limited to matters related to work and income.
>
> (van der Mei, 2003:21)

In this respect, it took ten years after the entry into force of the treaty of Rome, and two years before the end of the transitional period envisaged for the application of the provisions included in the treaty, for the transcription in Community law of the dispositions on the movement of workers, namely through Regulation 1612/68 and Directive 68/360 (van der Mei, 2003:21-28). One of the effects of the framing of freedom of movement in the context of the construction of the European common market is that subsequent discussions largely crystallised upon the economically active/non-economically criteria for establishing categories of persons in movement. This informed subsequent evolutions, which have dealt, on the one hand, with certain aspects of the movement of workers (equal treatment, right of residence for persons in search of employment, access to social benefits), and on the other hand, with establishing frameworks for the definition of non-economically active individuals (such as students or pensioners) and the regulation of their movements. All these developments, however, did not go without tensions in the European governmental arenas. In this regard, for instance, initial discussions excluded from the scope of free movement of workers dispositions member states nationals from overseas territories, as well as the possibility for

[11] This directive consolidates and replaces the main legal texts on freedom of movement adopted since the entry into force of the treaty of Rome.

persons to move to another EC member state to seek employment (van der Mei, 2003:24-25). It took another two decades to reorganise the dispositions concerning the families of expatriate workers, or the "non-economically" active categories of persons on the move, such as tourists, students, pensioners (who were accordingly framed as service recipients) or persons seeking employment.

24. Matters are further complicated by the emergence, in the late 1970s and 1980s, of a major competing initiative to European construction as it was conducted in the framework of the common market programme. At a time when claims for a 'political Europe' and indeed a European citizenship, backed by the conclusions of the 1976 Tindemans report and of the 1984 Adonnino committee ('ad hoc Committee on a People's Europe'), the perspective of free movement being established among EC member states served as the baseline justification for the formalisation of a series of transformations of internal security apparels in Europe, particularly through the Schengen processes initiated in the mid-1980s.

25. Mobility in the context of Schengen was framed differently than in the context of the construction of the European common market:

> The main philosophy underlying the Schengen Conventions is that when borders are opened and free traffic of persons and goods is allowed, internal security can only be guaranteed by compensatory measures.
>
> (Anderson, den Boer, Cullen et al, 1995:57)

26. The Schengen conventions thus added another layer to the processes of European construction as regards mobility: they delineated another space where the movement of persons could be reorganised, which did not correspond to the formal contours of the European internal market, but also grafted another way of looking at mobility in the context of Europeanization processes, namely by framing it in terms of concerns for security. This is due to the fact that the genesis of Schengen is tied with the development of discreet and informal fora for cooperation between European security agencies, initiated in the mid-1970s, by the creation of the Trevi committee (1975) and its various working groups (see Bigo, 1992, 1996; Bunyan, 1993), under the auspices of the so-called 'European political cooperation', but outside of the EC institutional arenas. While the initial formal focus of Trevi was on terrorism, the 'Trevi 1992' group, established in 1988 in the perspective of the realisation of the European common market by 1992, operated in close relation with other structures such as the 'Mutual Assistance Group 92' on customs, and the '*Ad Hoc* Group on Immigration' which drafted among others the Dublin Asylum Convention (Anderson, den Boer, Cullen *et al.*, 1995: 55). The Schengen conventions participated from this framing, reflecting in particular the concern of high-level police and customs officials that the lifting of border checks in the context of the European common market would generate an upsurge in criminal activities, including illegal migration (Bigo, 1996).

27. The arrangements set up by the Schengen conventions continued to function alongside Community dispositions for the liberalisation of movement in the context of the European common market until their incorporation into Community law with the entry into force of the treaty of Amsterdam on 1 May 1999. The dynamics initiated in the 1970s with Trevi were formally incorporated in the 'third pillar' with the entry into force of the treaty of Maastricht: alongside the issues of police and judicial cooperation, the third pillar further comprised dispositions related to asylum, refuge and immigration. Following the entry into force of the treaty of Amsterdam, the issue of mobility was remodelled into the framework of the European 'area of freedom, security and justice'. The formal 'communautarisation' of the Schengen conventions is however misleading, in that it shadows the underpinning orientations that have structured the Schengen process. Schengen is sometimes qualified as a laboratory of European integration, which has prefigured some of the Community measures

on the movement of persons as well as in justice and home affairs (Monar, 2001), and whose experience was eventually incorporated in Community law and practice. However, as some have argued, Schengen embodies an attempt, in the initial context of the Commission proposals to establish the European common market by 1992, to maintain and enforce an intergovernmental logic with regard the issues of the movement of third country nationals and police cooperation

> The image of the Schengen "laboratory" is thus largely erroneous, since Schengen was constituted as much to avoid a Commission take-over in this domain as to assist it and anticipate on the measures that would allegedly be blocked by the British government. The Commission was not, in addition, the only opponent. The European Court of Justice, which had supported the Commission against the member states in its interpretation of the 1984 decision on its capacity to coordinate migration policies, had established a very strong incentive for ministries of Interior to constitute another "club" which would allow them to act without the Commission.
>
> (Bigo & Guild, 2003:41. Our translation)

28. This, of course, is tied to a number of factors. It has to do, in particular, with how mobility understood as migration (of nationals from non-EU countries to which were associated so-called 'stateless persons'), was politicised from the end of the 1970s onwards in European countries, *i.e.* as a peril not only to the labour markets of European countries, but beyond, to the welfare state and to the identity of the countries perceived to be at the receiving end of immigration patterns (*inter alia*, Huysmans, 2000). Migration control, or at least, claims to the control of migration, became in the process a precious symbolic resource for professionals of politics – and remains so even today. Schengen, in this perspective, was as much a means for ministries of Interior to compete with Community bureaucracies for the government of mobility as a resource for professionals of politics to claim that they were 'in control' of migration policies.
29. The re-articulation of EU mobility policies in the context of the AFSJ takes stock of this trend: it highlights a shift, whereby the dominant framing of mobility in the European governmental arenas, which so far had been that of the liberalisation of movement for economically-active individuals and recipients of services, fades in the background, while the framing dominant in the context of Schengen is formalised as the main orientation of EU mobility policies. In the 'Action Plan of the Council and the Commission on how best to implement the provisions of the treaty of Amsterdam on an area of freedom, security and justice' adopted by the Justice and home affairs council of 3 December 1998, mobility hence features as the first matter of concern, under the heading of 'A wider concept of freedom':

> Freedom in the sense of free movement of people within the European Union remains a fundamental objective of the Treaty, and one to which the flanking measures associated with the concepts of security and justice must make their essential contribution. The Schengen achievement has shown the way and provides the foundation on which to build. However, the Treaty of Amsterdam also opens the way to giving 'freedom' a meaning beyond free movement of people across internal borders. It is also freedom to live in a law-abiding environment in the knowledge that public authorities are using everything in their individual and collective power (nationally, at the level of the European Union, and beyond) to combat and contain those who seek to deny or abuse that freedom.

(Council of the European Union & European Commission, 1998: point 6. Our emphasis)

30. The re-conduction of the Schengen framing of mobility in the context of the AFSJ was accompanied by the continuation of an intergovernmental logic, despite the formal competences attributed to the Commission[12]. This continuation, of course, was not a formal one, but resulted from a variety of developments, including the staffing of the newly created Commission directorate for justice and home affairs (DG JHA) by seconded experts from ministries of Interior[13]. What is important, here, is to understand the movement encapsulated in the devising of Schengen and its subsequent evolutions. Schengen clearly embodies an effort by specific actors from national ministries of Interior and Justice as well as from national customs, border guard and police services, to take on the seemingly ineluctable institution of the European single market and frame it in their own terms. At the same time, it constitutes a further step in the 'governmentalisation' of Europe through the question of mobility. Schengen did not aim at blocking free movement, but rather at organising it through the specific techniques of government related to security[14]. Schengen, therefore, is not an operation 'against' mobility and freedom of movement, but rather an operation *about* mobility and freedom of movement. This is confirmed, for instance, by the progressive evolution in the terminology designating the measures regarding police cooperation and the reinforcement of external border control and surveillance: initially dubbed "safeguards" in the initial Schenge agreement, they were relabelled "compensatory" in the Schengen convention of application, and "flanking" measures in the "Action Plan of the Council and the Commission on how best to implement the provisions of the treaty of Amsterdam on an area of freedom, security and justice" (see excerpt above).

31. The third tenet of the narrative of the EU as an internal space of freedom of movement is that freedom of movement applies homogeneously to all EU citizens. This assumption however, can be quickly dismissed. The recent process of enlargement has shown clearly, in this respect that the conditions of mobility enjoyed by EU citizens were differential, based on whether they are nationals of a 'new' or 'old' Member State, and whether their country has adhered or not to Schengen. Even more insidious than discrimination on the basis of nationality, in this respect, is the distinction based on barely disguised ethnic grounds – e.g. the situation of Roma and Sinti people in Italy (Merlino, 2009).

## 2. Security technologies and the policing of movers across borders: the generalisation and individualisation of controls.

32. The use of security technologies for the purpose of policing movers across the borders of the EU embodies a twofold demarche: on the one hand, the generalisation of controls, and on the other, their increasing individualisation. We need, however, to be more specific about individualisation: individualisation is not synonymous with personalisation, nor is it correlated with the authentication of a person's identity. Individualisation, in fact, involves the reduction of a given profile, composed of various categories of information, to a single unit. As argued by Scherrer, Guittet and Bigo:

[12] Which was further attenuated by the fact that the treaty of Amsterdam established a five-year transitional period where the right of initiative in the communautarised domains of JHA would be shared between the Commission and the Council.

[13] As of today, DG JHA (or Justice Liberty Security, as it was relabelled by commissioner Franco Frattini when the Barroso college came into office) features a very high ratio of seconded national experts. In the interviews conducted with officials from Commission services other than DG JHA, the latter was repeatedly pointed out as the one 'talking to the ministries of Interior' of the member states.

[14] On security as a technique of government, see Huysmans, 2006.

> Technologies for the securisation of mobility are increasingly conjugated with the absence of blockades, walls, checkpoints and barbwires. They move away from queues and individualised controls. They operate through the identification of the characteristics of a person within a flow, a mass of persons on the move. They are enacted through the tracing of the movement of a whole group and the anticipation of trajectories. Technologically, the speed of transmission of information only has to be higher than the speed of their physical movement for surveillance to win.
>
> (Scherrer, Guittet & Bigo, 2010: 13. Our translation)

33. These processes apply to EU citizens and non-citizens, albeit differentially. As Table 1 on the next page highlights, current and future EU databases contain information on both EU citizens and non-citizens. This is the case for the SIS and SIS-II, as well as for the VIS, which holds information on visa applicants but also on the person issuing the invitation to the visa applicant. We further consider the case of PNR databases, highlighting how a common modality can cover both EU and non EU nationals, while at the same time allowing for an individualisation of controls. The PNR also allow us to introduce another dimension, which we will not develop further in the context of the INEX project but might constitute an angle for future research, namely the transatlantic dimension of EU and US security practices. Finally, we examine the case of biometric identification, which is currently being put in place both for EU citizens and third-country nationals, in particular through the adoption of new travel and identity document standards.

34. Our interest in this section is not so much the description of the abovementioned systems than the process through which databases that were initially designed for different purposes, end up being harnessed for intelligence purposes by intelligence and police services. This process of "function creep" occurs through technology, through the development and implementation of technologies such as datamining or the possibility to run searches that independently connect individual files. What is interesting, in this respect, is that terminologies are changed through computer technologies. The SIS-I and its current "one4all" version[15], and the SIS-II, are not the same systems, despite the fact that they bear the same name, because they allow for searches that the SIS did not allow. The VIS seeks to go even further: firstly, by allowing the linkage of searches and the inclusion of biometric information, but also by rationalising the process of function creep.

[15] SIS –one4all was proposed in October 2006 by the Portuguese delegation (Council of the European Union, 2006b). Its main purpose, in the view of the delays incurred by development of the SIS-II (which was supposed to come online by 2007, in parallel with the scheduled enlargement of Schengen) was to allow for an extension of SIS-I to the ten most recent EU member states, through the "cloning" of the Portuguese N-SIS I. The proposal was accepted by the Justice and Home Affairs Council on 5 December 2006. See also Faure Atger (2008: 9).

**Table 1: Profile search categories and personal information in the main EU databases**

| Database | Profile search categories | Categories of personal information |
|---|---|---|
| SIS | ▪ Persons wanted for arrest/extradition purposes<br>▪ Third country nationals to be refused entry into the Schengen territory<br>▪ Missing persons (minors and adults) or persons that for their own protection need to be placed temporarily under police protection<br>▪ Persons to be put under surveillance or subjected to specific checks | ▪ Names and known aliases<br>▪ Specific physical characteristics<br>▪ Place and date of birth<br>▪ Gender<br>▪ Nationality<br>▪ Status: armed, violent or on the run<br>▪ Action to be taken |
| SIS-II | ▪ Persons wanted for arrest for surrender on the basis of a European Arrest Warrant or for extradition purposes<br>▪ Third country nationals to be refused entry into the Schengen territory<br>▪ Missing persons<br>▪ Witnesses and persons required to appear before judicial authorities<br>▪ Persons to be put under surveillance or subjected to specific checks | ▪ Names and known aliases<br>▪ Specific physical characteristics<br>▪ Place and date of birth<br>▪ Photographs<br>▪ Fingerprints<br>▪ Gender<br>▪ Nationality<br>▪ Status: armed, violent or on the run<br>▪ Action to be taken<br>▪ Links to other alerts in SIS-II |
| Eurodac | ▪ Applicants for asylum<br>▪ Persons apprehended in connection with the irregular crossing of borders coming from a third country. | ▪ Full ten fingerprints and control photographs of all persons from the age of 14<br>▪ Member State of origin |

| | | |
|---|---|---|
| | ▪ Persons found illegally residing in a Member State (not kept in the Eurodac Central Unit) | ▪ Place and date of asylum application or of apprehension<br>▪ Gender<br>▪ Reference number used by Member State of origin<br>▪ Date on which fingerprints were taken |
| VIS | ▪ Visa applicants<br>▪ Details of the person issuing invitation and/or liable to pay the applicant's subsistence costs during his stay | ▪ Application procedure and application history<br>▪ Fingerprints and digitised photograph<br>▪ Surname, surname at birth, first names<br>▪ Gender<br>▪ Date, place and country of birth<br>▪ Current nationality and nationality of birth<br>▪ Type and number of travel documents with issuing authority, date of issue and expiry<br>▪ Place and date of application<br>▪ Type of visa requested<br>▪ Main destination and duration of intended stay<br>▪ Purpose of travel<br>▪ Intended date of arrival and departure<br>▪ Intended border of first entry and/or transit route<br>▪ Residence<br>▪ Current occupation and employer<br>▪ For students, name of school<br>▪ For minors, name of father and mother |

### *2.1. The SIS: policing movements at a distance.*

35. The use of the Schengen Information System for the purpose of policing movers occurs mainly in the context of visa deliveries. This is an important point to highlight: the SIS is not designed for border guards and for border management, but for the policing of movements at a distance. Consultation of the SIS, in this respect, is an integral part of the procedures for delivering Schengen visas. The CCI specifies:

> *Verification of the visa applicant's identity* and verification as to whether an alert has been issued on the applicant in the Schengen Information System (SIS) for the purpose of refusing entry or verification as to whether the applicant poses any other threat (to security) which would constitute grounds for refusal to issue the visa or whether, from an immigration point of view, the applicant poses a risk in that on a previous visit he/she overstayed the authorised length of stay.
>
> (Council of the European Union, 2005b: 10)

This is consistent with the observation that, since its inception, the SIS has evolved mainly into a system of migration control, where valid entries on persons overwhelmingly concern the category of 'unwanted aliens' (Art. 96 records) – as highlighted by Table 2 below.

**Table 2: Proportion of Art.96 valid records in SIS, 2004-2008.**

| Year | Number of Art.96 valid records | Proportion of total valid records on persons |
|---|---|---|
| 2004 | 714 078 | Total valid records: 818673<br>Proportion of Art.96 records: 87% |
| 2005 | 751954 | Total valid records: 882627<br>Proportion of Art.96 records: 85% |
| 2006 | 752338 | Total valid records: 894776<br>Proportion of Art.96 records: 84% |
| 2007 | 696419 | Total valid records: 859300<br>Proportion of Art.96 records: 81% |
| 2008 | 746994 | Total valid records: 927318<br>Proportion of Art.96 records: 80% |

Source: Council of the European Union 2005a, 2006a, 2007, 2008, 2009a.

36. Inscription in the SIS for this category as for other records is the premise of Schengen Member States, as Art.96 underlines:

> 1. Data on aliens for whom an alert has been issued for the purposes of refusing entry shall be entered on the basis of a national alert resulting from decisions taken by the competent administrative authorities or courts in accordance with the rules and procedures laid down by national law.

> 2. Decisions may be based on a threat to public policy or public security or to national security which the presence of an alien in national territory may pose.
>
> This situation may arise in particular in the case of:
>
> (a) an alien who has been convicted of an offence carrying a penalty involving deprivation of liberty of at least one year;
>
> (b) an alien in respect of whom there are serious grounds for believing that he has committed serious criminal offences, including those referred to in Article 71, or in respect of whom there is clear evidence of an intention to commit such offences in the territory of a Contracting Party.
>
> Decisions may also be based on the fact that the alien has been subject to measures involving deportation, refusal of entry or removal which have not been rescinded or suspended, including or 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 aliens.

37. In this respect, the procedure for delivering Schengen visas, despite being dubbed 'uniform' for all EU Member States, is still highly reliant on the practices of national law enforcement (as regards the creation of records in the SIS) and consular authorities. It has to be noted, in this respect, that decisions to input a record in the system 'may arise' in the circumstances mentioned in Art.96.2(a) and (b) and 96.3, implying that there are other possibilities. Interpretations of this stipulation have in fact varied considerably from country to country: in the case of France, both the courts and the administration of the ministry of Interior have considered the motives laid down in Art.96 as limitative, but this is not the case of all Schengen Member States (Saas, 2003) Far from being a homogenising modality, in this respect, the Schengen Information System re-enacts and to some extent reinforces the piecemeal and arbitrary outlook of the visa delivery procedure.
38. The information currently available on the SIS-II confirms the trends identified above (see Amicelle & al., 2009). One item of concern in this respect is the planned evolution from "one-to-one" to "one-to-many" biometric searches in the system. "One-to-one" searches involve running the biometric information obtained from a person against the record held in the system on the same person. "One-to-many" searches, however, moves beyond such a verification of identity towards the use of the system for identification purposes[16]. In addition, it is envisaged that at a later stage the system might be holding DNA profiles and retina scans (Hobbing & Kosloswki, 2009: 6-7). Finally, as we have argued in our previous deliverable, the various evolutions in the legislation related to SIS-II have since its inception in 1996 have led to a general broadening of access to the system, to a large number of EU and national security agencies, bodies and services, transforming it into a general purpose intelligence database[17] for the objective of policing movements at a distance.

[16] Without this requiring any additional legislative act. The Commission's DG JLS, in this respect, seems to envisage this evolution as a mere matter of implementation and technical development, whereas it would fundamentally change the outlook of SIS-II. See the examination of Jonathan Faull, director of DG JLS and officials Frank Paul and Marie-Hélène Boulanger by the House of Lords' European Union Committee (House of Lords, 2007: 89-102).

[17] As ascertained by Art.1(2) of Regulation (EC) No 1987/2006 and of Council Decision 2007/533/JHA which both state that the SIS II is being established with the very broad purpose of "ensur[ing] a high level of security within the area of freedom, security and justice of the European Union".

### *2.2. The Visa Information System: the generalisation of biometrics and the broadening of access.*

39. To this date, the VIS has still to come online. Therefore, most of the elements presented in this subsection concern the potential operations conducted through the system, and how they converge/diverge with current practices.

40. The most visible has been the increase in the administrative fees paid by applicants to a Schengen visa, from 35 to 60 euros. This increase was supported in particular by the French government, which tied it to the additional costs incurred by the requirement to introduce biometrics in the visa application procedure (Beaudu, 2009: 114) – a development confirmed by recitals (4) and (5) of the related Council decision:

> (4)The amount of EUR 35 no longer covers current visa application processing costs. Moreover, the consequences of the introduction of the European Visa Information System (VIS) and the biometrics required to introduce the VIS in the visa application examining process should be taken into account.
>
> (5) The current amount of EUR 35 should be readjusted accordingly in order to cover the additional costs of processing the visa application corresponding to the introduction of biometrics and the VIS.
>
> (Council Decision 2006/440/EC)

41. A second effect of the yet-unused VIS has been the generalisation of the issuance of biometric visas by Member States, in anticipation of the coming online of the system, and despite the absence of a specific EU legal basis[18]. Indeed, following on the call issued by Member States governments in the conclusions of the Veria Informal JHA Ministers' meeting of 28-29 March 2003, and reiterated in the conclusions of the 19-20 June 2003 Thessaloniki European Council, the Commission tabled in September 2003 a proposal for amending Regulations (EC) 1683/95 on a uniform format for visas and (EC) 1030/2002 on a uniform format for residence permits, to include biometric features in these documents (European Commission, 2003). The proposal concerning residence permits was finally adopted on 18 April 2008[19] while the proposal concerning visa formats was withdrawn in its initial form. The legal basis for the collect of biometric identifiers by Member State consular posts was subsequently established by an amendment to the CCI, proposed by the Commission in May 2006 (European Commission, 2006a) and adopted by the Parliament and the Council on 23 April 2009[20]. In the meantime, however, the collection of biometric data for the purpose of delivering travel authorisations has become established practice among Member States diplomatic and consular representations. French consular posts, for instance, have been systematically collecting biometric data and delivering biometric visas since October 2008 for short stays but also for other purposes of travel (e.g. long stays for students, workers or family members).

---

[18] For visas, this development has been justified on the basis of the Council decision establishing the VIS (2004/512/EC), which, however, does not lay down any specific provisions regarding the organisation, procedures and rules to be applied. Decision 2004/512/EC merely establishes the legal base to initiate the development of the system, and should not be confused with the 'VIS Regulation' per se which was adopted in July 2008 (Regulation (EC) No 767/2008).

[19] Council Regulation (EC) No 380/2008.

[20] Regulation (EC) No 390/2009.

42. The VIS opens up the perspective of collecting personal and biometric data on a much larger scale than what has been done so far in the EU. As highlighted in Table XX above, the number of valid records on persons contained in the SIS between 2004 and 2008 oscillated between 818673 (2004, lowest figure) and 927318 (2008, highest figure). By contrast, the VIS is expected to store 20 million visa applications annually, which would result, according to the estimate of the Art.29 Working Party, in the storing of 70 million sets of fingerprints over the 5-year period during which data is supposed to be conserved within the database (DPWP, 2005: 6). In this respect, the VIS will collect biometric data from all applicants from the age of six – the other major biometric database in the EU, Eurodac, starts from the age of fourteen - without any upper limit of age, and this despite the fact that biometrics are known to be unreliable for young children and elderly persons. Furthermore, whereas the SIS is used in the context of visa applications to check whether an applicant already has a record in the system, the VIS will be used to systematically collect personal information on all applicants, regardless of the outcome of the application process: as Art.8 of the VIS Regulation specifies, records are to be created by consular officers 'on receipt of an application', for all categories of short-stay visas covered by the 'uniform' Schengen visa, including long-stay visas in specific circumstances:

    (a) 'short-stay visa' as defined in Article 11(1)(a) of the Schengen Convention;

    (b) 'transit visa' as defined in Article 11(1)(b) of the Schengen Convention;

    (c) 'airport transit visa' as defined in part I, point 2.1.1. of the Common Consular Instructions;

    (d) 'visa with limited territorial validity' as defined in Articles 11(2), 14 and 16 of the Schengen Convention;

    (e) 'national long-stay visa' as defined in Article 18 of the Schengen Convention;

    (Council Regulation (EC) No 767/2008, Art.4(1)

43. The generalisation of biometrics as a requirement for Schengen visas in anticipation of the VIS has had two further, interrelated effects. The first one is the requirement for the applicant to appear in person at the consular post where s/he is applying, which, in countries where consular offices are concentrated in the capital city, can prove a problem. Personal appearance was already a quasi-obligation prior to the introduction of biometrics, but the CCI provided for a (very limited) measure of flexibility in this respect:

    As a general rule, the applicant shall be called on to appear in person in order to explain verbally the reasons for the application, especially where there are doubts concerning the actual purpose of the visit or the applicant's intention to return to the country of departure […] This requirement may be waived in cases where the applicant is well-known or where the distance from the diplomatic mission or consular post is too great, provided that there is no doubt as to the good faith of the applicant and, in the case of group trips, a reputable and trustworthy body is able to vouch for the good faith of those persons concerned.

    (Council of the European Union, 2005b: 9)

With the introduction of biometrics, this already narrow degree of flexibility disappears since applicants are obliged to be present in order to have their fingerprints recorded - unless the consular post in question has 'externalised' parts of the visa application procedure to a private body.

44. Externalisation of visa application procedures is another development that has been allowed in the move towards the establishment of the VIS. The first reports on such practices have been issued in 2004-2005 (Beaudu, 2007), and are currently developing significantly among Member State consular and diplomatic missions. Externalisation initially covered domains such as the making of appointments (usually through contracting with call centres), the provision of information to applicants (on the visa procedure itself or on the status of their application), the receipt of visa applications and their transfer to consular posts, the perception of visa fees, and the restitution of her/his passport to the applicant at the end of the procedure (Beaudu, 2007). It is only in 2009 that a legal framework was established in EU law, through the adoption of Regulation (EC) No 390/2009 amending the CCI and which we have already discussed above. The regulation establishes the possibility for Member States to use the services of external service providers:

> Member States shall endeavour to cooperate with an external service provider together with one or more Member States without prejudice to public procurement and competition rule.
>
> Cooperation with an external service provider shall be based on a legal instrument that shall comply with the requirements set out in Annex 19.
>
> Member States shall, within the framework of local consular cooperation, exchange information about the selection of external service providers and the establishment of the terms and conditions of their respective legal instruments.
>
> (Regulation (EC) 390/2009: 6)

The domains for which external service providers can be solicited are:

> (a) providing general information on visa requirements and application forms;
>
> (b) informing the applicant of the required support documents, on the basis of a checklist;
>
> (c) collecting data and applications (including collection of biometric identifiers) and transmitting the application to the diplomatic mission or consular post;
>
> (d) collecting the fee to be charged;
>
> (e) managing the appointments for personal appearance at the diplomatic mission or consular post or at the external service provider;
>
> (f) collecting the travel documents (including a refusal notification if applicable) from the diplomatic mission or consular post and returning them to the applicant.
>
> (Regulation (EC) 390/2009: 6-7)

The regulation thus consecrates the practice and possibility for private bodies to collect biometric data for the purpose of visa applications. It further stipulates that Member States are responsible and liable for the activities of external service providers, including with regard to the personal data of applicants:

> The Member State(s) concerned shall remain responsible for compliance with data protection rules for the processing of data and shall be supervised in accordance with Article 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
>
> Cooperation with an external service provider shall not limit or exclude any liability arising under the national law of the Member State(s) concerned for breach of obligations with regard to the personal data of applicants and the processing of visas. This provision is without prejudice to any action which may be taken directly against the external service provider under the national law of the third country concerned
>
> (Regulation (EC) 390/2009: 7)

This implies, in particular, that Member States and not external service providers are considered as data processors[21] and can be investigated as such by national data protection supervisors. It is, however, up to the Member State diplomatic mission or consular post to take action against the service provider 'under the national law of the third country concerned' – which means, in other words, that the degree to which services providers are held liable will vary significantly from country to country and from one Member State representation to the other.

45. Externalisation raises a series of questions beyond the issue of liability and the possibility for TCNs to seek redress. Firstly, it has been proved to contribute to a rise in the overall price of the Schengen visa ranging from 15 to 75% (Beaudu, 2007). Regulation (EC) 390/2009 basically validates this trend, while laying down basic rules:

> External service providers may charge a service fee in addition to the fee to be charged as set out in Annex 12. The service fee shall be proportionate to the costs incurred by the external service provider while performing one or more of the tasks referred to in point 1.5.
>
> […]
>
> The service fee shall not exceed half of the amount of the visa fee […] irrespective of possible exemptions from the visa fee…
>
> (Regulation (EC) 390/2009: 8)

These provisions, however, only cover the domains evoked above. They do not cover optional services that providers can offer to potential visa applicants such as picture-taking, assistance to fill in visa forms, travel insurance or mailing of the applicant's passport to his personal address (Beaudu, 2009: 113). In addition, the regulation does not address the

[21] *I.e.* according to Directive 95/46/EC, 'a natural or legal person, public authority, agency or any other body which process personal data on behalf of the controller' (Article 2(e).

difference in service fees from country to country: it only establishes that Member States 'shall aim to harmonise the service fee applied' in the context of 'local consular cooperation' (Regulation (EC) 390/2009: 8). Finally, while Member States are bound by the regulation to respect 'public procurement and competition rules' (Regulation (EC) 390/2009: 6), the current practice shows that one company in particular, VFS Global[22] (Beaudu, 2009: 112), is enjoying a strongly dominant position.

46. We have focused significantly on the 'external' surface of the VIS, *i.e.* its effects in the context of visa applications procedures and before travellers actually enter the EU. But, similarly to the SIS/SIS-II, the VIS will also operate internally, reactivating the border for TCNs within the territory of the Member States. This involves in particular the possibility built in the VIS for alerts to be emitted on persons who are believed to stay in the EU after their visa has expired, as well as the extended possibilities of access to the VIS for a growing range of security agencies, bodies and services. In addition, one has to draw attention to the fact that the VIS will be storing information on the persons issuing an invitation to an applicant or liable for the applicant's subsistence costs – whether they are EU citizens or long-term residents. Although not presented as a category of profile search but as a category of information tied to the individual files of applicants, it is unclear how this information will be used by the services which will be granted access to the VIS.

### *2.3. EURODAC: asylum, migration and the temptation of conflation.*

47. Eurodac is the first EU-wide biometric database – in technical terms, an 'Automated Fingerprint Identification System' (AFIS) – established in 2000[23], and operational on 15 January 2003[24]. Eurodac was established to participate in the application of the 1990 Dublin convention, to help establish which participant state is responsible for the reception of an asylum application as well as to prevent so-called 'asylum shopping' (*i.e.* to prevent persons in search of international protection to submit multiple asylum applications among the parties to the convention). Eurodac concerns only third country nationals – indeed, citizens of an EU Member State cannot claim asylum in another Member State[25].

48. Eurodac, however, is also used for purposes of migration control. The Eurodac regulation distinguishes between three categories of movers: 'applicants for asylum' (Chapter II), 'aliens apprehended in connection with the irregular crossing of an external border' (Chapter III)

---

[22] Based in Mumbai, India, and part of the Zurich-based Kuoni Travel Group, VFS Global was established in 2001. On its website, it presents itself as 'a specialist partner for diplomatic missions worldwide […] VFS serves diplomatic missions by managing all the administrative and non-judgemental tasks related to the entire lifecycle of a visa application process, enabling diplomatic missions to focus entirely on the key tasks of assessment and interview' (VFS Global website: http://www.vfsglobal.com/). VFS Global outsources visa procedures for the following EU Member States: Austria, Belgium, Bulgaria, Czech Republic, Denmark, France, Germany, Greece, Ireland, Italy, Malta, Netherlands, Portugal, Spain, Sweden and the United Kingdom. It also services other governments: Australia, Canada, China, Iceland, India, Russia, Singapore, Switzerland, Thailand, the United Arab Emirates and the United States. In total, the company claims to be processing 'in excess of 7 million visa applications (contracted) annually' (VFS Global website: http://www.vfsglobal.com/).

[23] Regulation (EC) No 2725/2000.

[24] For an overview of the establishment of Eurodac and the lay-out of the system, see our previous deliverable (Amicelle & al., 2009) as well as the remarkable study of Evelien Brouwer (2008: 118-121).

[25] The Protocol on Asylum for Nationals of the Member States (Aznar Protocol) attached to the Amsterdam Treaty establishes that citizens of an EU Member State cannot apply for asylum in another, which '[g]iven the level of protection of fundamental rights and freedoms' that they guarantee, are all considered as 'safe countries'. This, of course, is not without raising questions, for instance with regard to the case of political activists whose activities are considered as pertaining to terrorism by the authorities of their country (e.g. Guittet, 2004, for the case of Spain).

and 'aliens found illegally present in a Member State' (Chapter IV). Different rules of data transmission and conservation apply to these three categories of persons. Fingerprints of persons applying for asylum are to be stored for ten years. The duration is of two years for persons crossing irregularly an external border, while data on persons found illegally present within the territory of a Member State is only transmitted to the Eurodac Central Unit for purpose of comparison with the fingerprints of applicants for asylum already entered in the system, but are not recorded (Brouwer, 2008: 124-125). Both categories are normally used to ascertain which Member State should take responsibility for readmitting the person and/or receiving an asylum application from that person.

49. Eurodac mainly operates as a distribution mechanism for asylum seekers among the parties to the Dublin Convention (Brouwer, 2008: 126). There are, however, some doubts as to the ways the system is used by Member States authorities. This uncertainty looms in the background of the three annual reports on Eurodac published by the European Commission (2004, 2005a, 2006b), as well as the two reports published so far by the Eurodac Supervision Coordination Group (2007, 2009), and concerns the 'special searches' which is originally provided for by Article 18(2) of the Eurodac Regulation for data protection purposes[26]. The Commission's first annual report, in this respect, observes that:

> During the last year, the Central Unit has registered a significant number of "special searches" […] It should be remembered that the national data protection authorities are responsible for monitoring the lawfulness of the processing of personal data by the Member States. However, representatives of these authorities gathering at their meeting in January 2004 could not corroborate this information regarding the "special searches" launched in their own countries.
>
> It also appears that some Member States almost always use the same or a very short range of user identifiers for performing the electronic transactions with the Central Unit […] The Commission services note that Member States never notified the penalties which would be applicable in case of a misuse of the data recorded in the Central Unit database…
>
> (European Commission, 2004: 15)

In the following report, the Commission indicates that:

> In 2004, the Central Unit registered a surprisingly high number of "special searches" […] The number of "special searches" ranges from 1 to 611 across all Member States […] The important increase compared to last year was mainly due to two Member States while a few other Member States continue to apply this provision frequently […] As in 2003, some Member States continue to use almost always the same or a very short range of user identifiers for performing the electronic transactions with the Central Unit. Existing data protection rules require that each Member State can identify the persons or bodies responsible for the processing (controllers) of the personal data

[26] Article 18(2) thus states: 'In each Member State any data subject may, in accordance with the laws, regulations and procedures of that State, exercise the rights provided for in Article 12 of Directive 95/46/EC […] Without prejudice to the obligation to provide other information in accordance with point (a) of Article 12 of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him/her recorded in the central database and of the Member State which transmitted them to the Central Unit. Such access may be granted only by a Member State'.

> exchanged within EURODAC. In the same context, Member States must keep an up-to-date list with the designated authorities that have access to data from EURODAC and communicate it to the Commission…
>
> (European Commission, 2005a: 14)

The same concern is echoed in the 2006 report, to the extent that 'the Commission services have alerted the European Data Protection Supervisor (EDPS) and contacted bilaterally a Member State of particular concern' (European Commission, 2006b: 10)[27]. Accordingly, special searches were given accrued attention by the Eurodac Supervision Coordination Group[28]. The report remains evasive as to the exact implications of this discrepancy in the use of the 'special search' function of Eurodac by Member State authorities[29]. The report clarifies some of the 'special searches' as occurrences of manual errors, or misunderstandings regarding the possibility to train staff on Eurodac and test the system itself. Its overall conclusion, however, is somewhat surprising: firstly, that in '8 [!] Member States (a third of the Member States participating in the coordinated inspection), the Eurodac Regulation was fully complied with' (Eurodac Supervision Coordination Group, 2007: 9), while in 3 Member States 'staff has been incorrectly trained as regard special searches and uses them either as CAT3 searches[30] or in order to check the data already fed into the system previously, when there is a suspicion that data needs to be corrected' and in '2 Member States, no explanation at all has been received in the course of this inspection' (Eurodac Supervision Coordination Group, 2007: 10).

It seems clear, then, that there remains a lingering concern with the 'temptation' (Brouwer, 2002) of using Eurodac for purposes other than the ones listed in the Eurodac regulation – *i.e.* for policing purpose, through cross-referencing with information held in other databases or even interoperability between these databases. In this regard, the 'temptation' of Eurodac has been regularly reactivated, either by Member State governments or the European Commission – *e.g.* in its 2005 communication on 'improved effectiveness, enhanced interoperability, and synergies among European databases':

> The EURODAC Regulation is also under-exploited. Although the EURODAC Regulation obliges Member States to take fingerprints of all persons aged over 14 who cross their borders irregularly and cannot be turned back, the quantity of such data sent to EURODAC is a surprisingly low fraction of the total migratory flow.
>
> (European Commission, 2005b: 5)

The communication thus proceeds to highlight 'the absence of access by internal security authorities' to the VIS, SIS-II immigration data and EURODAC data as a 'shortcoming'

[27] The report further specifies that '[s]ome national authorities have already informally explained the reasons for such a frequent use of this special category of searches. Namely, such transactions which do not lead to storage of data, would be used in cases where the responsible authorities have lost track of a previous transaction they have made and therefore lost the fingerprints sent back by the EURODAC Central Unit when a hit occurred' (European Commission, 2006b: 10). The use of the conditional in this remark is worth noting.

[28] Composed of representatives from each Member State Data Protection Authority (DPA) and of the European Data Protection Supervisor (EDPS).

[29] The 2007 report limits itself to observing: 'The main concern is the following: if the number of requests for access by individuals does not match the number of special actually performed, this discrepancy needs to be explained' (Eurodac Supervision Coordination Group, 2007: 9).

[30] CAT3 searches concern undocumented aliens.

(European Commission, 2005b: 6) and to make a number of suggestions in this regard, including 'more consistent introduction and use of certain data (for example SIS II alerts on persons who are likely to commit serious criminal offences and EURODAC data on irregular border-crossers, etc.) should be made by Member States.

50. The transformation of the purpose of Eurodac from an administrative tool implementing the Dublin convention into an instrument of law enforcement and intelligence is currently underway. In September 2009, the Commission introduced a proposal for a Council Decision opening the possibility for Member State law enforcement authorities and Europol to request comparisons with Eurodac data (European Commission, 2009b)[31]. Recital (6) of the proposal quite explicit as to the remit of the envisaged modification to the use of Eurodac:

> Since EURODAC has been established to facilitate the application of the Dublin Regulation, access to EURODAC for the purpose of preventing, detecting or investigating terrorist offences and other serious criminal offences *constitutes a change in the original purpose of EURODAC*, which interferes with the right to respect the private life of individuals whose personal data are processed in EURODAC.
>
> (European Commission, 2009b: 10. Emphasis added)

The proposal follows, but is kept separate from, the 'recast' of the Eurodac Regulation initiated by the European Commission in December 2008[32]. As summed up by the EDPS in his opinion of 7 October 2009:

> The proposals establish the basis for the right of designated authorities of Member States as well as Europol to request a comparison of fingerprint data or a latent copy with the EURODAC data. A successful comparison which results in a 'hit' reply from EURODAC will be accompanied by all the data that is held in EURODAC regarding the fingerprint. Requests for supplementary information following a hit are not regulated in the proposals but are covered by existing instruments on the exchange of law enforcement information.
>
> (EDPS, 2009: 2)

In other words, the proposal would allow Member States' law enforcement bodies and Europol to check fingerprints gathered in the course of an investigation against the data held in the Eurodac Central Unit[33] and, in the case of a 'hit', obtain all the information linked to

---

[31] We will not run a full assessment of the proposal. See the opinion by the EDPS (2009) and the note by the Meijers Committee (2009) for a detailed overview.

[32] See European Commission, 2008b for the original proposal, and European Commission, 2009a, for the amended version of the text (after first round of Council discussions and European Parliament amendments).

[33] Article 7(1) of the Commission proposal specifies that: 'Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprints databases and of the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA result negative'. It further lays down three conditions for comparison requests, namely that 'the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious crime offences', or that 'the comparison is necessary in a specific case', or finally that 'there are reasonable grounds to consider that such comparison with EURODAC data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question' (European Commission, 2009b: 15-16). Council Decision 2008/615/JHA incorporates in the Community framework the main elements of the Prüm Treaty (on the latter see Balzacq et al., 2006, Bellanova, 2008).

the concerned set of fingerprints (see Table 1 *supra* for the data categories contained in Eurodac) – including information on the Member State which was responsible for entering the data in the system in the first place, thus paving the way for additional exchanges of information. In this sense, Eurodac would depart from its original, 'hit/no hit' functioning, and the use of 'special searches' for purposes other than Article 18(2) of the initial Eurodac Regulation would be legalised. The purpose of Eurodac would then be modified, and the database turned into a general purpose intelligence database.

### *2.4. The life of data: PNR databases*

51. The question of PNR databases might give some further insights regarding the running themes of this section. It has to be noted that, although there are currently no EU-wide PNR systems – a proposal was nonetheless tabled by the Commission in November 2007 (European Commission, 2007c) – the issue of PNR data has become a tug of war within the European governmental arenas with regard to persistent requests from the US to be granted access to EU airline companies PNR data related to transatlantic flights.

52. **What it is.** PNR started as a database holding booking information of air travellers. A PNR record comprises 34 fields of data, including name, address, telephone numbers, email address, information on bank numbers and credit cards, but also more potentially sensitive information such as meals ordered for the flight. (Brouwer & Guild 2006:1).

53. The first PNR (commercial) database, SABRE, was established in 1959 as a computer reservation system (CRS), managed by airline companies; CRS later evolved into global distribution systems (GDS), four of which are currently in operation: Amadeus (only EU-based GDS), Galileo, SABRE and Worldspan which are all based in the US (Hobbing, 2008: 4). The use of PNR data by security agencies was initiated in the US in the late 1990s, after the destruction of TWA Flight 800 and the Centennial Olympic Park bombing in 1996[34], through the CAPPS (Computer Assisted Passenger Prescreening System) system, which was run by airline companies themselves. CAPPS I ran checks of PNR data against the US Transport Security Agency (TSA) terrorism watch lists, but only focused on passengers with check-in luggage. It was decommissioned after the 11 September 2001 attacks, and replaced in 2003 by CAPPS II, which was managed by the TSA. Despite the similarity in names (cf. our discussion of SIS, SIS one4all and SIS II in the introduction to this section), CAPPS II embodied a different logic: the PNR data of all passengers flying to the US were checked against both government and private databases, a process which resulted on the issuance of a risk score, which could result in "no fly" decisions. Concerns with high error rates, lack of transparency and effective remedy and problematic use of private data led to the cancellation of CAPPS II. In the meantime, the US Customs and Border Protection (CBP, under the remit of the Department of Homeland Security – DHS) had already been extending its Automated Targeting System (ATS), initially conceived for watching sea cargo, to monitor travellers[35]. In the description provided by the DHS in the ATS "Privacy Impact Assessment" of November 2006:

> ATS is an Intranet-based enforcement and decision-support tool that is the cornerstone for all CBP targeting efforts. CBP uses ATS to improve the

[34] Information in this paragraph is derived from Hobbing (2008: 13-15).

[35] ATS is currently the main system dealing with PNR in the US. Another system, dubbed Secure Flight, was established by the DHS in 2007. However, due to security vulnerabilities in the system and in the terrorist watch lists against which Secure Flight is supposed to run PNR data, the programme has officially been halted until 2010 (Hobbing, 2008: 15).

> collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. Additionally, ATS is utilized by CBP to identify other violations of U.S. laws that are enforced by CBP […] ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveller, import, or export in context with previous behaviour of the parties involved. Every traveller and all shipments are processed through ATS, and are subject to a real-time rule based evaluation
>
> […]
>
> ATS receives various data in real time from the following different CBP mainframe systems: the Automated Commercial System (ACS), the Automated Export System (AES), the Automated Commercial Environment (ACE), and the Treasury Enforcement Communication System (TECS). ATS collects certain data directly from commercial carriers in the form of a Passenger Name Record (PNR). Lastly, ATS also collects data from foreign governments and certain express consignment services in conjunction with specific cooperative programmes.
>
> ATS accesses data from these sources, which collectively include electronically filed bills, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land-border crossing and referral records for vehicles crossing the border; airline reservation data; non-immigrant entry records; and records from secondary referrals, incident logs, suspect and violator indices, and seizures.
>
> (DHS, 2006: 2)

54. The purpose of this somewhat lengthy excerpt is to highlight the logics underpinning practices of datamining. Indeed, what comes out of the DHS' description is that ATS is essentially a datamining tool, based on the contrasting of information categories against pre-established profiles (the so-called "real-time rules based evaluation"). One ambiguity, in this respect, is the claim that ATS is a "real-time" instrument, which might lead to the conclusion that it does not store data per se. In fact, a close reading of the DHS' ATS privacy assessment shows that ATS does store personal information, in two qualities: the "primary" information, on the one hand, and the "secondary" information (i.e. profiles) on the other:

> The retention period for data in ATS reflects the underlying retention period for the data in its source records (for example, since the data from ACS, AMS, and ACE is retained for six years, the associated information in ATS is only retained for that period of time). Provided the data is not associated with an open investigation (in which it is retained until the investigation is closed), this retention period will not exceed forty years for the source record data and is forty years for the risk assessment and associated rules upon which the assessment is based.
>
> Generally, data maintained specifically by ATS will be retained for up to forty years. Certain data maintained in ATS may be subject to other retention

> limitation pursuant to applicable arrangements (e.g., PNR information derived from flights between the U.S. and the European Union). Cost and performance impact of data retention may lead to retention periods less than forty years.
>
> (DHS, 2006: 11)

More precisely, although this does not appear explicitly until the very last pages of the privacy statement, ATS is the "source record" for PNR data, including data obtained from EU based airline companies.

55. ATS stresses the logic that we were highlighting in the introduction to this section, i.e. the idea that the "function creep" observable in certain technical systems is enabled through the use of other security technologies. The datamining and profiling functions of ATS allow for the generation of new categories of data, which become themselves information to be stored and to which specific, separate rules of data retention then apply – a form of digital "double penalty" as it were. The ATS example, in this regard, also highlights the point on individualisation that we introduced earlier on: the crux of the system is not to "know" a person, but to reduce a given risk profile to the "unit" that fits into this profile.

56. US insistence on collecting PNR data created a real issue for European airline companies, who were prevented from complying by EU legislation on data protection. Despite this fact, after 2003, the sharing of the information with US authorities became mandatory, and a fine of up to US$ 5,000 was set up for each passenger whose data could not be obtained by the US authorities. (Evelien Brouwer and Guild 2006:1). An urgent agreement was therefore needed.

57. **Data protection in the EU.** In the member countries of the European Union, the protection of data is regulated at the European level since 1995 by Directive 95/46/EC[36], which according to the European Commission ensures

> 'a high standard of protection for personal data throughout the EU [and] has brought considerable benefits for citizens, business and authorities'.('Communication from the European Commission to the European Parliament and Council on the follow-up of the Work Programme for better implementation of the data protection directive', COM(2007) 87 final, 7 March 2007, p 2.) quoted in Kosta (2007:347)

58. However, even if covered by other European treaties[37] the specificity of the European institutions is such that the data protection regime does not apply to the second and third pillars of the EU, as stated in article 3(2):

> This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing

[36] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', *Official Journal* L 281, pp 31–50, 23 November 1995

[37] In particular Article 8 of the Convention on Human Rights, Convention 108 of the Countril of Europe for the protection of individuals with regard to automatic processing of personal data.

operation relates to State security matters) and the activities of the State in areas of criminal law.

59. **The negotiations.** It was decided by all member states that the European Commission would centralize the negotiations with the US. In order to ground it in EU law - and in particular in the context of Directive 95/46, it was necessary to consider the exchange of PNR information as a first pillar activity, namely as the sharing of commercial information (Hailbronner, Papakonstantinou, et al. 2008:189). This meant, that according to article 25(2) of the directive, the criterion of 'adequacy' was met:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

60. This decision allowed for the signature of an agreement on 17 May 2004 between the United States of America and the European Community. The latter based the agreement on two decisions stating the congruence of the agreement with EU law[38]. The agreement was however hotly contested, and the European Parliament - who had not been consulted for the agreement, and was eager to reinforce its institutional power - took initiative against those two decisions in front of the European Court of Justice, arguing of both infringement of fundamental rights, and the lack of legal authority to base the decisions. The European Data Protection Supervisor, recently created, supported the Parliament's initiative. (Hailbronner, Papakonstantinou, et al. 2008:190).

61. It took two years to the court to reach a decision[39]. On 30 May 2006, without entering the detail of the Parliament's claims and in particular the question of the infringement of fundamental rights, the court judged that the 2004 agreement was simply unlawful. According to the court, the PNR agreement did not fall under commercial matters, but was clearly an issue of security, fight against terrorism and organized crime. As such, it fell under the third pillar, which the EU had not competence for, and therefore EC directive 95/46 could not apply.

62. In July 2006, negotiations started for a new PNR Agreement. This time, it was the council that would take the lead. Under the Finnish Presidency, a new interim PNR agreement was signed on 18 October 2006 with validity until 31 July 2007. The agreement referred to the Undertakings by the Department of Homeland Security (DHS) incorporated in the first PNR Agreement and was later amended by a later agreement. This time however, the agreement was no longer subject to the Parliament scrutiny. Another difference with the initial PNR Agreement is that on the US side, not only the CBP, but other agencies such as the Immigration and Customs Enforcement (ICE) and the office of the Secretary, among others,

---

[38] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, p. 83, and corrigendum at OJ 2005 L 255, p. 168) and Commission Decision 2004/535/EC on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection .

[39] CNS/2004/64

have access to the PNR records (Evelien Brouwer and Guild 2006:1, Hailbronner, Papakonstantinou, et al. 2008:190). A subsequent agreement was signed on July 2007, and a short time afterward, the Bush administration excluded one part of the DHS' database network, namely the Arrival and Departure System (ADIS) and the Automated Target System from the 1974 privacy act. 40.

63. **What is at stake.** Throughout its institutional itinerary, the PNR agreement has remained highly controversial, raising concern from both institutional and non-institutional actors. The European Parliament has been highly critical of the different versions of the accord, independent commissions have regularly pointed out flaws on the EU and US side, and the DHS itself has acknowledged several limits in its ability to fulfil the requirements of data protection of passenger's information - whether they are EU citizens or not.

64. A first, general point to be acknowledged is the principle of the agreement is reciprocity, a basic principle of international law. Accordingly, the EU could require from US airlines coming to Europe the same data that the US demands to EU airlines. Yet the US does not have a system of registration for citizens and legal foreign residents. Therefore the US approach, more lenient in terms of its own citizens and legal foreign citizens could arguably undermine the accord (Hailbronner, Papakonstantinou, et al. 2008:196).

65. However recurrently throughout the past decade, the highest concern regards the quantity of data that is transmitted to the US authorities, and the capacity of the US to comply with the "adequacy" requirement of the agreement. The question of the quantity of data is related to the method by which PNR data is obtained/retrieved. The "push" systems consist in EU based airline companies sending the requested information to the US authorities. The "pull" system, instead, means granting access to the DHS (and possibly other US agencies) full access to the PNR data. While the US advocated for a "pull" access, the European side advocated a "push" system, which was eventually adopted in the agreement. Yet in practice, as argued by Hailbronner et al (2008)

> the essence of the PNR Agreement abolishes in practice any significance to that distinction from a data protection perspective, since DHS controls what kind of PNR data are collected and which categories are transmitted. (Hailbronner, Papakonstantinou, et al. 2008:193)

Paradoxically, however, the "push" system has become a modality of resistance for a variety of EU actors – albeit for different reasons - confronted with US requests

66. The "Adequacy Requirement"[41] - meaning the trust that the EU institutions put in the third country institutions in guaranteeing the same level of protection of the data as in the EU - has been a repeated point of contestation, by EU parliament, NGOs such as Statewatch or the several working groups that have carried out surveys in this regard. In September 2005, a US-EU team conducted a joint review in Washington, D.C. on the implementation by the US CBP of the Undertakings as set out in the Commission Decision 2004/535 of 14 May 2004[42] The joint commission found its access to institutions severely limited and subject to confidentiality agreements. The commission found that the compliance, on the US side had only arrived late, and therefore the US authorities had operated from 2004 to 2005 without

[40] See Statewatch: "US changes the privacy rules to exemption access to personal data" URL: http://www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm, visited 2/2/2010

[41] As established by the Commission Decision 2004/535/EC

[42] Commission Staff Working Paper on the Joint Review, 12.12.2005, revised version (see http://www.statewatch.org/news/2006/jun/eu- usa-pnr-com-review-2005.pdf) quoted in Brouwer (2006:2).

complying to the agreement in terms of data protection. At stake was the collection of more data then permitted, and in particular the intention by US authorities to maintain a "pull" system, even if the agreement had been on a filtered "push" system. Similarly, the European Data Protection Working Party (established on the basis of Article 23 of the EC Directive 95/46 raised several times its concern over the level of protection guaranteed by the CBP [43].

67. As argued by Brouwer and Guild (2006), even if eventually the US will comply to the data protection standards currently in place in the EU, it leads to the conclusion that "the compliance of the US authorities with the agreements as adopted between US authorities and the EC is not a matter-of-course" (Evelien Brouwer and Guild 2006:2) and that constant monitoring of the life of data outside the EU borders is necessary.

68. In addition to allowing for datamining practices, the question of PNR data, in which sensitive information such as meal preferences allow the US authorities to already target Muslims according to their dietary preferences - in addition to the interpretation that can be made of first names, last names and credit card information - shows a practice of pro-active policing that does not make a difference between citizens and non-citizens. There is therefore a high risk of ethnic profiling to which both EU citizens and TCN are submitted, without even knowing it. The PNR data transmission is in fact part of these new technologies of control which, because they are not directly acknowledged by the person subjected to the control are deemed to be less invasive and more respectful of the freedom of the travellers; preventing the unwanted to travel, allowing for the majority to do so without the feeling of being controlled. A notion well encapsulated in the idea of "smart borders".

### *2.5. Biometrics, "smart borders" and data doubles*

69. At the core of the promotion of biometric technologies lies the assumption that documents - including national identity documents - are not a reliable source of information to identify a person and locate her or him in an array of statistical information that might help determine her or his level of 'danger'. Two elements are therefore central in this perspective: first, it is the body itself that is believed to tell the truth about an individual's identity. Second, citizenship is only one of the possible markers that contribute to the profiling of an individual, to the assessment of the level of risk that a person might present in terms of security. In this context, and although it has not been smooth and linear process, it is not surprising that biometric identification techniques have progressively crossed the border marking the limit between TCNs and EU nationals.

70. As shown in the previous section, biometric identifiers were initially introduced at the European level as a technology of security in relation to the question of immigration. First in terms of asylum, the objective of the introduction of biometry was to produce a 'reliable identity' for asylum seekers. This led to the creation of the establishment of Eurodac. Secondly, this logic is currently being expanded to other categories of movers, through the SIS II and VIS, as discussed previously (Evelyn Brouwer 2007:49)[44].

71. Yet biometrics have been progressively introduced for EU citizens after 9/11, in the name of tighter security, and under the pressure of the United States government[45]. With the June

[43] For a full list of the Working Party's opinions, see http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#pnr, visited 2/2/2010

[44] Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by these authorities, COM (2005) 600 final, 24.11.2005

[45] Particularly with the adoption of the US-VISIT programme under the remit of the newly established Department of Homeland Security (DHS) – see Amoore, 2006.

2003 EU council in Thessaloniki and the 2004 EU Council Regulation, biometric identifiers were introduced for all EU citizens[46] US pressure was part of the reasons for the adoption of the biometrics passports which were required to continue the visa waiver program after 26 October 2006 (Evelyn Brouwer 2007:50). Another explanatory factor comes from the burgeoning security industry, which in a sense defined the technical possibilities (Lock and Schreiber 2007). The spinoff effect of these measures was the justification for the introduction of biometric identifiers in national identity documents, since they can be used as travel documents. This was the argument behind the planned introduction of biometric identity cards such as the INES project in France (Piazza 2006) or the current debate for its implementation in the UK on the basis of EU regulation 2252/2004, and the US Visit program (Crettiez and Piazza 2006:219,220).

72. Although the INES project and the introduction of biometric IDs in the UK have sparked a large wave of protests ('Non à INES' campaign[47] , 'No to ID' campaign[48]) an increasing number of voluntary biometric programs are appearing. Although some of these programs require the customer to be a EU citizen, for some suffice is to have a work permit or permanent resident permit to enrol. In the case of PRIVIUM in Schiphol (Amsterdam), IRIS UK airports, ABG Pilot (Frankfurt/Main) or PEGASE (Paris), what is at stake is to mark the distinction between 'trusted' and 'distrusted' travellers[49]. Through this system, 'trusted' travellers have more facility to cross the border, travel at a quicker and smoother pace, while others, who have not been previously pre-screened and pre-identified face longer queues and tougher controls.

73. In this configuration, freedom is equated with comfort. One is believed to enjoy more freedom because she or he is less subjected to bodily checks, blocks and controls, to the point that the enrolment in biometric programs can be seen as a desirable choice. In the meantime, however, the level of control is not reduced. It is simply dematerialized and rendered more agreeable. But the 'data double', that is generated through biometric information, stored in interconnected databases travels without the physical person always being aware of it. It is shared, checked against other databases, black lists and records of individuals deemed dangerous. Then two main issues are raised, independently of whether one is an EU citizen or a TCN: first how securely is this data protected? Can we be sure that the data collected in the EU is as safely protected abroad?[50] And second, is there a way to control how is the data processed, and what are the possibilities of false positives (mistaken matches between a name and a list of unwanted/dangerous individuals)?

[46] OJ L 385, 29.12.2004 in (Evelyn Brouwer 2007:51).

[47] http://www.ines.sgdg.org

[48] http://www.no2id.net

[49] Cf. FRONTEX (2007:25)

[50] See for instance the recent rejection by the European Parliament of the EU-US SWIFT agreement, which undeniably has to do with MEPs' eagerness to assert their newly enhanced competencies under the Lisbon treaty, but was also clearly linked to the lack of satisfying guarantees regarding the rights of European citizens to privacy and data-protection in US law.

## Conclusion - Analysing the impact of security technologies on movers: European borders and freedom.

74. As can be concluded from the examples analysed so far, because security has been associated with stops, blocks and checks, the opposite, enhanced mobility is currently being framed as "freedom". This is however distinct from the traditional definition of freedom as being "free from control" in a society where privacy is respected. As it has been shown, security is not only about stopping. Opening borders, facilitating mobility can also be a move towards increased security (Bigo, forthcoming 2010:1).

75. In fact, the larger trend in liberal regimes of the West has progressively allowed for the development of practices organizing security which privilege Jean-Baptiste Say's "laissez faire, laissez passer" doctrine of liberalism, limit as much as possible the flows of people and goods (Bigo, forthcoming 2010:3). In this regard, the years post-September 2001, which marked a return to exceptional measures, enhanced border controls, discriminatory measures towards minorities have only been a parenthetical return to closed frontiers as the horizon of security. The return to a conception of borders as promoting mobility has been achieved with the promotion of the "smart borders" idea.

76. Along with Sergio Carrera, Anastasia Tsoukala and others, Didier Bigo has analyzed the struggle within the field of professionals of (in)security between the "classics" and the "neo moderns" (Bigo, Carrera et al. 2007; Bigo and Tsoukala 2008).

> If the "Classics" (border guards, immigration officers, border polices, customs, traditional military people) considered that the border of the territory was a line of defence, and may be sealed if necessary for reason of survival, the "neo Moderns" (antiterrorists squads, intelligence services, antidrug services, counter subversive operators, data base analysts) have attacked this idea on both the capacity to be efficient and even on the legitimacy of such a reaction. They have insisted on the danger for the government of sealing the borders and have proposed "smart borders" insisting in the fact that the uneasiness of all passengers was obliging to adapt the model before too much contestation, and to try to transform it into a "smart" model regulating flow of population and not territories. They have partly convinced the neo-conservative in the US and certainly the EU members of the alliance, as well as the democrats in the US.

77. The logic behind the implementation of "smart borders", is to perform and individualization by authentification of the body - in order to detect potential terrorists - but also to mass control travel documents, checking large number of individual data against databases. What is behind the logic of voluntary biometric programs and other voluntary pre-check programs is to carry out the control before the traveling occurs: "The watch lists were simultaneously a way to exclude some persons, but also to normalise 90% of the population in order to speed up the process."(Bigo, forthcoming 2010:X)

78. Independently of the citizenship of the traveller, forms of "policing at a distance" have therefore emerged as alternatives to tough border controls (Bigo and Guild 2005). As explained by the authors of the report on the surveillance society, "the everyday experience of surveillance at the border, then, is preceded by a dataveillant system that makes judgements about degrees of risk before the physical border checkpoint" (Surveillance Studies Network, Wood et al. September 2006)

79. The implications of these changes do not only concern legal practices or policing practices. Architectural forms are put at the service of this new vision of the policing at a distance of mobility, as airports move towards the creation of alternative tracks for "trusted" (fast track

channel, specific biometrics cards for specific airports, credit card privileges) and "distrusted" travellers. This is complemented by a progressive move away from controls which involve a bodily contact: fingerprint identifiers are progressively discarded as a technology of control, face recognition patterns, especially if they can be operated at a distance and without the knowledge of the person controlled (through a crowd for example) are seen as the future for comfortable and smooth travel (Coaffee, Wood et al, 2009). RFID technology is in this regard the paradigmatic tool of touch-less control, as plans are developed to track visa overstayers at a distance.

80. What is at stake however, is that "smart" techniques do not obliterate the arbitrariness of the control, and regardless of citizenship, continues to operate and channel the distinction between the suspicious and the trusted. The "advantage", in the broader political economy of movement is that the "trusted" travellers will have the impression of a lighter form of control, without the need to stop nor to wait. The "distrusted" and the "unwanted", on the other hand, categorized as potentially dangerous (be it because of the suspicion of terrorism, organized crime or maybe simply because they are suspected of potentially overstaying there visa) will be traced, and possibly face pre-emptive detention, "randomized" supplementary checks and other measures on the basis of a risk profile and through actuarial statistics. In sum: the surveillance operates on all, but will become control only for a few, leaving the majority with a sense of increased comfort - although under surveillance - in their travels.

81. There are however dangers at reducing fundamental rights and freedom to comfort. First, one is never sure of the "life" of one's data double. As several examples of wrong association between first name, name or nickname have shown (e.g. the case of Maher Arar, a Canadian citizen wrongly believed to be a terrorist, and send to Syria, where he was tortured – for an analysis, see Karazivan & Crépeau, 2010) the problem of false positives (wrong matches between a person's data and a database of researched individuals) might suddenly bring a traveller of course, from the fast track to detention and deprivation of fundamental rights. And here, citizenship is hardly a criterion that differentiates between trusted and distrusted. As Bigo puts it

> Examples are multiplying everyday because now it is not only you who have to be put under surveillance, it is also the frequentations of your data double. And certainly you have no control about it. Your data double encounters with other data doubles you never met, but it then drives your life and decides about who is suspect or not, who can travel or not.
>
> (Bigo, forthcoming 2010)

82. What is at stake is in fact a statistical logic, "where experts pretend they have the knowledge for filtering and sorting out preventively the potential terrorists, or criminal, or hooligan, or irregular migrant, from the genuine masses of tourists" (Bigo, forthcoming 2010).

83. Therefore, and this is the second point, because surveillance and control are less and less material it does not mean that it needs to go unchecked. The evolution of biometric technologies, the development of databases is indeed not always matched by the setting up of necessary checks and balances - as seen in the case of PNR.

## REFERENCES

### *Official Documents*

*1. Documents of EU bodies and institutions*


Art.29 Data Protection Working Party (2005), *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas*, Brussels, 1022/05/EN, WP110, 23 June.

Council of the European Union (2005a), *SIS Database Statistics*, Brussels, 8621/05, 2 June.

Council of the European Union (2005b), *Common Consular Instructions on visas for the diplomatic missions and consular posts (2005/C 326/01)*, Brussels, OJEU, C326, 22 December, 1-149.

Council of the European Union (2006a), *SIS Database Statistics*, Brussels, 5239/06, 12 January.

Council of the European Union (2006b), *Feasibility Study – SIS one4all – Schengen Information System*, Brussels, 13540/06, 12 October.

Council of the European Union (2007), *SIS Database Statistics*, Brussels, 6178/07, 13 February.

Council of the European Union (2008), *SIS Database Statistics*, Brussels, 5441/08, 30 January.

Council of the European Union (2009a), *SIS Database Statistics*, Brussels, 5764/09, 28 January.

Council of the European Union (2009b), *The Stockholm Programme – An open and secure Europe serving the citizen*, Brussels, 17024/09, 1 December.

Council of the European Union & European Commission (1998), *Action Plan of the Council and the European Commission on how to best implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice – text adopted by the Justice and Home Affairs Council of 3 December 1998*, Brussels, OJEU C 019, 1-15.

EDPS (2009), *Opinion on the Amended Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes*, Brussels, 7 October.

Eurodac Supervision Coordination Group (2007). *Report of the first coordinated inspection*. Brussels, 17 July.

Eurodac Supervision Coordination Group (2009). *Second coordinated inspection report*. Brussels, 24 June.

European Commission (2003), *Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas and Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals*, Brussels, COM(2003) 558 final, 24 September.

European Commission (2004), *First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, Brussels, SEC(2004) 557, 5 May 2004.

European Commission (2005a), *Second annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, Brussels, SEC(2005) 839, 20 June.

European Commission (2005b), *Communication on improved effectiveness, enhanced interoperability and synergies among European database in the area of Justice and Home Affairs*, Brussels, COM(2005) 597 final, 24 November.

European Commission (2006a), *Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visas*, Brussels, COM(2006) 269 final, 31 May.

European Commission (2006b), *Third annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, Brussels, SEC(2006) 1170, 15 September.

European Commission (2007a). *Report on the evaluation of the Dublin system*. Brussels, COM(2007) 299 final, 6 June.

European Commission (2007b). *Commission staff working document accompanying the Report on the evaluation of the Dublin system*. Brussels, SEC(2007) 742, 6 June.

European Commission (2007c), *Proposal for a Council Framework Decision on the use of Passenger Name Records (PNR) for law enforcement purposes*, Brussels, COM(2007) 654 final, 6 November.

European Commission (2008a), *Preparing the next steps in border management in the European Union*, Brussels, COM(2008) 69 final, 13 February.

European Commission (2008b), *Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person] (Recast version)*, Brussels, COM(2008) 825 final, 3 December.

European Commission (2008c), *Conformity Studies of Member States' national implementation measures transposing Community instruments in the area of citizenship of the Union – Horizontal Synthesis Report*, Brussels: European Commission, 8 December.

European Commission (2009a), *Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person] (Recast version)*, Brussels, COM(2009) 342 final, 10 September.

European Commission (2009b), *Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes*, Brussels, COM(2009) 344 final, 10 September.

European Commission (2010), *Draft Commission Decision of […] establishing the Handbook for the processing of visa applications and the modification of issued visas*, Brussels, C(2010).

FRONTEX (2007), BIOPASS, Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports., Warsaw, Poland.

Spanish Presidency (2010). *Draft Internal Security Strategy for the European Union: 'Towards a European Security Model'*. Toledo, Informal EU JHA Ministers Meeting, 21 January 2010.

*2. Legislation*

Council Decision of 20 May 1999 concerning the definition of the Schengen acquis for the determining in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis (1999/435/EC), *OJEU*, L176, 1-16.

Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC), *OJEU*, L213, 5-7.

Council Decision of 1 June 2006 amending Annex 12 to the Common Consular Instructions and Annex 14a to the Common Manual on the fees to be charged corresponding to the administrative costs of processing visa applications (2006/440/EC), *OJEU*, L175, 77-80.

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *OJEU*, L205, 63-84.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping-up of cross-border cooperation in combating terrorism and organised crime, *OJEU*, L210, 1-11.

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, *OJEU*, L261, 24-27.

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, *OJEU*, L316, 1-12.

Council Regulation (EC) No 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement, *OJEU*, L81, 1-7.

- Council Regulation (EC) No 2414/2001, *OJEU*, L327.
- Council Regulation (EC) No 453/2003, *OJEU*, L69.
- Council Regulation (EC) No 851/2005 of 2 June 2005
- Council Regulation (EC) No 1932/2006 of 21 December 2006
- Council Regulation (EC) No 1244/2009

Council Regulation (EC) No 693/2003 of 14 April 2003 establishing a specific Facilitated Transit Document (FTD), a Facilitated Rail Transit Document (FRTD) and amending the Common Consular Instructions and the Common Manual, *OJEU*, L099, 8-14.

Council Regulation (EC) No 694/2003 of 14 April 2003 on uniform formats for Facilitated Transit Documents (FTD) and Facilitated Rail Transit Documents (FRTD) provided for in Regulation (EC) No 693/2003, *OJEU*, L099

Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by the Member States, *OJEU*, L385, 1-6.

Council Regulation (EC) No 380/2008 of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, *OJEU*, L115, 1-7.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJEC*, L281, 31-50.

Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within

the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, *OJEU*, L158, 77-123.

Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Border Code), *OJEU*, L105, 1-32.

Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention, *OJEU*, L405, 1-22.

Regulation (EC) 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), *OJEU*, L381, 4-23.

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), *OJEU*, L218, 60-81.

Regulation (EC) No 390/2009 of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, *OJEU*, L131, 1-10.

Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), *OJEU*, L243, 1-58.

*3. Others*

Department of Homeland Security (2006), *Privacy impact assessment for the Automated Targeting System*, Washington, retrieved from: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf (accessed March 2010).

House of Lords (2007), *9th report of session 2006-2007: Schengen Information System II*, London: The Stationery Office Limited.

Meijers Committee (2009), *Note on the amended proposal for the Eurodac Regulation (COM(2009)342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM(2009) 344 final)*, Utrecht, 10 September.

***Literature***

Amoore, L. (2006), Biometric borders: governing bodies in the war on terror, *Political Geography*, 25, 336-51.

Anderson, M., den Boer, M., Cullen, P., Gilmore, W. C., Raab, C. D., Walker, N. (1995), *Policing the European Union: Theory, Law, and Practice*, Oxford: Clarendon Press.

Balibar, E. (2001), *Nous, citoyens d'Europe? Les frontières, l'Etat, le peuple*, Paris : La Découverte.

Balzacq, T., Bigo, D., Carrera, S., Guild, E., *Security and the Two-Level Game: the Treaty of Prüm, the EU and the Management of Threats*, CEPS Working Documents, 234.

Beaudu, G. (2007), L'externalisation dans le domaine des visas Schengen, *Cultures & Conflits*, 68, 85-109.

Beaudu, G. (2009), L'externalisation dans le domaine des visas Schengen (actualisation 1er mai 2009), *Cultures & Conflits*, 74, 85-109.

Bellanova, R. (2008), The "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange? In F. Geyer & E. Guild (eds), *Security vs. Justice? Police and Judicial Cooperation in the European Union*, London: Ashgate, 203-21.

Benhabib, Seyla (2006), Another cosmopolitanism, New York, Oxford University Press.

Bigo, D., ed. (1992), *L'Europe des polices et de la sécurité intérieure*, Bruxelles: Editions Complexe.

Bigo, D. (1996), *Polices en réseaux: l'expérience européenne*, Paris: Presses de Sciences Po.

Bigo, D. (2006). Protection: security, territory and population. In J. Huysmans, A. Dobson and R. Prokhovnik (eds), *The Politics of Protection: sites of insecurity and political agency*, London: Routledge, 84-100.

Bigo, D. (forthcoming 2010), Freedom and speed in enlarged Borderzones, In Squire,V. (ed.), *The contested politics of mobility: borderzones and irregularities*, London: Routledge, manuscript version.

Bigo, D., Guild, E. (2003), La logique du visa Schengen: la mise à l'écart des étrangers, *Cultures & Conflits*, 49, 1-137.

Brouwer, E. (2002), Eurodac: Its Limits and Temptations, *European Journal of Migration and Law*, 4, 231-47.

Brouwer, E. (2007), The use of Biometrics in EU databases and Identity documents, In J. Lodge (ed.), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen, Wolf Legal Publishers, 45-66.

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

Brouwer, E., Guild, E. (2006), *The Political Life of Data. The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Briefs, 109.

Bunyan, T. (1993), 'Trevi, Europol and the European State', in Tony Bunyan (ed), *Statewatching the New Europe: a handbook on the European state*, London: Statewatch, 15-36.

Côté-Boucher, K. (2008), The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada's Smart Border, Surveillance & Society, 5(2), 142-65.

Crettiez, X., Piazza P. eds (2006), *Du papier à la biométrie : identifier les individus*, Paris, Presses de Sciences Po.

Delanty, G. (1997), Models of Citizenship: Defining European Identity and Citizenship, *Citizenship Studies*, 1(3), 285-303.

Faure Atger, A. (2008), The abolition of internal border checks in an enlarged Schengen area: freedom of movement or a web of scattered security checks, *CHALLENGE Research Papers*, 8.

Guild, E. (2005), The Legal Framework: Who is Entitled to Move? In D. Bigo and E. Guild (eds), *Controlling Frontiers: Free Movement into and within Europe*, London: Ashgate, 14-48.

Guittet, E-P (2004), Identity through Security in Europe: : "Because we are all democracies", A closer look at the Aznar Protocol, Paper presented at the annual meeting of the International Studies Association, Montreal, 17 March.

Hailbronner, K., Papakonstantinou, V., Kau, M. (2008), The Agreement on Passenger-Data Transfer (PNR) and the EU-US Cooperation in Data Communication, *International Migration*, 46(2). pp. 187-197.

Hindess, B. (2000), Citizenship in the international management of populations, *American Behavioural Scientist*, 43(9), 1486-97.

Hindess, B. (2002), Neo-liberal Citizenship, *Citizenship Studies*, 6(2), 127-43.

Hobbing, P. (2008), *Tracing terrorists: the EU-Canada agreement in PNR matters*, Brussels: CEPS.

Hobbing, P., Kosloswky, R. (2009), *The tools called to support the 'delivery' of freedom, security and justice: a comparison of border systems in the EU and in the US*, Ad hoc briefing note for the European Parliament, PE 410.681.

Huysmans, J. (2000), The European Union and the Securitization of Migration, *Journal of Common Market Studies*, 38(5): 751-77.

Isin, E. F. (2002), *Being political : genealogies of citizenship*, Minneapolis, University of Minnesota Press.

Isin, E. F., Nielsen, G.M. (2008), *Acts of citizenship*, London ; New York, Zed Books.

Jileva, E. (2003), La mise en oeuvre de Schengen: la délivrance des visas en Bulgarie, *Cultures & Conflits*, 50, 31-48.

Kaluszynski, M. (1987), Alphonse Bertillon et l'anthropométrie, In Société d'histoire de la révolution de 1848 et des révolutions du XIXe sicècle (ed.), *Maintien de l'ordre et polices en France et en Europe au XIXe siècle*, Paris : Créaphis, 269-85.

Karazivan, N., Crépeau, F. (2010), Le rôle des tribunaux dans l'affirmation de la primauté du droit en temps d'insécurité: l'affaire Arar, In Scherrer, A., Guittet, E.P., Bigo, D. (ed.), *Mobilités sous surveillance : perspectives croisées UE-Canada*, Montréal: Athéna, 27-42.

Kosta, Eleni, Fanny Coudert, and Jos Dumortier (2007), Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive, *International Review of Law, Computers & Technology*, 21(3). pp. 347-362.

Lock, P., Schreiber, W. (2007), The economic dynamics of biometric control technologies, Working Paper, Challenge FP6 Programme, WP4.

Maas, W. (2008), Migrants, states and EU citizenship's unfulfilled promise, *Citizenship Studies*, 12(6), 583-96.

Marshall, T. H. (1950), *Citizenship and social class, and other essays*, Cambridge: Cambridge University Press.

Meehan, E. (1993), *Citizenship and the European Community*, London: SAGE.

Merlino, Massimo (2009), The Italian (In)security package: security vs. rule of law and fundamental rights in the EU, *CHALLENGE Research Papers*, 14.

Monar, J. (2001), The Dynamics of Justice and Home Affairs: Laboratories, Driving Factors and Costs, *Journal of Common Market Studies*, 39(4): 747-64.

Murakami Wood, D. ed. (2006), *A report on the surveillance society*, London: Surveillance Studies Network.

Piazza, P. (2004), *Histoire de la carte nationale d'identité*, Paris: Odile Jacob.

Piazza, P. (2006), Les résistances au projet INES, *Cultures & Conflits*, 64, 65-75.

Saas, C. (2003), Les refus de délivrance de visas fondés sur une inscription au Système d'Information Schengen, *Cultures & Conflits*, 49, 63-83.

Scherrer, A., Guittet, E.P., Bigo, D. (2010), Introduction, In Scherrer, A., Guittet, E.P., Bigo, D. (ed.), *Mobilités sous surveillance : perspectives croisées UE-Canada*, Montréal: Athéna, 7-24.

Schnapper, D. (2002), Citizenship and national identity in Europe, *Nations and Nationalism*, 8(1), 1-14.

Soysal, Y. N. (1994), *Limits of citizenship : migrants and postnational membership in Europe*, Chicago: University of Chicago Press.

Spire, A. (2008), *Accueillir ou reconduire: enquête sur les guichets de l'immgration*, Paris: Raison d'Agir.

Tilly, C. (1997), A Primer on Citizenship, *Theory and Society*, 26(4), 599-602.

Torpey, J. (1998), Coming and Going: On the State Monopolization of the Legitimate "Means of Movement", *Sociological Theory*, 16(3), 239-59.

Torpey, J. (2000), *The invention of the passport : surveillance, citizenship and the state*, Cambridge : Cambridge University Press.

Van der Mei, A.P. (2003), *Free Movement of Persons within the European Community: Cross Border Access to Public Benefits*, Portland: Hart Publishing.

Weiner, A. (1997), Making Sense of the New Geography of Citizenship: Fragmented Citizenship in the European Union, *Theory and Society*, 26(4), 529-60.

Zolberg, A. (2000), The Dawn of Cosmopolitan Denizenship, *Indiana Journal of Global Legal Studies*, 7(5), 511-18.