Technische Universität Berlin

Zentrum Technik und Gesellschaft

Discussion paper Nr. 29/09

March 2009

Leon Hempel, Michael Carius & Carla Ilten

Exchange of information and data between law enforcement agencies within the European Union

ZTG Themenschwerpunkt:

Genese und Gestaltung von Innovativität

Nr. 29/09 Leon Hempel, Michael Carius & Carla Ilten
Exchange of information and data between law enforcement agencies within the European Union

Zentrum Technik und Gesellschaft
Sekretariat: ER 2-2
Hardenbergstraße 36a
10623 Berlin

Tel: (030) 314-23 665
Fax: (030) 314-26 917

www.ztg.tu-berlin.de

Zusammenfassung

In den letzten anderthalb Jahrzehnten hat sich der transnationale Informationsaustausch zwischen Strafverfolgungsbehörden innerhalb der Europäischen Union beträchtlich intensiviert. Ausgelöst wurde diese Ent–wicklung durch die Abschaffung der routinemäßigen Kontrollen an den Staatsgrenzen im Schengen–Raum, deren Fehlen zu kompensieren war. Die Entwicklung treiben die Identifizierung einer immer weiter wachsenden Zahl von Sicherheitsbedrohungen, ein naiver Glaube an das Problemlösungs–vermögen der Technik sowie eine Politik der Überbietung zwischen einigen Mitgliedsstaaten der EU und Brüssel. Die Entwicklung zielt auf die Errichtung einer pan–europäischen Ordnung innerer Sicherheit.

Das vorliegende Papier, verfaßt im Auftrag des Ausschusses *Bürgerliche Freiheiten, Justiz und Inneres* (LIBE) des Europäischen Parlaments und veröffentlicht als Studie PE 419.590 (April 2009), untersucht die einschlägige Gesetzgebung zum transnationalen Informationsaustausch und die sie organisierenden Prinzipien. Das Papier gibt einen Überblick über arbeitende und geplante Datenbanken und Systeme des Informationsaus–tausches innerhalb der EU, klärt einige zentrale Begriffe des elektronischen Informationsaustausches, beschreibt einige der Verfahren des transnatio–nalen Informationsaustausches zwischen europäischen Strafverfolgungs–behörden und nennt einige seiner unerwünschten Nebenwirkungen. Ab–schließend werden einige Vorschläge skizziert, wie Apparate und Praktiken zu verbessern sind.

Abstract

Over the last one and a half decades, transnational information exchange between law enforcement authorities within the European Union has been stepped up considerably. This process was originally triggered by the abolition of national borders within the Schengen Area. In the meantime, the process is fed by an ever–growing number of perceived security threats, a misled belief in the problem–solving capacity of technology and a policy of overbidding between some Member States and the EU level. The goal of this process is to establish a pan–European regime of internal security.

The present paper, requested by the European Parliament's *Committee on Civil Liberties, Justice and Home Affairs* (LIBE) and published as Study PE 419.590 (April 2009), discusses the legislative aspect of this process and considers its organising principle(s). The paper provides a review of operational and planned databases and systems of information exchange within the EU. It clarifies some of the central concepts in the field of automated information exchange. It describes some of the procedures of information exchange between law enforcement authorities. It identifies some of the side effects of transnational information exchange. Finally, it makes some recommendations how to better manage apparatuses and practises.

Table of contents

1. Introduction

In June 2008, the White Paper *Défense et Sécurité nationale* drawn up under the authority of the French President Nicolas Sarkozy was published. It is a striking example for a technocratic utopia of an all–embracing national security regime in which collection, processing, centralisation and/or exchange of data and information play the key role in anticipating palpable risks in a frightening fog of looming threats. In this utopia *anticipative knowledge* is the first line of defence, the warrantor of security:

> Le développement de la connaissance et des capacités d'anticipation est notre première ligne de défense. […] La bataille du XXIe siècle se jouera d'abord sur le terrain de la connaissance et de l'information, des hommes comme des sociétés. […] Les responsables politiques doivent pouvoir disposer de l'ensemble des données qui permettront d'éclairer leurs décisions et d'apprécier les situations en toute souveraineté. [It must be ensured that] les pouvoirs publiques font le maximum pour éclairer l'avenir, analyser les risques, tenter de les éviter, et préparer les moyens d'y faire face.
>
> (*Défense et Sécurité nationale: Le livre blanc* 2008, p. 66)

In order to ensure anticipative power and to develop knowledge for security, law enforcement authorities in Europe are increasingly obliged by policy makers to make use of information technologies for collecting, linking and exchanging data for their purposes. Two main requirements are seen as necessary in this respect: data have to be available, and therefore systems must become interoperable. However, interoperability is not a mere technological problem as the designing engineers of the 21st century security architecture wish it to be. De Hert and Gutwirth argue:

> Indeed, technological developments are not inevitable or neutral, which is *mutatis mutandis* also the case for technical interoperability. Technologies are interwoven with organization, cultural values, institutions, legal regulation, social imagination, decisions and controversies, and, of course, also the other way round. This means that technologies cannot be considered as *faits accomplis* or extrapolitical matters of fact. (De Hert and Gutwirth 2006, p. 3)

Systems are hybrids, combining human and technological agency characterised by multifaceted interactions. On a small scale, these take place in systems such as biometrics, and on a large scale in electronic data processing systems. Instead of the usual delegation from humans to machines, interactions occur between human and technological partners in one and the same multilateral coordination context. These interactions become even more complicated at the transnational level of the EU: the cultural, social, organisational and legal differences between the data exchanging law enforce-

ment authorities increase to a maximum of complexity. The principal problem is twofold: On the one hand, it lies in the fact that the movement of goods, persons, services and capital within the EU is to a large extent unrestricted. This extensive freedom of transnational movement produces a bundle of adverse effects. It makes life easy for crime, but most difficult for law enforcement. On the other hand, we are witnessing an increasing opacity because of an ever–growing patchwork of emerging security agencies, systems, procedures and technologies as well as regulations. We all are facing an enormous black boxed security regime.

At the policy level the problem is hardly perceived. Like engineers, policy makers also judge the problem to be a mere technological issue. Their technology is legislation. They do not take into regard the social implications of an extensive transnational cooperation via large–scale IT systems. This unawareness is the expression of ideological assumptions which underlie the European Security Regime currently under construction. Sarkozy's *livre blanc* is intensely and jealously debated among security policy makers of the Member States of the EU, and the question is: who will overbid and translate Sarkozy's utopia to the European level? Indeed, European security policy is in search of the right method of *converging* technologies, systems, practices, organisations and laws which is, of course, much easier at the national level. The strategy, however, will remain the same because the guiding political culture is the same. It will follow inevitably a further development of technology, confusing means and ends in the process. This precisely is the case when Franco Frattini announces for the post–Hague Programme:

> The overarching future challenge is the *further development of new technologies and their link to financing at EU level*, including in the area of security research and structural funds. Databases and new technologies will play a central role in further developing JLS JHA policies in the areas of border management, migration, fight against organised crime and global terrorism. (Cit. by Bunyan 2008, p. 7)

When we look at the big picture, we see a strong tendency towards an integration of technological systems in order to enable what has been termed *interoperability*. Justified by a rhetoric of new threat, data collection, availability and exchange as well as the extension of entire security systems to the EU level on a — supposedly neutral — technological basis are propelled. Neither the different contexts of the hitherto distinct information systems nor aspects of legitimacy of these binding agreements are included in the debate. Visions and decisions — such as the Treaty of Prüm — have so far been negotiated and adopted in a very non–transparent way and without democratic control. Technological systems have politics, though: both the purposes and the architecture of the future security systems need to be evaluated broadly and determined very precisely if they are to work at all,

and in order to stay within the boundaries of legitimate operations. This political and constructive process, of course, takes time for research and decision taking. This paper gives an overview of the top priority issues and problems to be handled.

2. Towards an EU strategy on data sharing?

Today, the entire territory of the EU, with the exception of the UK and Ireland, is (or will soon be) part of an area which comprises (or will comprise) also the non–EU States Iceland, Norway, Switzerland, and Liechtenstein — the *Schengen Area*. It covers a population of over 450 million people, and a territory of about four and a half million square kilometres. Within this vast area all systematic border controls have been abolished. This has changed dramatically the conditions under which European law enforcement authorities have to fulfil their duties. In its 2008 strategy paper, the Association of European Police Colleges (AEPC) declares: 'International police co–operation must encompass the whole of Europe as one "criminal–geographic space"' (AEPC, 2008). The European law enforcement authorities are facing a truly Herculean task. There are indications that this task possibly overstrains them.

A range of documents with a specific view on serious crime and terrorism may give first insights into the problem. The Replies to questionnaire on Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU (5815/1/05 REV 1), a Framework Decision known as the *Swedish Initiative*, illustrate the difficulties for the exchange of data which lie in the different legal provisions authorizing police agencies to exchange personal data across national borders. The replies clearly show that there is no common regulation of data access among law enforcement authorities, and the question which remains open until today is not only whether such a common access standard can be achieved and how, but also whether standard harmonisation is really desired by law enforcement authorities. Anyway, in an interview with representatives of a counter–terrorism unit taken in the course of the preparation of this paper, we were told that such a harmonisation will take generations.

The European Union Counter–Terrorism Strategy (14469/4/05 REV 4) of 30 November 2005, grouping the measures to be taken under the headings PREVENT, PROTECT, PURSUE and RESPOND, is strongly based on sufficient flow of information between Member States as well as between Europol and the Member States. In a Note on the Implementation of the Strategy and Action Plan to Combat Terrorism (15411/07) of 23 November 2007, which assesses the progresses and further priorities to take, the EU Counter–Terrorism Coordinator (CTC) addresses the difficulties of information sharing. The CTC states: 'This round of mutual evaluation has highlighted, however, that considerable deficiencies remain in sharing information at national level. Despite a general trend among the Member States in favour of a "multi–agency" approach, those deficiencies constitute one of the main obstacles to cooperation at European level. They relate chiefly to the lack of platforms bringing together the different agencies (police, customs, FIU,

etc.) and to insufficient links between the agencies' databases.' That can be seen, by the way, as an interesting anticipation of the things to come in the post–Hague Programme. Thus, next to *legal* disharmonies, in this case *technical* obstacles are addressed. Security policy making at EU level has so far been concentrated on these two dimensions, the technical and the legal.

A year later, the CTC again has to report that data exchange remains behind expectations. In his Note of 19 November 2008 (15983/08), embedded in the outline of an EU strategy on data sharing, he indicates that, according to a report by Europol, 'the implementation of Decision 2005/671/JHA remains unsatisfactory'. Referring to Council Decision 2003/48/JHA (OJ 2003 L 16) on the implementation of specific measures for police and judicial cooperation to combat terrorism, which has been one of the central responses to the terrorist attacks of 9/11, Decision 2005/671/JHA (OJ 2005 L 253) had called for the extension of information exchange after the London bombings: 'The scope of information exchanges must be extended to all stages of criminal proceedings, including convictions, and to all persons, groups or entities investigated, prosecuted or convicted for terrorist offences' (preamble, para. 4). Again, the CTC demands to take action, 'if necessary by amending Decision 2005/671/JHA' which plays a crucial role in his strategy outline for upgrading information sharing. He identifies the following priorities:

- establishment of a mechanism for the management of large–scale IT systems;
- systematic transmission of information to Europol and Eurojust according to Decision 2005/671/JHA (amended or not) as well as integration of Europol and Eurojust into joint investigation teams on terrorism by the Member States;
- intensification of the cooperation between Europol and Eurojust and its assessment;
- invitation to all Member States to carry out analyses of extremist Islamic sites in order to add information to the portal *Check the Web*;
- establishment of central bodies at national level responsible for coordinating the exchange and analysis of information on terrorism;
- further discussions in preparing the negotiation of a binding agreement on data protection in the course of information exchange with the United States.

These suggestions touch upon four dimensions: *technological harmonisation* (IT-support for data exchange and management of large–scale systems); *legal harmonisation* (i.e., at least in this case, ensuring the application of legislation in force); *cultural approximation* of police work (i.e., trust building aiming at furthering the readiness to share information); and finally *organisational centralisation* of counter–terrorism at national level aiming at facilitating information exchange at transnational level (reduced number of actors; clearly identified communication partners). While in 2007, the CTC had mainly identified technological problems as obstacles to a smooth

transnational information exchange, the Europol report on the difficulties as regards the application of the provisions of Decision 2005/671/JHA motivated him to take 'a broader and coherent way'. Of course, the main interest of the CTC still is establishing a central coordinating counter–terrorism agency at EU level, but now he develops a multidimensional approach. The question, however, remains whether this approach is sufficient to overcome the difficulties. It seems that his new multidimensional approach to improving transnational information exchange reflects the precarious status of Europol and Eurojust in matters of combating terrorism and thus the weakness of his own position. But this is only half the story. The reluctance of some Member States to transmit their data to Europol and Eurojust is, at the same time, an at least symbolic answer to the overall EU strategy of integrating national security policies at EU level, thereby consuming essential parts of national sovereignty. According to the CTC's Note, the Europol report stressed 'three types of obstacles to a systematic transmission of information relating to investigations:

- the refusal by the judicial authorities in certain Member States to transmit information relating to investigations in progress;
- Some agencies with dual competencies as Law Enforcement and as Security Services are experiencing legal difficulties in identifying what can be shared with Europol.
- the requirement laid down in Article 2(3) of the Decision, that the information affects, or is likely to affect two or more Member States'.

Art. 2(3) of Decision 2005/671/JHA reads: 'Each Member State shall take the necessary measures to ensure that […] information […] concerning criminal investigations and the information […] concerning prosecutions and convictions for terrorist offences which affect or may affect two or more Member States, gathered by the relevant authority is transmitted to […] Europol […] and […] Eurojust.'

All three obstacles the CTC mentions stem from the phenomenon of what has been called 'information property' (Bigo et al. 2007), that is: they have their common origin in the experience that knowledge is power. More precisely: the power of knowledge referred to in the present context is the ability to maintain law and order at national level. This power, this ability is the characteristic of sovereignty. So the obligations expressed in Decision 2005/671/JHA lead to classic loyalty conflicts: The agent/police officer obliged to transfer information to Europol, for instance, may have the feeling to act against his genuine mission, namely, to protect (national) State security; and the third obstacle to information transmission to a transnational body is obviously loyalty among two or more Nation States. To sum up: What is intended to serve as a security measure — sharing of information — may be perceived as an attempt of expropriation and insofar as its very opposite: a competence threat and the surveillance of national task fulfilment. Even before the implementation of converging technological and

legal systems, the idea of data and information sharing is a highly political issue in itself.

3. Review of existing and planned databases and systems of information exchange

The idea of technology as being a potent, but neutral problem solver is accompanied by the neglect or the downplaying of technology's apparent social and political side effects. The only way to avoid this error is placing technology back in the social and political context of its development. In this section, the main information systems at EU level will be described briefly with some remarks regarding current status and problems before we will discuss the issue of interoperability and efficiency in some concluding remarks in general.

3.1. Information Systems

Since the Treaty establishing the European Economic Community (1957), the principal objective of the European policy of economic integration has been to establish a Common Market. In 1985, the intergovernmental Schengen Agreement took a decisive step towards the establishment of a Common Market. The contracting parties were 'prompted by the resolve to achieve the abolition of checks at their common borders on the movement of nationals of the Member States of the European Communities and to facilitate the movement of goods and services at those borders' (fourth recital to the Schengen Agreement, in Schengen Acquis, OJ 2000 L 239). They were well aware of 'the adverse consequences in the field of immigration and security that may result from easing checks at the common borders' (Art. 7). They stressed 'the need to ensure the protection of the entire territory of the five States against illegal immigration and activities which could jeopardise security' (Art. 7). They declared that 'the Parties shall reinforce cooperation between their customs and police authorities […] To that end […], the Parties shall endeavour to improve the exchange of information and to reinforce that exchange where information which could be useful to the other Parties in combating crime is concerned' (Art. 9). In 1990, the Convention implementing the Schengen Agreement (Schengen Convention) was signed. In 1995, the Schengen Convention came into force, abolishing checks at the internal borders of the signatory States, and creating a single external border. Compensatory measures, such as a common visa regime, but first and foremost the Schengen Information System (SIS), were put in place. In 1999, the Schengen Acquis, and with it the SIS, was integrated into the EU framework by the Treaty of Amsterdam. The SIS is the mother of all existing and future pan–European IT systems which support the transnational information exchange between law enforcement authorities.

Schengen Information System (SIS)

The SIS database is operational since 1995. Its *legal basis* is the Convention implementing the Schengen Agreement of 14 June 1985 (OJ 2000 L 239), as last amended by Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism (OJ 2004 L 162) and Council Decision 2005/211/JHA (OJ 2005 L 68).

Purpose: It shall 'enable the authorities […] by means of an automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks' (Art. 92(1)).

The following *categories of objects* are entered into the SIS: stolen or lost motor vehicles, boats, aircraft, industrial equipment, containers, firearms, passports, identity cards, driving licenses, residence permits, travel documents etc. (Art. 100(3)).

The following *categories of persons* are entered into the SIS:

- persons wanted for arrest or extradition (Art. 95);
- aliens [third country nationals] to be refused entry [into the Schengen Area] (Art. 96);
- persons missing or to be placed under temporary police protection (Art. 97);
- witnesses etc. (Art. 98);
- persons (or vehicles) wanted for the purposes of 'discreet surveillance' or of 'specific checks' (Art. 99).

Finally, the following *information about these persons* are entered into the SIS: surname and forenames; aliases; specific objective physical characteristics not subject to change; date and place of birth; sex; nationality; whether the persons concerned are armed; whether the persons concerned are violent; reason for the alert; action to be taken (Art. 94(3)).

Architecture: The SIS (current version: SIS I+) is an interconnection of national databases (N–SIS), via a secured communication network, with a central server in Strasbourg (C–SIS) sending and receiving data to and from the national databases (radial shape). Information is supplied by each contracting State via its N–SIS and distributed subsequently via C–SIS among all other N–SIS. Therefore, the content of all N–SIS is identical, and it is identical with the content of C–SIS (parallel storage). Information search in each contracting State only takes place in the N–SIS of this State. The databases only contain the indispensable information (the so–called 'alert data') allowing the identification of a person or an object and the nec-

essary action to be taken. The SIS is supplemented by the national SIRENE Bureaux (Supplementary Information Request at the National Entry) which provide additional information not stored in the database if requested. The SIRENE Bureaux are connected through a protected telecommunication system (SISNET).

Authorised users: 'In practice a wide ranging set of national authorities have access to SIS […] police, state security services, public prosecutors and judges, custom authorities, ministerial departments, immigration offices and vehicle registration authorities' (Geyer 2008, p. 14). To these add Europol and Eurojust (since the mentioned amendments).

By June 2005, the SIS included more than 15 million records on objects and persons. More than one million of these records concerned persons (Brouwer 2005). The number, of course, is steadily growing. By February 2008, the SIS included more than 17 million records (SEC(2008) 153; see below under Publications of the Commission of the EC). Quite naturally the question arises whether all these *alerts* can be transformed into *actions*.

Issues: One of the principal problems of transnational information exchange between law enforcement authorities is the simple fact that the countries exchanging information exhibit strong cultural and legal differences between them. That is shown clearly by a report by the Joint Supervisory Authority of Schengen of 18 December 2007 (Report nr. 07–02; not available on the JSA website) on an inspection of the use of Article 99 alerts in the SIS. According to Art. 99, an alert may be issued when there is clear evidence that (a) the person concerned intends to commit or is committing numerous and extremely serious criminal offences and/or (b) when an overall assessment of the person concerned, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit extremely serious criminal offences in the future. Based on the figures of 1 October 2006, the SIS contained the following numbers of Art. 99 alerts:

Country	**Surveillance**	**Specific Checks**	**Total # alerts**
France	9,615	6,493	16,108
Italy	11,604	100	11,704
Spain	15	2,142	2,157
Netherlands	3	1,135	1,138
Germany	790	0	790
Austria	714	0	714
Sweden	394	0	394
Denmark	196	0	196

Belgium	96	80	176
Finland	58	0	58
Norway	58	0	58
Luxembourg	33	0	33
Portugal	14	0	14
Greece	1	0	1
Iceland	0	0	0
Total	23,591	9,95	33,541

Source: JSA report, p. 5. The table in this (rearranged) form is taken from Hayes 2008, p. 3.

What is the reason for the extreme variations in the number of Art. 99 alerts entered by the different Schengen States? The JSA report answers: 'The use of Art. 99 is governed by a variety of laws and is administered by a number of different authorities in the different Schengen States' (p. 6). 'The Schengen Convention does not define the term "serious criminal offence". As a result, the method for selecting criminal offences leading to Art. 99 alert varies between the States' (p. 8). And finally: 'It is clear that the differences in national interpretation of what is a serious criminal offence and national perceptions on how to investigate crimes or to use pro–active methods of investigation seems to be the most critical factor for using an Art. 99 alert' (p. 11). The JSA report makes clear beyond any doubt that the area of freedom, security and justice *cannot* be harmonised in terms of law enforcement through the establishment of communication channels as such. Transnational spread of information is necessarily spread of very different translations and interpretations of only formally general provisions. Such different translations and interpretations are dependent on a diversity of actual practices as well as strongly varying degrees of threat awareness between the different countries. It is doubtful whether legal harmonisation could alter this situation. The findings of the JSA report should be taken as a warning against including, for instance, the offence 'violent troublemaking' into the SIS.

Schengen Information System II

Purpose: The SIS database was initially put up for connecting only eight countries. It soon became obvious that this would not be enough. Already in 1996, the Schengen Executive Committee considered a second generation SIS. The planning of this SIS II gained growing attention, especially due to the rising awareness of new threats, including organised crime and, since 9/11, terrorism. SIS II is not yet operational. Actually, it seems to be in serious trouble. The Press Release of the 2927th meeting of the Council JHA in Brussels (26–27 February 2009) reads: 'Given the time required to resolve

outstanding issues, the date for migration from SIS I+ to SIS II, set for September 2009, is no longer realistic.' An 'alternative technical scenario for developing SIS II based on SIS I+ evolution as part of a contingency plan' has to be created (p. 21).

The *system architecture* of SIS II will be basically the same as in the old, still operational SIS. In preparation of SIS II, the number of *authorised users* has already been enlarged (Europol, Eurojust, national prosecutors, vehicle licensing authorities etc; a list of all national authorities having access to SIS is provided in Council doc. 6073/2/07 REV 2, 25.6.2007). The content will be widened (inter alia, fingerprints and photographs). Finally, its *technical platform* will be shared with VIS, EURODAC etc. (see the section about S–Testa below).

The *legal basis* of SIS II consists of:

- Regulation (EC) No 1987/2006 of the European Parliament and of the Council (OJ 2006 L 381) will govern the immigration aspects of SIS II ('alerts in respect of third–country nationals') — further referred to as *the Regulation*.
- Council Decision 2007/533/JHA (OJ 2007 L 205) will govern the use of SIS II for police and judicial cooperation in criminal matters ('alerts on persons and objects') — further referred to as *the Decision*.
- Regulation (EC) No 1986/2006 of the European Parliament and of the Council (OJ 2006 L 381) opens for vehicle registration authorities the access to SIS II.

Issues: On 19 October 2005, the European Data Protection Supervisor (EDPS) published an Opinion on those three Proposals which subsequently led to the just mentioned three regulations (OJ 2006 C 91). Because the latter have remained substantially unaltered in comparison to the Proposals, it is possible to discuss the factual legal basis of SIS II in the light shed by the Opinion of the EDPS on the Proposals. The EDPS observes that 'the objective of the SIS II seems much broader than the objective of the current SIS as laid down in Art. 92 of the Schengen Convention' (C 91/43), namely, to 'enable the authorities […] to have access to alerts on persons and property for the purposes of border checks and other police and customs checks'. The corresponding provision of both the Regulation and the Decision reads: 'The purpose of SIS II shall be […] to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States' (Art. 1(2)). In comparison to the Proposals, the wording has become even broader, all–encompassing. The pompous and shallow rhetoric may be read, on the one hand, as an alarming sign indicating that an ideology of security has gained a momentum of its own. Such a reading is certainly correct, but on the other hand, Art. 1(2) has to be taken simply as meaning what it seemingly

wants to say: *SIS II is to be an all–purpose tool*. This proposition expresses the rationale of the legislation under consideration. If SIS II is to be a giant information machine *producing security in every conceivable respect*, then there is no principle limitation as regards the categories of data entered into it, the categories of security authorities having access to it or the search functions executed by it. The ends determine the means and the measures as well as the actors to be involved. This trivial insight is guiding the Opinion of the EDPS. He is pleading for purpose limitation — not only in this Opinion, and he is right in doing so.

Contrary to a limitation of its purpose, SIS II is conceived as a general investigative tool. Making reference to, inter alia, asylum authorities, Europol and Eurojust, the EDPS comments: '*Access is granted to them as a source of information for their own purposes*' (C 91/45). Art. 37(1) of the Regulation and Art. 52(1) of the Decision also fit neatly into the investigative character of SIS II: 'A Member State may create a link between alerts it enters in SIS II. The effect of such a link shall be to establish a relationship between two or more alerts', i.e., first and foremost, between two or more persons. The EDPS comments: 'Since the establishment of links is left to national legislation, it has as a possible consequence that links which are illegal in one Member State can be established by another one, thus feeding "illegal" data into the system' (C 91/46). As already demonstrated in connection with the Art. 99 alerts, this problem does not arise only in *linking* alerts. It has to be reiterated that transnational information exchange on a large scale inevitably leads to an absolutely uncontrollable *factual fusion* of fundamentally different national legislations and practices of law enforcement. This is one of the main reasons for the opacity of the situation in matters of (internal) security at EU level. Another important point in this context concerns the unchanged system architecture of SIS II compared to that of SIS I: an interconnection of national databases which store in parallel (or at least, could do so) the complete set of data. The EDPS recommends 'dropping the possibility for Member States to use national copies', 'because the multiplication of copies increases the risks of abuse' (C 91/52).

EURODAC

Purpose: EURODAC is a database which registers and compares fingerprints via an automated fingerprint identification system. Its purpose is to establish the identity of applicants for asylum and of persons who unlawfully crossed the external borders of the Community. Each Member State is obliged to promptly transmit to the Central Unit the following data in relation to any alien, who is not turned back: Member State of origin, place and date of the apprehension; fingerprint data; sex; reference number used by the Member State of origin; date on which the fingerprints were taken; date on which the data were transmitted to the Central Unit. Asylum seekers are assigned to EU Member States depending on their first appearance in the

register. EURODAC processes fingerprints of the following categories of persons:

(a) applicants for asylum;

(b) aliens apprehended who unlawfully crossed the external borders; and

(c) aliens found illegally present in a Member State.

EURODAC is operational since 2003. It is the first common Automated Fingerprint Identification System (AFIS) within the EU. The *legal basis* is provided by Council Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (OJ 2000 L 316).

Architecture: EURODAC consists of a central unit which includes a database which stores the fingerprints. Requests are made in a hit/no–hit process, such that data remains stored centrally and no direct access may be possible. When hits occur, the involved Member States can act bilaterally according to the Dublin Regulation (Council Regulation (EC) No 343/2003) which defines the responsible asylum application recipient (OJ 2003 L 50).

Issues: Interesting are the main findings of the Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007 (COM(2009) 13 final (26 January 2009)). There seem to exist technical as well as problems of acceptance or trust:

- 300.018 successful transactions (transactions correctly processed by the Central Unit) in total (against 270.611 in 2006)
- 197.284 asylum seekers (against 165.958 in 2006)
- 38.173 persons who unlawfully crossed an external border (against 41.312 in 2006)
- 64.561 persons illegally residing in a Member State (against 63.341 in 2006)
- *obsolescence of the technical platform* (upgrading of the EURODAC system is planned to be finalised 2009)
- quality of transactions: *rejected transactions* for all Member States is 6.13%; 14 Member States have a rejection rate over the average (the causes of this rejection rate are mainly the low quality of the fingerprints images submitted, human error or the wrong configuration of the sending Member States' equipment)
- some Member States still produce *important delays* by sending fingerprints up to almost 12 days (Spain, Bulgaria, Greece and Denmark)
- the problem of Member States' reluctance to systematically send 'category 2' ('border–crossers') transactions still prevails. *8 Member States did not send any 'category 2' transactions* (Cyprus, the Czech Republic, Denmark, Estonia, Iceland, Latvia, Luxemburg and Portugal)

Visa Information System (VIS) in development

Purpose: Every year, 160 million EU citizens, 60 million third country nationals (TCNs) who do not require a visa, and 80 million requiring a visa, cross the EU's external border in either direction. That, of course, poses problems. It has been estimated that 'there were up to eight million illegal immigrants within the EU25 in 2006'([1]), many of them 'overstayers'. Therefore, it is planned to establish a new border management, in particular an entry/exit system for all TCNs (COM(2008) 69 final: Preparing the next steps in border management in the EU). The European Parliament does not believe that this system will solve the problem, unlike Franco Frattini (Speech/08/142 on 12 March 2008). The VIS is a future system which will be 'fully operational in 2012 at the earliest' (COM(2008) 69 final). It will be one among other tools of the new border regime. According to a report drafted by Jeanine Hennis–Plasschaert, the fact that the VIS as well as SIS II are not yet operational will be an obstacle to the correct functioning of the planned entry/exit system ([2]).

Envisioned architecture and functions: The architecture of the future VIS system seems to be based on a central database (C–VIS) that allows for direct access by the respective National Visa Information Systems (N–VIS). The VIS shall provide National Visa Information Systems with data to verify, on entry, the authenticity of the visa and the identity of its holder. All TCNs requiring a visa could provide their biometric data (photograph, fingerprints) for the VIS when applying for a visa at a Member State's consular post, and border crossing points could be equipped to transmit data to and from the N–VIS. For checks within the Schengen Area law enforcement authorities will have access to the VIS allowing for identifying undocumented persons if they had been previously issued with a visa.

Issues: (1) The EDPS, in his Opinion on VIS (OJ 2006 C 97), is concerned about 'the general trend to grant law enforcement authorities access to several large scale information and identification systems'. He sees in this a serious violation of the principle of purpose limitation. (2) It is not quite clear how secure the transmission of the data of the visa holders from the Member States' consular posts to the Member States will be. About that point, there is no indication in the documents (inter alia: Council Decision 2004/512/EC (OJ 2004 L 213); Proposal for amending Regulation (EC) No 562/2006 (COM(2008) 101 final)).

[1] "The European Parliament discusses new measures for border management" (9 March 2009). Source: http://soderkoping.org.ua

[2] Ibid.

The European Criminal Records Information System (ECRIS) in development

Purpose and envisioned architecture: ECRIS is a planned system for exchanging criminal records in a standardised format. No new functionalities are envisioned so far. The data transferred via ECRIS will still be stored in the respective databases in each Member State (Draft Council Decision (14571/08 of 20 January 2009, Art. 3(2))). No central database will be established, ECRIS has a peer to peer architecture. 'Central authorities of the Member States […] shall not have direct online access to criminal records databases of other Member States' (Art. 3(3)). The information transmitted between the Member States will be 'extracted from criminal records' (Art. 1). The reason for the establishment of ECRIS is the following: 'Information on convictions is currently exchanged according to the European Convention on Mutual Assistance in Criminal Matters of 1959 […] This system presents important shortcomings […] The result is that national courts often pass sentences on the sole basis of the past convictions featuring in their national register without any knowledge of convictions in other Member States' (Proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS); COM(2008) 332 final).

Issues: Considering the architecture of ECRIS, it becomes obvious that no other approach than a decentralised system is possible. Crime data throughout Europe and within Member States suffer from high diversity. Thus, before establishing a common system, it seems reasonable to agree on a nomenclature of criminal offences. Otherwise, formalised systems will lead to high error rates and misinterpretation. ECRIS essentially only facilitates the transmission of data, whereas the responsibility for data protection and access remains with the Nation States — which does not pose much of a *new* threat for data protection according to the Opinion of the EDPS on the Proposal for a Council Decision on the establishment of the ECRIS (OJ 2009 C 42). Information security depends on the transmission infrastructure, which is planned to be S–TESTA.

3.2. S–TESTA — The Communication Infrastructure

S–TESTA (Secure Trans European Services for Telematics between Administrations) is the European Community's own private, IP–based network, a telecommunication infrastructure parallel to, e.g., the Internet in order to connect national networks of administrations, agencies and databases. The development of S–TESTA is part of a programme of the IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens), to be followed by ISA (Interoperability Solutions for European Public Administrations) from 2010. The purpose behind building a dedicated (separated) infrastructure for the exchange of data within the EU is to facilitate faster data exchange in a secure manner. As the IDABC puts

it: 'The need for tight security may sometimes appear to clash with the need to exchange information effectively. However, S–TESTA offers an appropriate solution.'

In fact, the S–TESTA architecture can be seen as a compromise between *cost*, *interoperability* on several levels and *security risks*. Being a network of networks, S–TESTA only connects existing decentralised Local Domains via its centralised structure. This architecture is recognised by the EDPS as offering better possibilities of risk management and data protection than a peer to peer architecture, where all networks establish links to each other (Opinion on ECRIS, OJ 2009 C 42). Data, for example ECRIS' criminal records, remains more or less securely within the national networks (instead of building one central database) and is only to be exchanged for specific purposes via the infrastructure of S–TESTA.

On the one hand, this separation of databases offers physical data protection, on the other hand, issues of interoperability still need to be solved for data exchange to make sense. This concerns all layers of interoperability: data formats, contents, used codes etc.. Here lies a possible source of errors during data exchange, use and interpretation which becomes more important for sensitive data. These issues are to be addressed by the eLink and CIRCA programmes on middleware and application interoperability.

The S–TESTA infrastructure is planned to be a one–for–all telecommunications infrastructure, that is: more and more purposes of data exchange are going to be fulfilled via S–TESTA. Data on natural and technological hazards, food ingredients, health, statistics, traffic, but also asylum seekers (EURODAC), visa (VIS), travelers (SIS II) and convicts (ECRIS) will be exchanged via the same hardware infrastructure. This is, from the management point of view, the most *cost–efficient* way to use the infrastructure.

Security–wise, this means that the information security of the S–TESTA infrastructure becomes the Achilles' tendon of all the data exchanges involved. The data protection risks on the physical layer are reduced to the *actual* moments of physical exchange — of information packet transport. But then again, the risk that the centralised system poses is generalised for all kinds of data and all exchange acts: if the system has *one* security gap, it can affect all transactions. It is a question of information security management then whether system monitoring, problem detection and handling are up to the security needs of the most sensitive data involved. The IDABC states that 'the continuing enhancement of security on S–TESTA will lead to the communications infrastructure being accredited, by 2009, to transport information classified to the level of EU RESTRICTED, according to the Council's security regulations (Council Decision 2001/264/EC [OJ 2001 L

101])'. An ongoing review of risks, technology development, contexts of data exchange on a legal and political basis (e.g., criteria of accrediting) needs to be coupled with high quality network management and maintenance of infrastructure — which might be another critical point, since the infrastructure is built, operated and supported by a consortium of private companies (Orange Business Services and HP): that adds another division of responsibilities to the whole system.

3.3. Interoperability, efficiency and data protection

On 24 November 2005, a Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs was published (COM(2005) 597 final). The Communication calls for a more powerful system of European databases, especially SIS II, VIS and EURODAC, and for new functionalities in the use of these databases. The Communication is motivated by a perceived need for the improvement of internal security due to terrorist attacks, as indicated by the given '*context*'. However, the identified shortcomings as well as the proposed scenarios are not exclusively directed towards terrorist threats — in fact, the arguments evoke the impression of a complete makeover, a reconfiguration of the existing data flows, contents and agencies in the European Security Regime. The context of an elevated terrorist threat, which arguably is hardly an issue of, say, illegal immigration, is used to make a point reshaping the informational systems in general for a variety of purposes.

Accordingly, the perceived shortcomings of the existing structures are less about interoperability than about *new* data and functionality *plus* interoperability: Limitations of alphanumeric searches, lacking possibilities of identification of illegal immigrants, no access to databases by internal security authorities, incomplete monitoring of exit as well as lack of biometric tools and especially lacking registration of EU citizens are *not* issues of interoperability, but extensions of the systems' functionality — a qualitative growth in tasks and possibilities. This growth might be a reason for the Commission's call for *efficiency*. In fact, the use of the term is not defined in the Communication, whereas *interoperability* and *synergy* are — but in a most problematic manner.

Interoperability is defined in a seemingly technical way, 'disconnected from the question of whether the data exchange is legally or politically possible or required'. This statement is extremely problematic, which is elaborated by both the EDPS (Comments on the Communication, 10 March 2006) and De Hert and Gutwirth (2006). First of all, interoperability is a multi–layer

concept which can be applied to data, connections, legal structures and other categories — the Communication is not clear about this term. Secondly, even *technical* interoperability always encompasses social, organisational, semantic etc. aspects. It is naïve to conceive of scenarios of infrastructures without anticipating their effects such as a *technological imperative* well known in Technology Studies. Thirdly, the Communication uses interoperability in a partial, positive way that suggests a linear relation between the grade of interoperability and the efficiency or effectiveness of systems. This is a view that should be complemented with the EDPS' expertise on using *missing* interoperability purposefully to technically enhance and ensure data protection (cf. the EDPS' remarks on possible 'restrictions on the sharing of primary keys' on p. 3 of his Comments). That perspective includes both function and data protection in the design of the infrastructures' characteristics instead of producing a contrast between the technological *possibilities* on the one hand and the legal or political *regulation and restriction* on the other. Interoperability should thus *not* be disconnected from legal and political questions.

This leads to the *synergy* and *efficiency*, which are pronounced as goals to be met by interoperability. The terms are well known from the 1990s management literature promoting lean production, flat hierarchies, or *streamlining*, as in the Communication. In relation to organisations, these terms imply using less resources by pooling them, which also suggests dependence on centralised assets. Synergy, on the other hand, should not be confused with efficiency, but implies enhanced effectiveness and even new competences. These terms point towards a *reduction of infrastructure overhead* that results from the connection and administration of the many national sources. Hence the idea to centralise the 'daily management' under the auspices of the FRONTEX agency. From a data protection point of view, as De Hert and Gutwirth (2006) argue, *the physical separation of data and systems is the most secure means of preventing misuse.* Efficiency and data protection, therefore, *cannot be balanced*. (For a general discussion of the 'metaphor of a balance between freedom and security', see Guild, Carrera and Balzacq (2008). This balance metaphor of which is made ritualistic use of in the current official security discourse whenever additional restrictions on personal liberty are introduced in the name of security *does not work*.)

The proposed biometric searches can be criticised as probability–based methods as argued by the EDPS. Other problems concern the compatibility with human rights and data protection. The Communication differentiates between 'innocent', clean record 'bona fide travelers' and, e.g., immigrants without ID documents: bona fide travelers may be segregated from other individuals rendering the checks more 'efficient' — this proposal is a direct contradiction to the statement of the proportionality principle in the Communication. Moreover, this proposal seems to not only exceed, but to clash entirely with the original purpose of preventing terrorist attacks. The Com-

munication does not specify any knowledge on the criminal nature of 'terrorist attacks' as, e.g., opposed to 'illegal immigration', which should be a departure point for the design of the informational structures. Instead, the Communication deals with a variety of very different purposes, scenarios, functions and data — all included in one new *interoperable* system possibly offering all combinations thereof.

To sum up, information systems need to be analysed in a differentiated way in order to make statements on interoperability, efficiency, data protection and security risks. The architecture of the respective systems — which encompasses social organisation as well as technical infrastructure — makes a great difference to their possible effects.

- First of all, the type of data stored must be taken into account. How 'sensitive' is the data? How is it coded? Is it 'interoperable' on an interpretive level (Does it make sense? Will errors be made?), on a legal level (Can it be used? Who accounts for it?), and on a technical level (What format does the data come in?)?
- How, where and how long for is the data stored? Is it (1) centrally stored? Or (2) decentrally distributed over all the Member States within their respective databases. In the second case, do the databases contain different data? Or is data matched between the Members?
- How can the data be accessed? Directly or via request? Fully or partially? Logically or in full text information (e.g. hit/no–hit)? Depending on whose decision?
- Who can access the data? What formal reasons must be given, what legal conditions do exist? How are they enforced? Are access activities logged and reviewed? How are results used?
- What Hardware infrastructure is used for the access? What else is connected through the infrastructure? How is the connection secured? Who maintains and manages the infrastructure? Who else knows the infrastructure well?
- How strict are rules for the users, both requesting and sending party? Can Member States apply tighter rules of data protection, e.g., refuse access?

All these aspects taken together form specific architectures of information systems that exhibit certain characteristics —strengths and weaknesses — when it comes to interoperability, efficiency and security risks. Accordingly, these characteristics amount to different levels of data protection.

4. Failure of Hague? Overview of the relevant EU legislation on information exchange

The abolition of national borders within the EU, originally triggered by the Schengen Agreement, has turned a huge part of the European continent into one criminal–geographic space. And the concept of an area of freedom, security and justice qualifies the territory of the EU in its entirety as indivisible in matters of internal security, i.e., *de facto* as territory of *one state*. Under these conditions, an enormous transnational security regime is under construction. The core of this new European Security Regime is to be a system of transnational information exchange. This system is to be a system of systems within which the totality of security–related information collected and processed at the national levels freely flows between all national and transnational security agencies across the EU.

The already mentioned Council Decision 2005/671/JHA (OJ 2005 L 253) has to be seen as one of many legal tools for the mobilisation of information which are in use in order to realise the ideal of absolutely free flow of information. The Decision obliges each Member State to transmit information concerning criminal investigations, prosecutions and convictions for terrorist offences to Europol and Eurojust (Art. 2(3)). Moreover, Art. 2(6) of the Decision obliges each Member State 'to ensure that any relevant information included in documents, files, items of information, objects or other means of evidence, seized or confiscated in the course of criminal investigations or criminal proceedings in connection with terrorist offences can be made accessible as soon as possible […] to the authorities of other interested Member States'. So all information is to be centrally pooled and, at the same time, as far as possible distributed among the Member States. The principle expressed in this twofold obligation (to spontaneously transmit and to make available as much information as possible) is known and has been heavily discussed as the *principle of availability*. It is the most radical response to the increased awareness of ubiquitous threats the EU could possibly produce.

4.1. Defining availability

Over the last years, the legislative process in matters of transnational information exchange has been highly dynamic. It shows a clear tendency towards ever further intensification which finds its expression in the continuous extension of the list of possible threats necessitating information exchange and the subsequent extension of the categories of data considered as security–relevant.

The advent of terrorism in Europe accelerated the process. On 25 March 2004, two weeks after the train bombings in Madrid, the European Council adopted a Declaration on combating terrorism: 'The Union and its Member States pledge to do everything within their power to combat all forms of terrorism in accordance with the fundamental principles of the Union, the provisions of the Charter of the United Nations and the obligations set out under United Nations Security Council Resolution 1373 (2001)' (7906/04).

The Declaration called, inter alia, for legislation 'simplifying the exchange of information and intelligence between law enforcement authorities of the Members States'. In response to the request a whole range of Notes and Communications followed, iterating the need for information exchange to combat terrorism. On 16 June 2004, a first contribution from the European Commission was published (COM(2004) 429 final). It set out five elements 'that are critical to achieving *free circulation of information* between the law enforcement authorities of the Member States, in a more structured way than has been the case up till now'[emphasis added]. These elements are:

1. the principle of equivalent access to data between law enforcement authorities;
2. scoping of the conditions for access;
3. data collection;
4. data exchange and processing; and
5. research.

On 22 September 2004, the Netherlands' EU Council Presidency responded with a Note (12680/04). It referred especially to the first element of the Commission's Communication, the principle of equivalent access to data, and renamed it as the 'principle of availability': 'With effect from 1 January 2008, exchange of information in the policy fields pertaining to the area of freedom, security and justice must be based on the principle of availability.' That is vividly illustrated:

'What the principle of availability means in practice is that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State without any problem, and that the law enforcement agency in the other Member State which holds this information is obliged to make it available for the stated purpose. It is essential that citizens be protected against abuses and incorrect information.'

The expression 'principle of availability' was introduced into the official discourse of the EU with the Hague Programme (5 November 2004) which adopted the concept and the definition just cited. The Programme claims: 'The mere fact that information crosses borders should no longer be relevant.' Passed in haste, the principle of availability immediately became a leitmotif of subsequent policy making in the field of internal security. Its

elaboration has been since then subject of a contest among Member States proposing legislation on transnational information exchange. Moreover, the Hague Programme explicitly recommends that 'the methods of exchange of information should make full use of new technology and must be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (on–line) access, including for Europol, to existing central EU databases such as the SIS.' The principle of availability accordingly became also the driving force for further security research on interoperable systems manifested in the Seventh Framework Programme for research and technological development which is devoted to stimulating the development and uptake of Information and Communication Technology over the period 2007–2013.

A Note of the Luxemburg Presidency of 25 March 2005 (7641/05) sketched a two step realisation of the principle of availability: firstly, the principle has to be established in its general legal outline and must, secondly, consist of the use of any new technological possibility available. The Note identified four modalities of implementing transnational access to information on the basis of the principle:

1. indirect access to information upon request;
2. indirect access to information of another Member State through a central index on a hit/no–hit basis;
3. direct access to the databases of another Member State; and
4. the creation of central European databases.

What is striking about these modalities is that they can be read as the description of a stepwise process towards total data integration. In this case, national sovereignty in terms of internal security would be liquidated completely. Indeed, the translation of Communications and Notes into either proposed or even implemented EU legislation shows that this process is likely to attain its goal — unless pronouncements of national sovereignty impede it.

4.2. A first approach: The 'Swedish Initiative'

The Note of the Luxemburg Presidency already referred to the Initiative of the Kingdom of Sweden to adopt a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts (OJ 2004 C 281).

Published on 18 November 2004 in the Official Journal, immediately after the adoption of the Hague Programme, the Swedish Initiative seemingly disturbed the debate on the principle of availability, at least to some degree. It was explicitly perceived by security experts at EU level to be de-

signed for improving transnational information exchange only in the short term. As Director General Jonathan Faull (JHA Directorate General) argued: 'Our proposal, on the establishment of a right of equivalent access is seen by delegations in the relevant Council working group (known as the multi–disciplinary group) as a longer–term project which will provide for a wider sharing of information between law enforcement authorities of the Member States in the future' (House of Lords 2005, Oral Evidence, p. 39).

However, in line with the Declaration of the European Council the Swedish Initiative clearly expressed concern about the lack of common structures and procedures for the exchange of relevant information between Member States. Paragraph 8 of the preamble reads: 'The absence of a common legal framework for the effective and expeditious exchange of information and intelligence between law enforcement authorities of the Member States is a deficiency that will have to be remedied […].' Facing terrorism, the main purpose of the Initiative is to set the basis for a legally binding framework in order to increase the effectiveness of data sharing within the EU. Following the modality of indirect access to information upon request, four aspects stand in the core of the Swedish Initiative:

1. Direct requests and responses for information exchange between law enforcement authorities;
2. time limits for the provision of information;
3. obligation to answer a request; and
4. equal conditions for intranational and transnational information exchange.

In 2006, the Initiative finally turned into a Framework Decision (2006/960/JHA; OJ 2006 L 386). Nevertheless, the full realisation of the principle of availability required further legislative action, as will be shown. Between the original proposal of the Swedish Initiative and the actual Council Framework Decision, there are some changes and additions that deserve attention. In the Framework Decision the key concern of the proposal has been made invisible: the phrase referring to terrorism in the title is deleted. Terrorism is now seen — so to say, *normalised* — as one serious offence among others, whereas next to organised crime its importance to justify transnational data exchange remains unquestioned: 'It is important to promote the exchange of information as widely as possible, in particular in relation to offences linked directly or indirectly to organised crime and terrorism […]' (preamble, para. 10). Nevertheless, the rewording of the title expresses clearly the intention to stress the *continuity* of the EU policy on transnational data exchange since the Schengen Convention.

The second change concerns the definition of the authorities competent to request or receive information via the request system. While the original proposal was, at least, unclear on this point, the Framework Decision ex-

cludes explicitly secret services from the information and data exchange procedure (Art. 2(a)). On the other hand, the power to define which agency counts as a competent law enforcement authority remains with the individual Member States in accordance with their individual national law. That is crucial. The Framework Decision does explicitly not purport to change the existing national law systems (preamble, para. 7). Because the Framework Decision accepts the different law systems as they are, this turns the declared exclusion of secret services upside down. If in an individual Member State the separation between police forces and secret services blurs or does not exist, the possibility that those services nevertheless become engaged in the transnational information exchange is actually given. A similar problem exists as regards the application of coercive measures in obtaining information and intelligence (Art. 1(6)).

A further change between the proposal and the Framework Decision concerns the communication channels used for the information exchange. While the proposal suggested different channels such as the SIRENE bureaux (Art. 7(1)), the Framework Decision does not bind the procedure regulated in it to any specific channel (Art. 6(1)). At least theoretically, this means that any law enforcement agency may communicate with any other agency throughout the EU. That already ensures the fulfilment of the principle of availability, admittedly, within the framework of indirect access to information upon request: information is taken after it has been given. It cannot be simply taken. The respective law enforcement officer in one Member State who needs information in order to perform his duties must justify his request before data is transmitted through the law enforcement agency in the requested Member State. The procedure of requesting and answering is standardised. In this respect, the most important addition to the original proposal are two forms annexed to the Framework Decision which are to be used in the exchange procedure. They limit the communication on a set of predefined items such as the nature of offences, the purpose for which the information or intelligence is requested, the persons being the subject of the criminal investigation involved and some others more. Only three free fields are given to specify the grounds for the urgency of the request, the type of information requested and the type of criminal activity investigated. This, at a first glance, only bureaucratic instrument is factually highly important because it regulates the exchange procedure preventing direct access to databases of another Member State. It is valuable in two respects: First, the documentation of the acts of information exchange allows for tracking the requests and answers for purposes of the investigating agencies. Increasing the level of transparency of the exchange, the very same documentation may serve, secondly, as a means for data protection measures.

COUNCIL FRAMEWORK DECISION 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities (LEAs) of the Member states of the EU (OJ 2006 L 386)

The FD regulates the transnational information exchange between 'competent' LEAs on the basis of a request system. 'Competent law enforcement authority' is defined as 'national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities […] Agencies or units dealing especially with national security are not covered' by this concept (Art. 2(a)). 'Information and/or intelligence' is defined as 'any type of information or data' held by LEAs or 'held by public authorities or by private entities' and which is available to LEAs 'without the taking of coercive measures' (Art. 2(d)). But 'Member States shall, where permitted by and in accordance with their law, provide information or intelligence previously obtained by means of coercive measures' (Art. 1(6)). The essential provision of the FD reads: 'Member States shall ensure that conditions not stricter than those applicable at national level for providing and requesting information and intelligence are applied for providing information and intelligence to competent law enforcement authorities of other Member States' (Art. 3(3)). Time limits are set for the provision of information (Art. 4). But the requested Member State may refuse the provision of information requested. Information may be withhold, inter alia, if its provision would 'harm essential national security interests of the requested Member State' (Art. 10(a)). In respect to data protection, the information and intelligence exchange is subject to the national data protection laws of the receiving state, whereas personal data must be protected in accordance with the the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and, for those Member States which have ratified it, the Additional Protocol of 8 November 2001 to that Convention, regarding Supervisory Authorities and Transborder Data Flows (Art. 8). Finally, two forms are annexed to the FD to be used by the requested and the requesting Member State, respectively.

The Framework Decision provides a regulative framework for transnational information exchange on the basis of a rather simple and technologically less sophisticated system. It can be assumed that its easy manageability was responsible for the fact that it quickly gained acceptance among relevant actors and agencies. Member States have implemented the procedure. In urgent cases requests have to be answered within eight hours and at the latest after 14 days. Nevertheless, in regard to the legislation on transnational information exchange under the principle of availability this Framework Decision remains an intermediate step.

4.3. Towards availability via Prüm?

The Treaty of Prüm paved the way in this respect. It was signed between Belgium, Germany, Spain, France, Luxemburg, the Netherlands and Austria on 27 May 2005 (10900/05). Pronouncing national sovereignty while claiming 'to play a pioneering role in establishing the highest possible standard of cooperation' it was perceived in the context of the efforts at EU level as, at least, an ambivalent step, if not as a bypassing of the EU framework. The treaty challenged the balance between inter–governmental and supra–governmental actions, 'creating a hierarchy within the EU' as scholars argued (Balzacq et al. 2006). Designed to intensify cross–border police cooperation, especially in the fight against terrorism, cross–border crime and illegal immigration, the Prüm system implies a mixture of modalities of mutual access by the creation of a network of specific databases: First, indirect access to DNA and dactyloscopic information held by another contracting party through a central index on a hit/no–hit basis and, secondly, direct online read access to the vehicle registration database of another contracting party. Admittedly, the information exchange is restricted to National Contact Points with designated personnel in charge. Nevertheless, with this model the Prüm Treaty has established an advanced form of transnational information exchange. Information exchange and other forms of cooperation in connection with major events, disasters and serious accidents as well as in the event of imminent danger are also regulated in the Prüm Treaty. Additionally, law enforcement and immigration agencies may be authorised to execute joint operations within a contracting party's territory. The Treaty entered into force on 1 November 2006. The EDPS characterised the approach the Treaty of Prüm follows as the 'data field–by–data field approach', 'a more cautious approach which involves one type of data' and then monitors 'to what extent the principle of availability can effectively support law enforcement, as well as the specific risks for the protection of personal data' (para. 50 of the Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability; OJ 2006 C 116). Less harmless, on the other hand, is the fact that the Treaty of Prüm 'necessarily leads to the establishment of new databases which in itself presents risks to the protection of personal data' (para. 49).

TREATY OF PRÜM

Relevant for the subject under consideration are Art. 2–15. The Contracting Parties (CPs) keep national DNA analysis files. They allow other CPs' national contact points access to the reference data in their files (hit/no–hit access). Should the procedure show a match between DNA profiles, the supply of any further information is governed by the national law (Art. 2–6). On request the requested CP shall provide legal assistance by collecting and examining cellular material from a person present within the requested CP's territory under the requested CP's law (Art. 7). The CPs allow other CPs' national contact points access to the reference data from the file for the national automated fingerprint identification systems, 'with the power to conduct automated searches by comparing fingerprinting data' (Art. 8–9(1)). 'Firm matching of fingerprinting data […] shall be carried out by the searching national contact point' (Art. 9(2)). '[T]he supply of any available further personal data and other information relating to the reference data shall be governed by the national law' (Art. 10). The CPs allow other CPs' national contact points access to national vehicle registration data comprising data relating to owners and operators, and data relating to vehicles 'in compliance with the searching CP's national law' (Art. 12(1)). 'For the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings, the CPs shall, both upon request and of their own accord, in compliance with the supplying CP's national law, supply one another with personal data if any final convictions or other circumstances give reason to believe that the data subjects will commit criminal offences at the event or pose a threat to public order and security, in so far as the supply of such data is permitted under the supplying CP's national law' (Art. 14(1)). 'The data supplied must in any event be deleted after not more than a year' (Art. 14(2)). (Cf. the overview of status of ratification/entry into force of the Treaty of Prüm in Annex A to the present paper.)

As the Initiative of the Kingdom of Sweden, the Treaty of Prüm definitely increased the given pressure on the EU Commission's law making intentions since the adoption of the Hague Programme. Given the step forward that Prüm took on the path towards the realisation of the principle of availability, the question arised how a further step could be taken at EU level. Reference to both, the Swedish Initiative as well as the Treaty of Prüm, as the 'most important' approaches, were made in the Proposal for a Council Framework Decision on the exchange of information under the principle of availability presented by the Commission on 12 October 2005 (COM(2005) 490 final). Although similarities between the current Proposal to implement the principle of availability and Prüm are seen, also criticism was expressed. The explanatory memorandum to the Proposal stresses 'seven main obstacles' that

existed ‘to information to be generally available throughout the EU’. Inter alia, ‘bi– and multilateral agreements between Member States’ are criticised as ‘either geographically restricted’ (Prüm) or for not obliging ‘Member States to provide information, making the exchange of data dependent on discretionary factors’ (Swedish Initiative). Moreover, ‘current forms of law enforcement cooperation usually require intervention of national units or of central contact points. Direct information exchange between authorities is still the exception’. The potential of the principle of availability is thus seen as not exhausted. The Swedish Initiative and Prüm are welcomed to highlight the extended approach of the current Proposal itself, which:

> introduces online access to available information and to index data for information that is not accessible online, following the Member States’ notification of information available within their jurisdictions. By doing so, it avoids fishing for data, as it allows knowing whether the information sought is available before issuing an information demand, and permits efficient and targeted requests. It furthermore harmonises the grounds for refusal that are also binding on the authorities that — pursuant to national law — must authorise the access or transfer of information. Therefore, the uncertainty inherent in an information request is reduced to a minimum (p. 4).

COMMISSION PROPOSAL FOR A COUNCIL FRAMEWORK DECISION on the exchange of information under the principle of availability (COM(2005) 490 final)

The proposed Framework Decision (PFD) obliges Member States to ensure that law enforcement relevant information 'shall be provided to equivalent competent authorities of other Member States and Europol' (Art. 6). The equivalence of LEAs of different Member States is to be assessed on the basis of a criteria list (Art. 5(1)). 'Information' is defined as 'existing information' (Art. 3(a)) of the following types: DNA–profiles, fingerprints, ballistics, Vehicle registration information, telephone numbers and other communications data (content data excluded), personal data (Annex II). 'Information that has been lawfully collected by means of coercive measures shall be treated as available information' (Art. 2(2)). The equivalence of LEAs of different Member States is to be assessed on the basis of a criteria list (Art. 5(1)). The obligation to provide information includes the obligation to ensure 'that equivalent competent authorities of other Member States and Europol shall have online access to the information contained in electronic databases to which their corresponding competent authorities have online access' (Art. 9(1)), whereas 'online access' means 'the automated access to an electronic database for the purpose of consultation of and access to its content, from another location than in which the database is located, without intervention of another authority or party' (Art. 3(f)). That is the first of the two essential, because revolutionary, provisions of this PFD. The second reads: 'Member States shall ensure that index data of information that is not accessible online, shall be available for online consultation […] and shall establish to this end the appropriate technical infrastructure' (Art. 10(1)). When consultation of index data results in a match, an information demand may be issued (Art. 11). Provision of information may be refused in order 'to protect the fundamental rights and freedoms of persons whose data are processed' under this PFD (Art. 14(1)(d)).

First, online access 'without intervention of another authority or party' means in fact the loss of control of a Member State over the processing of the data collected by the very same State. Secondly, the obligation stated in the Proposal to establish an appropriate technical infrastructure for index data files is extremely costly and time–consuming. Given this background, the Proposal remained at the level of a hopeful monstrosity. Instead, the Swedish Initiative actually succeeded, although it stays behind what is envisioned at the EU level. The Initiative must be seen as a pragmatic common sense solution of the burning problem to have to implement a legal framework for transnational information exchange as fast as possible.

Given that the Proposal remained in the status of a proposal, at least at this stage, it seems that Prüm actually provided a path for the further continua-

tion of implementing the principle of availability. From the perspective of their seven initiators, the Treaty reads as a success story. Finally, under increasing pressure due to an increasing number of further Accession States to the treaty (cf. Annex A to this paper), in June 2008, 'the substance of the provisions of the Prüm Treaty' was integrated 'into the legal framework of the European Union' by Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ 2008 L 210). The German Presidency had initiated the debate on the integration of Prüm into the EU legal framework at the informal Ministers' meeting in Dresden on 15–16 January 2007 and immediately gained broad support. While the Council Secretariat needed not more than four days after the meeting to publish a first draft of a Council Decision, only a month later, on 15 February 2007, it was already agreed upon at the Justice and Home Affairs Council by 15 Member States to adopt a Council Decision without any further consultation of other Member States and the European Parliament, further impact assessments and so forth as the Hague Programme actually demanded. 'It was *fait accompli* […] The method in which the arrangement was reached demonstrates just how underhanded Eurocrats can be in getting their way — all at the expenses of national sovereignty' (Kierkegaard 2009).

The Council Decision catches up with the Prüm system by identifying it as being compliant with the principle of availability. That shows, beyond any doubt, that Prüm did not circumvent the EU framework. If the Treaty of Prüm had breached the law of the EU (breach of the obligation of cooperation under Art. 10 TEC; cf. Balzacq 2006), this, however, had no consequence: 'One could argue that the Prüm Convention breaches the law of the European Union […]. However, this argument is mainly of a theoretical nature, in the framework of the third pillar with limited powers of the Commission to ensure compliance with the law of the European Union by the Member States […]' (Opinion of the EDPS of 4 April 2007 (OJ 2007 C 169), para. 14). As history shows, the initiators could calculate with some certainty to be finally consumed by the common EU policy as Art. 1(4) of the Prüm Treaty intended. The mutual strategic instrumentalisation of national proposals, inter–governmental initiatives and Europeanisation constitutes the dynamic of the ongoing legislation on transnational information exchange. Other Member States were encouraged to join or simply remained unheard. The German Presidency was highly aware of the fact that the EU with their executing apparatuses wanted to keep leadership and stay in control of the process. Sooner or later, despite all ambivalences, the EU would welcome the high integrative potential of Prüm in order to fulfil the demands of the Hague Programme. Hugo Brady is right therefore when he adjusts the criticism of some observers like Balzacq et al. (2006) that the Treaty 'provokes a relapse of EU integration' (p. 2):

> Some observers feared the Prüm group would undermine efforts to facilitate information–sharing in the EU as a whole, since it involved only a handful of countries and ignored related initiatives by the European Commission. But it turned out that the Prüm treaty was the best way to encourage wider information–sharing. The seven Prüm countries have acted as a 'laboratory', working out the complicated technical arrangements for querying each others' police databases quickly and effectively in a small group. (Brady 2007, pp. 21–22)

The integration of Prüm into the EU framework was a highly appreciated outcome. It is in perfect accordance with the idea of Europeanisation as transformation of the Common Market into a common European State already heralded in the area of freedom, security and justice. Indeed, in some respect the Europeanisation of Prüm can be seen as the realisation of the Commission Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final). To further insist on the Proposal has become unnecessary, because Decision 2008/615/JHA ('Prüm Decision') has pushed the legislative process as far as it is possible at the time being. Also the Swedish Initiative is integrated into the provisions of the Decision: in the case of a hit in the index data related to, e.g., a DNA content data file, the well–established mechanism based on Decision 2006/960/JHA (Swedish Initiative) may be used for requesting the content data (preamble, para. 10). Thus, the Prüm Decision fuses the different streams of legislation on transnational information exchange having emerged since the Hague Programme had called for innovative approaches.

COUNCIL DECISION 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ 2008 L 210)

The Council Decision (CD) incorporates 'the substance of the essential parts of the Prüm Treaty' into the legal framework of the EU (preamble, para. 1 and 9). 'For the Member States concerned, the relevant provisions of this Decision shall be applied instead of the corresponding provisions contained in the Prüm Treaty. Any other provision of the Prüm Treaty shall remain applicable between the contracting parties of the Prüm Treaty' (Art. 35(1)). The CD does not contain the following provisions of the Prüm Treaty: the provisions relating to Air marshals (Art. 17–19); Measures to combat illegal migration (Art. 20 –23); Measures in the event of imminent danger (*hot pursuit*) (Art. 25); Co-operation upon request (Art. 27). The corresponding provisions are nearly verbatim identical. Inter alia, the CD contains provisions on: (a) the automated transfer of DNA profiles, dactyloscopic and vehicle registration data (Chapter 2); (b) the conditions for the supply of information in order to prevent terrorist offences (Art. 16); (c) the supply of data in connection with major events with a cross–border dimension (Art. 18); (d) joint operations (Art. 17). The CD points to the possibility to make use of the request procedure according to CD 2006/960/JHA subsequent to a hit in an index data file. As regards data protection, the CD stresses strongly that 'data protection provisions should take particular account of the specific nature of cross–border online access to databases. *Since, with online access, it is not possible for the Member State administering the file to make any prior checks, a system ensuring post hoc monitoring should be in place*' (preamble, para. 17) [emphasis added]. The CD stresses also 'that the supply of personal data to another Member State requires an adequate level of data protection on the part of the receiving Member States' (preamble, para. 18). As regards implementation, 'Member States shall take the necessary measures to comply with the provisions of this Decision within one year of this Decision taking effect, with the exception of the provisions of Chapter 2 [see above] with respect to which the necessary measures shall be taken within three years' (Art. 36). Thus, the deadlines for implementation are August 2009 and August 2011, respectively.

The Prüm Decision is certainly not an implementation of the principle of availability in the full sense of its meaning. When the Hague Programme addressed the principle as a response to the '*fact* that information crosses borders should no longer be relevant' [emphasis added], then this seems hardly the case. There are different models covering different degrees of the principle that have to be considered in order to understand the rationale of its realisation. According to Bigo et al. (2007) the principle of availability divides into two sub–principles: *visibility* and *readability*. Taking as well the Swedish Initiative into account, a third has to be added, which could be called the *pragmatic* sub–principle. It is based on indirect access to informa-

tion upon request. The sub–principle of visibility of information is indeed already a stepping up. It is based on the hit/no–hit model to launch a data query at a central unit or a national database to identify whether it contains a specific item. If a hit is made the law enforcement authority can make a request to the Member State where the data is stored for further information. Only the sub–principle of readability of information implies the full online read access. Given that Prüm is a mixed system underlines that the sub–principle of full readability is only envisaged and that the claimed fact that information crosses borders should no longer be relevant is a mere technocratic phantasm or the natural ideology of a transnational body.

In his aforementioned Opinion of 4 April 2007 (OJ 2007 C 169), the EDPS commented the coming Prüm Decision: It 'only takes a small step. […] The initiative can be qualified as a step towards availability, but does not *stricto sensu* implement the principle of availability' (para. 24). However, does this mean that the process of full realisation of the principle has come to its end? The situation of EU data protection legislation fits perfectly into the picture of an ongoing realisation of the principle of availability beyond Prüm. The realisation of the principle of availability has to be accompanied by relating data protection legislation. In his Proposal for a Recommendation to the Council on interoperability and synergies among European databases in the area of JHA of 8 June 2006, Alexander Alvaro already expressed his strong concerns about inherent risks of large–scale databases in matters of data protection and privacy. He explicitly mentioned profiling, data–mining and misuse of databases for purposes for which they were not originally designed. The problem had been of principle nature. The absence of a General Framework Decision on Data Protection under the 3rd pillar had caused a situation in which the protection of personal data had become precarious. Under the impact of the principle of availability this situation exacerbated. It became inacceptable vis–à–vis a policy the guiding principle of which since the *European Security Strategy* (December 2003, drawn up under the authority of the HR Javier Solana) had become the intensification of measures to combat crime based on monitoring the every day life of the European citizens.

Solana's claim that internal and external security were indissolubly linked had two implications. First, it meant that internal security had not only to be ensured at home but also abroad, insofar external action shaped the environment in which the EU is embedded. Secondly, and this is most important to the argument, it meant that external security had not only to be ensured abroad but also at home. In the same vein the *9/11 Report* of the National Commission on Terrorist Attacks upon the United States (July 2004) argued: 'In the post-9/11 world, threats are defined more by the fault lines within societies than by the territorial boundaries between them' (*9/11 Report*, p. 361). This dramatic shift in the definition of the conditions under which security has to be provided necessarily alters the relationship be-

tween the state, its law enforcement authorities and the citizens: 'The real risk is freedom and the real enemy of security — in principle and in general — is the free citizen' (Nelles 2004, p. 84). *Under this definition data protection appears to be a security risk*.

The formulation of the principle of availability is one of the most serious consequences of situation assessments like those delivered by the *European Security Strategy* and the *9/11 Commission Report*. And this principle of availability is the natural enemy of the decisive principle of data protection — the principle of purpose limitation.

The latest opportunity to resolve the problem of highly diverse data protection regulations within the EU, affecting in particular transnational information exchange, has been wasted. Noteworthy, that this again happened under the German Presidency — in the very same year that saw the incorporation of Prüm into EU law. After several years of discussions and debates at European and national levels, the German Presidency redrafted the Commission's original Proposal for a Framework Decision, simply ignoring the manifold concerns on this matter. The Council Framework Decision 2008/977/JHA (OJ 2008 L 350) on the protection of personal data adopted last December reads like the turning away from the concept that personal data is in principle protected against complete state access.

The principle of availability will continue to be a leitmotif, but it will be complemented by the so–called *convergence principle* as it has been expressed by the Future Group in its June 2008 Report:

> The *convergence principle* would apply to all areas where closer relations between Member States are possible: agents, institutions, practices, equipment and legal frameworks. These closer relations would be based on the Union's Acquis and would make full use of the European Union instruments. Added value would be systematically sought in the definition and implementation of the corresponding projects. Seeking added value and developing the convergence principle lead to the same goal. The closer Member States cooperate with each other, the clearer the shared values as well as the national reservations will be. (p. 11)

This principle of convergence reminds strongly of the CTC's *broader and coherent approach*. European security policy obviously has realised that mere technical interoperability is not enough in order to step up effectiveness in combating security threats.

5. Concluding remarks and recommendations

The Hague Program was deficient. Its recommendation to make 'full use of new technology' under the principle of availability was not only unrealistic, but technocratic. This becomes visible in at least three aspects:

1. the complete failure to adjust data protection legislation appropriately, thereby endangering privacy and civil liberty;
2. the blinding out of what could be called the diversity of security cultures within law enforcement agencies leading to increasing discretion and consequently to a refusal of authorities to share data with each other; and
3. the reduction of the highly sensitive political as well as social issue of transnational information exchange to a mere technological problem as indicated most prominently in the misinvestments in SIS II as well as in preparations of the post–Hague Programme focusing on the creation of total information integration of daily life.

According to these three fields the following remarks and recommendations are made.

5.1. Slowing down the evolution of the European Security Regime

If the future of the European Security Regime is to be a future *order*, manageable in the best of the interest of the European citizens, other kinds of reflexivity and anticipation as well as democratic participation have to come into play. This implies necessarily that the further evolution of the European Security Regime needs urgently to be slowed down and its status quo thoroughly assessed before further action will be taken.

1. It is recommendable not to further extend the categories of persons to be entered into the systems of information processing and exchange (e.g., 'troublemakers').

2. It is recommendable not to further extend the categories of personal data to be entered into the systems of information processing and exchange.

3. It is recommendable not to further extend the categories of 'competent authorities' having access to the systems of information processing and exchange.

4. In this context, it is not only recommendable but imperative to assess the degree of access secret services have to the systems of transnational information exchange. This seems to be necessary because of the steadily

rising importance of the role secret services play in modern counter–terrorist efforts (cf. chap. 4 of the recently published *Report of the Eminent Jurists Panel on Terrorism, Counter–Terrorism and Human Rights)*.

5. It is recommendable not to further simplify the procedures of information exchange between law enforcement authorities (e.g., direct read access).

6. On the contrary, it is recommendable to recognise the further above described procedure of transnational information exchange under Framework Decision 2006/960/JHA (Swedish Initiative) as a *standard model*.

7. On the basis of this already working *Swedish Model*, an unsolicited, *voluntary* stepwise legal harmonisation as well as cultural approximation of police work within the EU seems to be conceivable because this model is the least aggressive on the scale of transnational data integration as outlined in the Note of the Luxemburg Presidency (see above, p. 27).

8. There still seems to be extremely little *independent academic research into the factual effectiveness* of the policy of stepping up transnational information exchange between law enforcement authorities within the EU. That may well be the result of the fact, as Fijnaut and Paoli (2004, p. 1040) observe in a similar context, 'that domestic and international government bodies have no interest in the results of such research revealing that there is a huge difference between the policy as formulated on paper and what has been achieved in practice'. But because transnational information exchange has considerable political and social consequences, this situation has to change: it is recommendable to step up such independent academic empirical research. That would be a decisive step towards the urgently needed democratisation of the current EU policy in matters of (internal) security.

5.2. Regulating data exchange practices

Data protection legislation has so far been subject to much criticism concerning its lack of effectiveness, its tendency to be reactive rather than proactive, its incapacity to keep pace with the rapid development of new surveillance and information technologies and procedures. And rightly so, because the need of data protection should determine technology, not the other way round.

9. An important approach to solve the problem of pure reactiveness of traditional data protection legislation is a methodology called "KORA" ("Konkretisierung rechtlicher Anforderungen", i.e., "concretion of legal require-

ments"), developed by Alexander Roßnagel (University of Kassel, Germany). KORA aims at bridging the gap between general legal provisions and specific decisions in the process of technical design. The application of KORA means that legal requirements for relevant technologies are developed from constitutional and other legal norms. These legal requirements are transformed into criteria for the design of specific technical systems. Lawyers and technical scientists work together to answer the question which essential functions the technology has to possess in order to meet the defined legal criteria. KORA is the attempt to integrate data protection into the technical design process. It is recommendable to make use of such a *hybrid (legal–technical) design method* for the development of future systems of information processing and exchange.

5.3. Constructive Technology Assessment

Another point, not mentioned yet explicitly in this paper, has to be addressed: the problem of lacking technology acceptance which goes hand in hand with the introduction of ever more sophisticated technologies, e.g., complex systems of automated information exchange.

10. An important approach to solve this problem is the so–called Constructive Technology Assessment (CTA). CTA aims to work towards *better technology*, i.e., *technology with less negative social effects*, from the early stages of technological life cycles on. In the perspective of CTA, technology assessment is considered as part of the reflexive co–evolution of science, technology and society — therefore, it is *constructive*: 'CTA can be seen as a new design practice (which includes tools) in which impacts are anticipated, users and other impact communities are involved from the start and in an interactive way, and which contains an element of societal learning' (Schot and Rip 1996, p. 255). It is recommendable to make use of CTA in order to support both policy makers on transnational information exchange and end–users of technical systems within law enforcement agencies in minimising mismatches, avoiding possible conflicts and misinvestments.

11. The authors of this paper finally hope that the coming Council Working Group on transnational information exchange will be aware of the fact that the problem–solving capacity of a technology cannot possibly be greater than the problem–solving capacity of the society which makes use of this technology.

6. VI. Bibliography

Publications in the Official Journal

— OJ 2000 L 239: Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [Schengen Agreement, 1985]

— OJ 2000 L 239: Convention implementing the Schengen Agreement of 14 June 1985 [1990]

— OJ 2000 L 316: Council Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention

— OJ 2001 L 101: Council Decision 2001/264/EC adopting the Council's security regulations

— OJ 2003 L 16: Council Decision 2003/48/JHA on the implementation of specific measures for police and judicial cooperation to combat terrorism

— OJ 2003 L 50: Council regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third–country national

— OJ 2004 L 162: Council Regulation (EC) No 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism

— OJ 2004 L 213: Council Decision 2004/512/EC establishing the Visa Information System (VIS)

— OJ 2004 C 281: Initiative of the Kingdom of Sweden with a view to adopting a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts

— OJ 2005 L 68: Council Decision 2005/211/JHA concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism

— OJ 2005 L 253: Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences

— OJ 2006 C 91: Opinion of the EDPS on the Proposals COM(2005) 230 final, 236 final and 237 final [concerning establishment, operation and use of SIS II]

— OJ 2006 C 97: Opinion of the EDPS on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final)

— OJ 2006 C 116: Opinion of the EDPS on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final)

— OJ 2006 L 381: Regulation (EC) No 1986/2006 of the European Parliament and of the Council regarding access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates

— OJ 2006 L 381: Regulation (EC) 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of SIS II

— OJ 2006 L 386: Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU

— OJ 2007 C 169: Opinion of the EDPS on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany etc., with a view to adopting a Council Decision on the stepping up of cross–border cooperation, particularly in combating terrorism and cross–border crime

— OJ 2007 L 205: Council Decision 2007/533/JHA on the establishment, operation and use of SIS II

— OJ 2008 L 210: Council Decision 2008/615/JHA on the stepping up of cross–border cooperation, particularly in combating terrorism and cross–border crime

— OJ 2008 L 350: Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

— OJ 2009 C 42: Opinion of the EDPS on the proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS)

Publications of the Council of the European Union

— Declaration on combating terrorism (7906/04; 29 March 2004)

— Exchange of Information [Note from the Presidency] (12680/04; 22 September 2004)

— The Hague Programme (16054/04; 13 December 2004)

— Replies to questionnaire on Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, in particular as regards serious offences including terrorist acts (5815/1/05 REV 1; 2 February 2005)

— Approach for the implementation of the principle of availability [Note from the Presidency] (7641/05; 25 March 2005)

— Prüm Convention [i.e., Treaty of Prüm] (10900/05; 7 July 2005)

— The European Union Counter–Terrorism Strategy [Note from the Presidency and the EU Counter–Terrorism Coordinator] (14469/4/05 REV 4; 30 November 2005)

— List of competent authorities which are authorised to search directly the data contained in the Schengen Information System pursuant to Art. 101(4) of the Schengen Convention (6073/2/07 REV 2; 25 June 2007)

— Implementation of the Strategy and Action Plan to Combat Terrorism [Note from the EU Counter–Terrorism Coordinator] (15411/07; 23 November 2007)

— EU Counter–Terrorism Strategy — Discussion paper [Note from the EU Counter–Terrorism Coordinator] (15983/08; 19 November 2008)

— Council Decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/…/JHA [draft] (14571/08; 20 January 2009)

— Press Release: 2927th meeting of the Council Justice and Home Affairs, Brussels, 26–27 February 2009 (6877/09 (Presse 51))

Publications of the Commission of the European Communities

— Towards enhancing access to information by law enforcement agencies [Communication to the Council and the European Parliament] (COM(2004) 429 final; 16 June 2004)

— Proposal for a Council Decision on the establishment, operation and use of SIS II (COM(2005) 230 final; 31 May 2005)

— Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of SIS II (COM(2005) 236 final; 31 May 2005)

— Proposal for a Regulation of the European Parliament and of the Council regarding access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final; 31 May 2005)

— Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final; 12 October 2005)

— Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs [to the Council and the European Parliament] (COM(2005) 597 final; 24 November 2005)

— Preparing the next steps in border management in the European Union [Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions] (COM(2008) 69 final; 13 February 2008)

— Preparing the next steps in border management in the EU [Commission Staff Working Document accompanying COM(2008) 69 final] (SEC(2008) 153; 13 February 2008)

— Proposal for a Regulation of the European Parliament and of the Council […] amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code (COM(2008) 101 final; 22 February 2008)

— Proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA (COM(2008) 332 final; 27 May 2008)

— Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007 (COM(2009) 13 final; 26 January 2009)

Other official documents and reports

— [Javier Solana]: *European Security Strategy (A secure Europe in a better world)*. Brussels, 12 December 2003

— *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Official Government Edition, 22 July 2004

— House of Lords: *After Madrid: the EU's response to terrorism*. 5th Report of Session 2004–05 of the European Union Committee, HL Paper 53, London, 8 March 2005

— European Data Protection Supervisor: *Comments on the Communication of the Commission on interoperability of European databases*. Brussels, 10 March 2006 [available on EDPS website]

— Alvaro, Alexander: "Proposal for a recommendation to the Council on interoperability and synergies among European databases in the area of justice and home affairs". Session document B6–0336/2006 of the European Parliament, 8 June 2006

— Schengen Joint Supervisory Authority: *Article 99 Inspection*: *report on an inspection of the use of Article 99 alerts in the Schengen Information System*. Report nr. 07–02, Brussels, 18 December 2007

— The Association of European Police Colleges (AEPC): *AEPC, the future*: *strategy document*. 2008 [available on www.aepc.net]

— Frattini, Franco: *Providing Europe with the tools to bring its border management into the 21st century*. Speech (08/142) at the Ministerial Conference on the Challenges of the EU External Border Management, Brdo (Slovenia), 12 March 2008

— The Future Group: *Freedom, Security, Privacy — European Home Affairs in an open world*. Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, June 2008

— *Défense et sécurité nationale: Le livre blanc*. Paris, June 2008

— [Eminent Jurists Panel]: *Assessing Damage, Urging Action: Report of the Eminent Jurists Panel on Terrorism, Counter–terrorism and Human Rights*. Geneva, 2009

Secondary literature

— Balzacq, Thierry: *The Treaty of Prüm and the principle of loyalty (Art. 10 EC)*. Briefing Paper for LIBE, 13 January 2006 [available on www.libertysecurity.org]

— Balzacq, Thierry et al.: *Security and the two–level game: the Treaty of Prüm, the EU and the management of threats*. CEPS Working Document No. 234, January 2006 [available on www.ceps.eu]

— Bigo, Didier et al.: *The principle of information availability*. 1 March 2007 [available on www.libertysecurity.org]

— Brady, Hugo: *The EU and the fight against organised crime*. Centre for European Reform Working Paper, London, April 2007

— Brouwer, Evelien: *Data surveillance and border control in the EU: balancing efficiency and legal protection of third country nationals*. 14 June 2005 [available on www.libertysecurity.org]

— Bunyan, Tony: *The shape of things to come — EU Future Group*. September 2008 [available on www.statewatch.org]

— De Hert, Paul and Serge Gutwirth: *Interoperability of police databases within the EU: an accountable political choice?* TILT Law & Technology Working Paper No. 001/2006, 1 April 2006, Version 2.0 & Tilburg University Legal Studies Working Paper No. 003/2006

— Fijnaut, Cyrille and Letizia Paoli [eds.]: *Organised crime in Europe: Concepts, patterns and control policies in the European Union and beyond*. Dordrecht, 2004

— Geyer, Florian: *Taking stock: databases and systems of information exchange in the area of freedom, security and justice*. Challenge Research Paper No. 9, May 2008 [available on www.ceps.eu]

— Guild, Elspeth, Sergio Carrera and Thierry Balzacq: *The changing dynamics of security in an enlarged European Union*. Challenge Research Paper No. 12, October 2008 [available on www.ceps.eu]

— Hayes, Ben: *Schengen Information System Article 99 report: 33,541 people registered in SIS for surveillance and checks*. February 2008 [available on www.statewatch.org]

— Kierkegaard, Sylvia: "Explanatory Notes: From Prüm to the EU." Presentation at the International Conference *Computers, Privacy and Data Protection*, Brussels, 16–17 January 2009

— Nelles, Ursula: "Steps towards harmonisation — steps towards friction." In Kauko Aromaa and Sami Nevala (eds.): *Crime and crime control in an integrating Europe: Plenary presentations held at the Third Annual Conference of the European Society of Criminology, Helsinki 2003*. European Institute for Crime Prevention and Control Publication Series No. 44, Helsinki 2004

— Schot, Johan and Arie Rip: "The past and future of Constructive Technology Assessment". *Technological Forecasting and Social Change*, Vol. 54, 1996

7. Annex A

Status as of 18 December 2008

Treaty of Prüm (27 May 2005)

Status of ratification/entry into force

Signatory States		
	Deposit of the ratification document	Entry into force
AT	**21/06/06**	**01/11/06**
BE	**05/02/07**	**06/05/07**
DE	**25/08/06**	**23/11/06**
ES	**03/08/06**	**01/11/06**
FR	**02/10/07**	**31/12/07**
LU	**08/02/07**	**09/05/07**
NL	**20/02/08**	**20/05/08**

Accession States			
	Declaration of accession	Deposit of the ratification document	Entry into force
BG	02/02/07		
EL	05/01/07		
EE	**-**	**23/09/08**	**22/12/08**
FI	**21/06/06**	**19/03/07**	**17/06/07**
HU	**12/04/07**	**16/10/07**	**14/01/08**
IT	04/07/06		
PT	23/06/06		
RO	**23/01/07**	**03/12/08**	03/03/09
SE	18/01/07		
SK	28/03/07		
SI	**28/07/06**	**10/05/07**	**08/08/07**

Source: Auswärtiges Amt (Federal Foreign Office of Germany)
[Germany is the depositary of the treaty]