University of Twente
School of Management and Governance
Centre for European Studies
BSK-ES
19 June, 2009

An Imbalance between Security and Liberty?

An Analysis of Cross-Border Information Exchange and Data Protection in the Context of the EU's Third Pillar since 9/11

Presented by: Katharina Leinius
Hammer Str. 56
48153 Münster, Germany
Student No: s0214507

Thesis Supervisor: Dr. L. Marin
Co-Reader: Dr. A J.J. Meershoek

1. Introduction

The shock of the terrorist attacks on 11 September 2001 "served as a catalyst for changed and changing laws" (Maurer 2009:76) as nation-states rushed to respond to the threat posed by a transnationally operating terrorism[1], which was abruptly perceived as one of the central security threats in today's world.

Consequently, states are in the process of re-evaluating their security strategies, as now, "individuals, rather than states, pose the primary threat" (Baird & Barksdale 2006:51) to national security and the asymmetric, extremely flexible and globalized character of transnational terrorism makes the established approaches of the military and intelligence complex inadequate (see Weidenfeld 2004:15). Central to any response adapted to the new circumstances of providing security is a strategy of prevention (see Baird & Barksdale 2006:51), which relies on the detailed and timely gathering of intelligence. Considering the globalized character of transnational terrorism, an essential requirement for preventing new attacks is improved information sharing between states – as the analysis of the 9/11 attacks shows, "one of the key failures of pre-September 11 counterterrorism efforts" (Baird & Barksdale 2006:52). The intelligence and law-enforcement agencies of different states may all possess mosaic pieces illustrating the transnational operation of terrorist networks (see Baird & Barksdale 2006:58), which makes disseminating this information crucial for effective counterterrorism efforts. Consequently, giving intelligence and law-enforcement actors better access to information on individuals seems to be the intuitive response, as well as supporting initiatives to improve the gathering of information held on individuals by the state.

As especially in Europe, transnational terrorism is essentially treated as law-enforcement challenge (cf. Maurer 2009:96; Monar 2007b), counterterrorism policies mostly concern the expansion of executive powers to collect, process, and share personal information. This trend is especially apparent in the EU's counterterrorism

[1] There is no generally accepted definition of terrorism, but Ganor offers a commonly accepted approximation of a definition when he defines terrorism as "the deliberate use of violence against civilians in order to attain political, ideological, and religious aims." (Ganor 2001: 1f, cited in Kratochwil 2003:121). Other basic elements of a possible definition include the intention to intimidate a population, to influence a government or to destabilize a political system (see Wiegand 2008:7-16 for a more detailed discussion).

strategy, which emphasizes cross-border law enforcement cooperation (see Monar 2007b:268), a direction of security policy which can be attributed to the externalization of internal security due to globalization processes and the changes in the security landscape since the collapse of the USSR.

Though internal security remains a prerogative of the member states, the EU has become an important actor in directing and coordinating its members' counterterrorism efforts, with a number of action plans, strategies and framework decisions being adopted since 9/11. Central are initiatives aimed at improving the efficiency of law enforcement authorities at the national and the EU level by promoting increased information sharing and granting access to national databases for a number of actors.

However, setting enhanced access to personal data on top of the counterterrorism agenda may "evoke the Orwellian nightmare of a paternalistic, omnipotent government that observes its citizens' every move" (Northouse 2006:8). In modern liberal democracies, the powers of the state executive – including police and intelligence agencies – are limited by the principle of the rule of law, which has to balance the principles of security and liberty, safeguarding the citizens' rights and freedoms against the powers of the state. Giving the government extensive access to personal information has the very real potential of violating these civil liberties.

But how does the trend towards creating improved access to personal data affect the balance of security and liberty in the European Union? Is the extension of executive powers counterbalanced by a sufficient level of individual rights protection?

The information sharing regimes that are being developed under the EU third pillar are an intriguing example of the new EU internal security policy. With the very recent adoption of a Council framework decision on data protection in the Third Pillar, a critical analysis of the protection offered by the framework decision in comparison to the strengthening of executive powers through information sharing may lead to a substantiated assessment of the balance between liberty and security in this specific case and help show that all too often, civil liberties are undermined in order to achieve an illusion of improved security.

In the following, I will embed the EU counterterrorism activities since 9/11 into the changed security framework of the new millennium and show how the EU is inevitably becoming a central security actor by facilitating extensive security cooperation between the member states, in particular regarding operational police cooperation (chapter 2.1). Then, I will analyze the initiatives developing enhanced information

sharing between law enforcement authorities which constitute a major step towards a European area of security (chapter 2.2). In the main part of my thesis I will first illustrate how a system of checks and balances safeguards the balance between security and liberty in a liberal democracy (chapter 3.1 and chapter 3.2), and then examine whether the initiatives facilitating cross-border information sharing threaten this balance by analyzing whether they are subject to effective democratic and judicial control (chapter 3.3) and whether information sharing is sufficiently covered by data protection rules (chapter 3.4), in particular by scrutinizing the Data Protection Framework Decision of November 2008 (chapter 4).

2. The EU Counterterrorism Strategy: Creating a European Security Regime

Security policies are shaped in a way that promises to most effectively counter potential threats to and manage security risks for a state's territory and its citizens' safety. However, what is considered to be a potential security threat[2] in a society is very much a matter of perception, as the interactions between politics, media and the public sphere influence how threats are understood and what priority they are given by the public institutions managing security (see Bigo 2008:94); security policies consequently focus on the direction a threat is perceived to most likely come from, with public opinion and public fears exerting a considerable influence on the formation of policy, as politicians know of the significance of appearing to be responsive to citizens' security concerns.

Traditionally, security was understood to be divided into external threats from hostile powers, to be countered militarily, and internal threats against public order and the political system, which was a task for law enforcement authorities. Clearly, the changes of the international system in recent decades inevitably have changed the way security is conceptualized today. With the diminished threat of invasion by a

[2] Security can be defined very broadly or very narrowly; in the context of this thesis, the term security refers to the protection of a state's territory and populace from internal and external threats; the term threat refers, respectively, to a situation in which "there are actors that have the capabilities to harm the security of others and that are perceived by their potential targets to have the intention to do so" (Wallander & Keohane 1999:25).

hostile power since the end of the Cold War and the growing interconnectedness of the world due to the processes of globalization, the understanding of security is undergoing its most fundamental change since the rise of the nation-states in the 17th century (see Anderson & Apap 2002:4). The concepts of external and internal security have begun to blur together (see Maurer & Parkes 2005:7-11), with internal security increasingly seen to be in danger from threats such as transnational terrorism and organised crime, which are understood to have both an internal and external dimension.

Security policies are changing in response to this changed threat perception. In the European Union, this re-conceptualization of internal security is reflected in the concept of the 'area of freedom, security and justice' (AFSJ), which links all three of the EU's pillars, integrating justice and home affairs concerns into all fields of European decision-making (cf. Anderson & Apap 2002; Bendiek 2006). The AFSJ is the logical security response to the finalization of the Schengen area, which abolished internal borders between the member states and as such removed the traditional demarcation line between internal and external security. With the Treaty of Amsterdam, the member states have given the EU an explicit mandate to "provide citizens with a high level of security within an area of freedom, security and justice" (Article 29 TEU), thus legitimizing the active role the EU had begun to play in building a European security regime.

Though security policy was at least partially coordinated on the EU level since the establishment of the TREVI group[3] in the mid-1970s, cooperation in these matters remained strictly intergovernmental. This is beginning to change, with the communitarization of visa, asylum and immigration policy in the Treaty of Amsterdam being the first step and the extension of the Community method to all EU policy fields with the Treaty of Lisbon being the second step towards a Europeanization of security policy driven by the perceived Europeanization of threats.

The dynamics between the changing conceptualization of security threats, the responding security policies and the influence of actors' interests are central to understanding the way decision-making in security issues is being shifted to the European level. In the following, this approach will be used to examine the development of

[3] In the TREVI group, the Ministers of Justice and of the Interior of the member states met regularly, chaired by the rotating Council Presidency, in order to exchange ideas and best practices on fighting terrorism, later also organised crime, drug trafficking and illegal immigration.

cross-border information exchange in the European Union, which illustrate how the reprioritisation of terrorism as primary security threat has become the catalyst for fundamentally transforming the framework of transnational law enforcement cooperation (chapter 2.2), with the European arena allowing security actors more decisional autonomy due to the weakening of domestic constraints (chapter 2.3).

2.1 The EU Counter-Terrorism Strategy: Facilitating Law-Enforcement Cooperation

The security discourse taking place between politicians, security actors, the media and the public shapes the form security policy takes; consequently, cooperation between European governments in security matters depends on whether the threat is conceptualized and prioritized similarly in the different political and social arenas of the member states (cf. Mitsilegas et al. 2003:2-3). In the 1970s, attacks by the German RAF, the Italian Red Brigade and a number of other terrorist groups made the fight against terrorism a top priority for many of the member states of the European Community (see Andreas & Nadelmann 2006:100). The informal and clandestine TREVI framework of working groups and regular high-level contact of senior officials was initiated in order for member states to coordinate their respective counterterrorist policies, as there was evidence for a certain level of transnational operation of the domestic terrorist groups, making a regular exchange of information seem reasonable (see Andreas & Nadelmann 2006:100). However, in the 1980s and 1990s internal security cooperation on the European level turned to other security issues with cross-border character such as organised crime, drug trafficking and illegal immigration, in particular as the abolishment of internal borders raised concerns about an increase in transnational crime (Anderson et al. 1995:54-56). Increasingly, these diverse issues were treated as part of the same security threat, as a 'security continuum' that shifted formerly primarily social issues such as asylum policy into the field of internal security policy-making (see Maurer & Parkes 2005:3).

After the 11 September attacks, however, "terrorism made a dramatic comeback as the priority policing issue in Europe" (Andreas & Nadelmann 2006:211). Shortly after 9/11, the member states agreed on a common definition of terrorism[4], which was

[4] See Article 1(3) of the Council Common Position of 28 December 2001.

then recognized as one of the major threats for European security in the *European Security Strategy* of December 2003, and security co-operation with the USA[5] was intensified, an "unprecedented opening of EU structures towards a third country" (den Boer & Monar 2002:14). But still, terrorism was not considered to be an immediate and urgent security threat in all member states.

This changed after the terrorist attacks on 11 March 2004 in Madrid and on 7 July 2005 in London, which violently forced member states to recognize that terrorists increasingly recruited their operatives in radicalised groups located within the European Union, and that the danger posed by 'home-grown terrorists' made cooperation under a coherent European counterterrorism strategy necessary, as in the EU, "terrorists – but not policemen – can easily move across national frontiers" (Keohane 2005:7). Due to the congruence in threat definition and threat perception, EU legislative activity related to internal counterterrorism measures sped up remarkably (cf. Howorth 2006). Shortly after the Madrid attacks, the European Council adopted the *Declaration on Combating Terrorism* of 24 March 2004, which significantly revised the *2001 Action Plan on Terrorism*[6] and laid the groundwork for the *EU Counter-Terrorism Strategy*[7] which was adopted in December 2005. The *Action Plan* is the central document on EU counterterrorism policy, encompassing more than 200 concrete counterterrorism measures[8] which are organized under seven strategic objectives[9] and which fall under all three pillars of the European Union.

---

[5] This included three public agreements with the USA (Mutual Legal Assistance, PNR, Extradition) as well the clandestine access granted to US authorities, including the CIA, to confidential banking information held by the Belgian bank consortium SWIFT, see Wiegand 2008: 85-92; Guild & Brouwer 2006.

[6] Commission document SEC (2006) 686, Council document 10043/06.

[7] Council document 14469/4/05 REV 4.

[8] The Action Plan is regularly updated, with the latest version being from December 2006.

[9] The seven counterterrorism objectives are the following: 1. to reinforce international efforts to combat terrorism; 2. to reduce terrorists' access to financial and economic resources; 3. to increase the capacity of the European institutions and Member States to investigate and prosecute; 4. to protect the security of international transport and set up effective systems of border controls; 5. to strengthen the coordination between the Member States and thus the EU's capacity to prevent and deal with the consequences of a terrorist attack; 6. to identify the factors that contribute to the recruitment of terrorists; 7. to encourage third countries to engage more efficiently in combating terrorism. See http://ec.europa.eu/justice_home/fsj/terrorism/fsj_terrorism_intro_en.htm.

The cross-pillar character of the *Action Plan* illustrates that in the EU, security is no longer understood to be clearly divided into external and internal security; the fight against terrorism is to be fought in all dimensions of EU activity, from foreign policy (cooperation with the USA) to financial policy (initiatives against money laundering). However, a large number of counterterrorism measures fall under Objective 3 of the *Action Plan*, which is concerned with increasing the capacity of the European institutions and member states to investigate and prosecute terrorism and which measures fall under the Third Pillar. Of particular relevance for the developing EU security regime are the *Framework Decision on the European Arrest Warrant*[10], the *Framework Decision on combating terrorism*[11] and the initiatives developing information sharing, improving access of law enforcement actors to national and European databases and enhancing police capabilities[12] (see Council 2006a:19-28).

The development of internal security policy coordination on the European level consequently closely followed changes in the prioritisation of security threats after high profile events such as the attacks by domestic terrorist groups in the mid-1970s, the abolishment of internal borders with the completion of the Schengen area, and the terrorist attacks of New York, Madrid and London. EU security policy has tended to accelerate in reaction to the subsequent heightened threat perception and change in its focus with the re-prioritization of threats. After 9/11, terrorism returned as top priority issue, subsuming asylum and immigration issues under the counterterrorism rationale, and EU activity in internal security policy-making increased considerably, with a clear emphasis on facilitating cooperation between national as well as European law enforcement authorities, reflecting the externalisation of internal security in the single "criminal-geographic space" of the Schengen area (2008 Strategy Paper of the Association of European Police Colleges, cited in Hempel et al. 2009:2).

2.2 Conceptualizing Information Sharing: the Principle of Availability

[10] Council Framework Decision 2002/584/JHA.

[11] Council Framework Decision 2002/475/JHA.

[12] Cf. Council Framework Decision 2006/960/JHA ('Swedish Framework Decision'), Council Decision 2008/615/JHA ('Prüm Decision').

The fight against terrorism relies on information and intelligence[13] in order to prevent attacks - policy-makers speak of 'anticipative knowledge' (Hempel et al. 2009:1). Considering the transnational character of today's terrorism, law enforcement agencies in several countries could all possess a small piece of the puzzle, in which the most inconspicuous detail could be key in preventing a terrorist attack. Especially the mostly unrestricted movement of goods, persons, services and capital "makes life easy for crime, but most difficult for law enforcement (Hempel et al. 2009:1). One possible solution would be the creation of federal law enforcement comparable to the American FBI, thus meeting the federalized spatial area of Schengen with a similarly federalized justice. The ratification of the Europol Convention in 1998 was seen as first step in this direction, but member states' reluctance to grant Europol operational powers as well as the heterogeneity of criminal laws in Europe stifle the development of Europol to a truly supranational policing institution (see Andreas & Nadelmann 2006:186-188). Instead, EU policy-making in internal security matters focuses on improving the flow of information between the law enforcement authorities of the member states and between member states and Europol and Eurojust.

The Madrid bombings of March 2004 acted as a catalyst in regard to information sharing; in the *Council Declaration on combating terrorism* of 15 March 2004, the European Council called for developing legislative measures "simplifying the exchange of information and intelligence between law enforcement authorities of the Member States" (Council 2004a:5) and named improved exchange of information several times as concrete measure to further the EU strategic objectives in combating terrorism regarding terrorist financing (Objective 2), intelligence (Objective 3) and passenger information (Objective 4) (see Council 2004a:14-15). Thus put squarely on the agenda, the Commission[14] and the 2004 Dutch Council Presidency[15] subsequently

---

[13] While the term 'information' refers to hard data such as first and last names, DNA profiles, fingerprints, addresses etc., 'intelligence' "takes raw information and analyzes it", a task of the secret service and equivalent security actors (Walsh 2006:626). Intelligence sharing in the EU is facilitated by the Berne Group, Europol and the European Union Military Staff (cf. Walsh 2006); the BdL network (bureau de liaison) is also an additional system aimed at exchanging information on terrorist attacks between member states (cf Bigo 2000). The security landscape in the EU is indubitably complex and an analysis of all information exchange networks unfortunately outside of the scope of this thesis.

[14] COM(2004) 429 final.

[15] Cf. Council document 12680/04, cited in Bunyan 2006:3.

developed a concept that aimed at making information held by national law enforcement authorities mutually accessible: the 'principle of availability'.

On 5 November 2004, just eight months after the *Council Declaration on combating terrorism* and less than a month after the Council made the first draft public on 11 October, the concept of availability became an official policy of the European Union with the adoption of the Hague Programme[16], the Council's five-year plan for justice and home affairs.

The principle of availability is defined as the following:

> *"... 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 and (...) the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State."*
>
> (Council 2004b:27)

Already in the Hague Programme, the principle of availability is positioned as a concept extending to EU security cooperation in general, not only to an exchange of information on terrorism. This is in line with the underlying perception of the fight against terrorism demanding a multidimensional approach in which apparently innocuous information has to be accessible to law enforcement actors. The principle of availability can therefore be understood an expression of the key rationale of the security agenda after 9/11.

2.2.1 The Swedish Framework Decision: Indirect Access on Request

The first legislative initiative developing the principle of availability was the 2006 'Swedish Framework Decision'[17], which established a standardised procedure for the exchange of "any type of information or data which is held by law enforcement authorities" (Article 2(d)[i]) as well as any information or data "held by public authorities or by private entities and which is available to law enforcement authorities" (Article 2(d)[ii]). The Framework Decision facilitated information sharing by introducing standardized forms for information requests and by establishing time limits in which

[16] Presidency Conclusions, November 2004.

[17] 2006/960/JHA. The framework decision is named after its initiator, the Kingdom of Sweden, which proposed the framework decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union on 18 November 2004

requested information should be transmitted[18]. Most importantly, compliance with the information request of another member state became obligatory, subject to certain exceptions[19]. The procedure is applicable in a broad range of cases, not merely terrorism, and covers all kinds of data held by law enforcement authorities. According to Article 2(e), the procedure covers information requests linked to the offences covered by the European Arrest Warrant[20], which spans a wide range of criminal acts.

The Framework Decision made information held in national databases more accessible to other law enforcement authorities. However, the access being granted is not direct or automated, but dependent on the forms to be found in the annex of the Framework Decision; information exchange under the provisions of the Swedish Framework Decision is therefore indirect and on a case-by-case basis. Moreover, the Framework Decision explicitly excludes intelligence services[21] and makes it mandatory for member states to list the respective authorities authorised to exchange data under the system established by the Framework Decision.

This system of indirect access and case-specific requests does not completely abolish the autonomy of law enforcement authorities in deciding whether to transfer data, but nevertheless, the Swedish Framework Decision constitutes an important first step towards realizing the principle of availability as it considerably simplifies law enforcement access to information held by other member states.

---

[18] Time limits according to Article 4 of the framework decision: eight hours for urgent requests, one or two weeks respectively for non-urgent requests.

[19] Information requests can be refused on grounds of "essential national security interests", current criminal investigations or if it would be disproportionate or irrelevant regarding the purpose for which it was requested. (see Article 10 of the framework decision).

[20] The European Arrest Warrant and consequently also the Swedish Framework Decision is applicable concerning thirty-two serious offences. In the Framework Decision, terrorism is explicitly mentioned once, when stating that 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", a sentence in which the limiting effect of mentioning organised crime and terrorism is directly cancelled out by calling for a scope that is as wide as possible.

[21] "Agencies or units dealing especially with national security issues are not covered by the concept of competent law enforcement authority."(Article 2[a]).

2.2.2 The Prüm Decision: Introducing Automated Direct Access

The Council Decision 2008/615/JHA, known as the 'Prüm Decision', has a troubled history[22]: the decision integrates the substantial parts of an intergovernmental treaty concluded outside the EU framework into the Community acquis. Signed between Germany, France, Spain, Austria, and the three Benelux countries on 27 May 2006[23], the Treaty of Prüm intensified police co-operation between the participating states especially in regards to terrorism, cross-border crime and illegal migration by, inter alias, establishing "an advanced form of transnational information exchange" (Hempel et al. 2009:17).

Contrary to the Swedish Framework Decision, the Treaty of Prüm introduced a form of automated access to specific national databases[24] as well as making the creation of a national DNA database mandatory for the signatories. Contrary to the generalized approach advanced by the Swedish Framework Decision, the Prüm Convention addresses the exchange of only certain types of data, namely DNA profiles, fingerprints, vehicle registration data and personal data. The most innovative feature of the Prüm system is the two-step access procedure; the member state searching information has direct automated access to the aforementioned national databases[25] and can directly compare a DNA sample or a fingerprint of a suspect with the data held in the equivalent databases of the other member states, immediately getting either a hit or no hit, meaning that the suspect's data matched data held in the other member state. Once a hit is indicated by the system, however, the member state holding the information may refuse to supply additional information, such as the identity of the subject. The decision to hand over additional data is made on a case-to-case basis, and is regulated by the specific national legislation of the member state holding the information; the national authorities therefore enjoy a high level of autonomy. Still, the Prüm decision intensified operational cooperation to a considerable degree. Especially remarkable is

---

[22] Cf. Balzacq et al. 2006 for a critical analysis of the Prüm Convention. They criticise Prüm for undermining EU policy-making, dismantling trust between the member states and violating the EU principle of transparency by excluding the European Parliament and the European Court of Justice. (p.17-18).

[23] Entry into force on 1 November 2006.

[24] DNA databases, fingerprint databases and vehicle registration databases.

[25] The automated search and subsequent supply of additional information in case of a match of data is operated by `national contact points`, which act as intermediaries between the specific law enforcement authority handling the case and holding the information respectively.

Article 7, which obliges member states to provide legal assistance to another member state by collecting and transferring a suspect's DNA profile, subject to certain conditions, if that suspect is in their territory. The Prüm Decision also sets up a system of interconnected national contact points, thus simplifying information exchange by providing clear communication channels, while the Swedish Framework Decision only referred to "any existing channels for international law enforcement cooperation" (Art. 6 [1]). Regarding access restrictions, Prüm is criticised for failing to restrict which kind of security actors may request information. This has the danger of potentially making the participation of secret service actors in information exchange "a general rule and not an exception" (Balzacq et al. 2006:124), which threatens to undermine the legal wall between law enforcement and intelligence actors, which is constitutionally protected in Great Britain and Germany (see Soria 2006). In this, the Prüm Decision deviates from the clear access restrictions which can be found in all other European systems of information exchange[26].

With the Prüm Decision, the system of automated access to certain national databases was integrated into the EU legal framework and thus extended to all member states. Prüm intensifies operational cooperation between national security actors and facilitates information exchange by creating clear communication channels and the hit/no hit system, while at the same time prolonging the decisional autonomy of national security actors.

2.2.3 The Future Group Report: Strengthening Information Sharing

Neither the Swedish Framework Decision nor the Prüm Decision fully implemented the principle of availability, though this may change in the near future. The direction the EU security discourse is taking vis-à-vis the principle of availability is well illustrated in the Future Group Report 'Freedom, Security and Privacy – the area of European Home Affairs' (2008). The Future Group was an informal Council group set up in January 2007, consisting of the Interior Ministers of the outgoing and the incoming

[26] Europol, Eurojust, the Schengen Information System (SIS) and Eurodac all facilitate the exchange of certain types of information between different security actors, but they have rules which regulate access; see Soria 2006:16-18.

trio of Council Presidencies[27]; its task was the development of a proposal for the next five-year JHA strategy for 2009-2014, which will be adopted in December 2009, following the Tampere Programme (1999-2004) and the Hague Programme (2005-2009). Though it is the European Commission that will propose the 'Stockholm programme'[28], its proposal will most likely be heavily influenced by the Future Group Report, as the Report expresses an informal consensus of the two Council Presidency trios on the central issues in Justice and Home Affairs policy for the next five years (see Hayes 2008:5). The Future Group Report is very adamant in putting an increase in law enforcement cooperation on the basis of new technologies on top of the JHA agenda for the next five years, and argues that

"this is an opportune moment to go beyond the limited perspective of a case-by-case approach and aim for a holistic objective in law enforcement information management".

(Future Group 2008: 44).

Though fairly convoluted sounding, this statement has a clear message: the principle of availability should be further developed. In the current information sharing regimes established by the Swedish Framework Decision and the Prüm Decision, requests for information are granted on a case-by-case basis, with each request being individually considered (cf. Future Group 2008:44). This case-by-case approach is envisioned to be replaced by a 'holistic' approach in which law enforcement authorities on principle have access to certain types of data, without the necessity to make a case-specific request. As next step towards further implementing the principle of availability, the Future Group Report suggest the extension of the Prüm system of automated access to

[27] The first trio being Germany, Portugal, and Slovenia, and the second trio being France, the Czech Republic, and Sweden. Also participating were representatives (not the Interior Ministers) from Spain, Belgium and Hungary, which form the future trio of Council Presidencies, as well as the UK, the President of the European Parliament's LIBE Committee and a representative of the Council Secretariat as observers (see Hayes 2009:6).

[28] As Sweden will be holding the Council Presidency in December 2009, the Council will most probably meet in Stockholm for their Justice and Home Affairs meeting; the JHA programmes usually take their name from the location they were adopted at, as shown by the Tampere and the Hague Programme, with the new programme therefore very likely to be called 'Stockholm programme'.

additional categories of data (Future Group 2008:9), such as communications data, ballistics, data from civil registers, photographs and income information[29].

In the next five years, information exchange between law enforcement authorities will thus become even more intensive, insofar as the security agenda proposed by the Future Group can be understood as an informal consensus between key national actors in the Council. The emphasis on further implementation of the principle of availability implies an erosion of the autonomy of law enforcement authorities, with more and more data being made directly accessible without an *a priori* evaluation of the request by the authority holding the information.

2.2.4 The Principle of Availability: A Contentious Concept

Information sharing between law enforcement authorities, though seemingly a reasonable essential part of enhanced police cooperation, comes up against the lack of trust between national authorities as well as the widespread belief that information belongs to the authority who stores it (see Bigo 2008:105). The principle of availability intends to sideline these obstacles to information exchange by making data exchange obligatory, and by doing so, causes an unparalleled upheaval in the traditional organisation of law enforcement cooperation by introducing a mandatory aspect to a field strongly depending on the goodwill of the participating actors (see Bigo 2005:106). Security activity usually is characterized by a clandestine and insular thinking that makes cooperation even between different security actors of the same member state difficult; the principle of availability therefore is no less than revolutionary in its intention.

Balzacq et al. (2006) argue that the Prüm Treaty can be seen as a successful attempt of a few member states to sway the development of information-sharing away from the generalized access established by the Swedish Framework Decision. They claim that therefore, many provisions of Prüm undermine the underlying rationale of the principle of availability by ensuring that information remains the property of the state which collected it; consequently, under the Prüm system, other member states may have the right to request access to additional information after a hit is indicated, but

[29] The Council already has a list of 49 categories of data to which Prüm cold be extended, with the first three named above already having been subject of assessments regarding their suitability (see Hayes 2009:44-45).

the autonomy of national law enforcement authorities in deciding whether to hand over this information remains strong (see Balzacq et al. 2006:117).

As apparent in the policy recommendations of the report of the Future Group, there is no clear direction yet in which the principle of availability might develop in the near future; the report suggests the extension of the Prüm system to other types of data, but also envisions a 'holistic' approach which overcomes the case-by-case character of current information exchange systems and which protects the decisional autonomy of security actors up to a certain degree.

2.3 Member States and Security Policy: Playing the Two-Level Game

The EU's role in counterterrorism is subject to a characterizing paradox: though the transnational character of the new form of terrorism makes more cooperation and even transfer of powers to the EU level reasonable, member states are very unwilling to do so, as national security is one of the core issues of sovereignty (cf. Keohane 2005: 9). As member states are reluctant to transfer any operational powers or exclusive competencies related to counterterrorism objectives to the EU institutions, counterterrorism policy on the European level remains a strictly intergovernmental activity, with the member states maintaining their ultimate national sovereignty (see Monar 2007b:273). This principle is also recognized in Art. 33 TEU, whose provisions determine that "the exercise of the responsibilities incumbent on Member States with regard to the maintenance of law and order and the safeguarding of internal security" shall not be affected.[30]

Therefore, it is the member states acting in the Council of Ministers that are the undisputed legislators on counterterrorism policies under the Third Pillar, with decisions being implemented through national legislation. Characteristically, the major documents on counterterrorism[31] are all in form of legal instruments that are non-binding and leave compliance and implementation up to the member states. Monar argues that

[30] Though the institutional capacity of the relevant European agencies (Europol, Eurojust, office of the Anti-Terrorism Coordinator) were strengthened after 9/11 and their mandate expanded, they continue to lack operational capabilities of their own.

[31] Namely the Council Declaration on Combating Terrorism of 2004, the Counter-Terrorism Strategy of 2006 and the Action Plan to Combat Terrorism of 2006.

this choice of legal instruments is deliberate, showing that "the EU institutions have gone to great lengths to avoid any direct interference with human rights" (2007b:271). As fundamental rights are central for the construction of a common European identity as well as in legitimizing the EU (Art 6 TEU, Copenhagen Criteria etc), any legal instruments directly restricting fundamental rights in the name of counterterrorism would "break up the basic consensus on which the European construction rests" (Monar 2007b:271).

However, this does not mean that its intergovernmental character keeps EU counterterrorism measures from infringing civil rights: framework decisions are an obligatory agreement on the "results to be achieved" (Art 34(b) TEU), and Council Decisions are binding as well (Art 34(c) TEU). Consequently, the security policies agreed upon in the Council may lead to the implementation of national laws that are invasive in nature and may unnecessarily infringe civil liberties (cf. Monar 2007b: 280). As counterterrorism legislation tends to be controversial, often met with strong opposition in national parliaments and civil society, the partial shift of legislative activity to the EU level allows governments to justify controversial measures as the result of a European consensus, and thus to strengthen their position vis-à-vis their parliament. In this context, one can point to the question of national DNA databases, which might serve as an example of national ministers playing just such a two-level game. Not all member states have DNA databases, as the storage of biometric data by police authorities is a sensitive issue due to the implications for privacy and data protection; the Prüm Decision however made it a legal obligation for national governments to create a DNA database, and thus side-stepped any potential parliamentary and civil society protest, for instance in Portugal (see Bellanova 2008:214-215).

The theory of venue shopping[32] suggests that political actors, in this case interior ministers, seek out the policy venue which is most favourable for the realization of their preferences. Guiraudon argues in the context of asylum policy that in the European Union, national ministers have an interest in shifting certain issues to the European level in order to sideline domestic institutional constraints that hinder the realization of their agenda (Guiraudon 2000:261). In asylum policy, the beneficial effects of changing the venue of policy-making were the avoidance of domestic judicial constraints, the exclusion of possible adversaries such as civil society organisations and

[32] The theory of venue shopping was developed by F. Baumgartner and B. Jones (1993) in the context of US politics, and applied to EU asylum policy by V. Guiraudon (2000).

the domestic legislature as well as the possibility of finding new allies. An in-depth application of the venue-shopping theory to the internal security context is beyond the scope of this thesis, but certainly, decision-making regarding security policy is less constrained by veto players in the EU Council than in the domestic venue of the member states. The secrecy of Council sessions disfavours transparency and shuts out civil society organisations and the media, the legislative procedure used in the Third Pillar marginalizes the European Parliament and the European Court of Justice (see chapter 3.3) and domestic parliaments only play a weak role in EU policy-making. Considering these institutional factors, it might be argued that it is in the interest of national ministers to shift such a contentious policy field as internal security to the EU Third Pillar, which offers fewer institutional constraints and also strengthens the bargaining position of the participating actors vis-à-vis other domestic actors, allowing them to play the two-level game.

3. The Conceptual Framework of Data Protection

Due the technological developments of recent years, an exponential amount of personal data is being generated, from telecommunications data to electronic trails caused for example by using credit cards as well as the increased use of biometric data (fingerprints, facial scans, iris scans, DNA profiles) unquestionably identifying individuals. This wealth of information on individuals is a very valuable for law enforcement purposes, and central for gaining the anticipative knowledge forming the core of counterterrorism activities.

Moreover, the rapid development of electronic storage capacities and online access technologies makes the sharing of information potentially instantaneous and virtually free of transportation costs by eliminating the significance of geographical distance. From a technological perspective, information sharing between law enforcement authorities is a matter of guaranteeing the interoperability of national and EU databases and then making data available by creating secure linkages between the different databases.

However, "technological developments are not inevitable or neutral" (De Hert & Gutwirth 2006:3). The development of interoperability and access to national databases is not merely a technological question to be solved by IT experts, but instead

has social and political implications. Since the Hague Programme of 2005, a transnational network of interconnected databases, national and European, is in the process of being built, with the purpose of improving the flow of information between law enforcement authorities. The information sharing network established by the legislation developing the principle of availability is only one security regime of many: SIS[33], CIS[34], EURODAC[35] and the planned VIS[36], ECRIS[37] and SIS II[38] are all European databases which also facilitate data sharing between different levels and types of security actors, all subject to their own data protection rules and access limitations. Without doubt, the European Union has become exceedingly active in building security systems, and this trend is apparently significantly accelerating, considering the policy suggestions of the Future Group Report (2008) and the number of planned European databases. This intensification of information sharing in the EU is a serious cause for concern. Personal data is of a very sensitive nature, relaying vital information about an individual. The capabilities of modern information technology and the plethora of digitalized information collected by private and public bodies make it possible to bring together apparently insignificant information from a multitude of sources to create a comprehensive profile of an individual, enabling practices such as profiling and data mining, by which the private life of an individual may come under close scrutiny by law enforcement simply due to their ethnic origin or acquaintance to a person suspected of crime. The processing of personal data by law enforcement au-

---

[33] SIS: Schengen Information System, current version SIS I+, operational since 1995; purpose of SIS is border security by allowing automated access to alerts on persons and objects for border and customs checks. Information entered into SIS (inter alias): stolen cars, passports, firearms, persons wanted for arrest or extradition, third country nationals who are not allowed to enter the Schengen area and missing persons.

[34] CIS: Customs Information System, operational since 2003; purpose is customs control by sharing information on breaches of customs regulations.

[35] EURODAC: registration of asylum seekers' and illegal immigrants' fingerprints; operational since 2003.

[36] VIS: Visa Information System, to be operational in 2012; VIS would store (biometric) information identifying third country nationals who hold EU visa. Purpose is border security, especially limitation of illegal immigration.

[37] ECRIS: European criminal records information system, aimed at standardizing the exchange of criminal records; in development.

[38] SIS II: not yet operational, should replace SIS I+; major changes: extended number of authorised users, content extended to include fingerprints and photographs of persons on whom there is an alert.

thorities inevitable infringes on civil liberties, but in the national context, this is counterbalanced by checks on executive powers such as data protection laws and public oversight. However, with the considerable increase of cross-border information exchange, the data protection framework has to be adapted to the new circumstances of data processing in order to guarantee that the protective mechanisms developed in the liberal democratic tradition also cover transnational data exchange and data processing by supranational bodies.

3.1 Liberal Democracy: Balancing Liberty and Security

The political system of liberal democracy answers the essential question of how to simultaneously provide citizens with security *and* freedom by establishing a complex constitutional order that gives the state the mandate to maintain public order, but also restricts the government's powers by institutionalizing constitutional checks and balances in order to ensure the greatest possible individual liberty. According to the principal liberal theorists Thomas Hobbes and John Locke, individuals which are organised in form of a society consent to give the state authority over them in order to create a central authority that maintains public order, guaranteeing "life, liberty and estate" (Locke, *Two Treatises of Government*, p.395, cited in Held 2006:63) in a world marked by insecurity due to competing individual interests and external aggressors. However, entrusting the central authority – Hobbes' *Leviathan* – with public power carries the danger of creating a tyranny, as "every man invested with power is apt to abuse it" (Montesquieu, *The Spirit of Laws*, p.69, cited in Held 2006:67). John Locke and Baron de Montesquieu emphasized in their writings that the conditionality of government is therefore crucial in order to protect the individual from arbitrary rule: the ultimate sovereignty must remain with the people, who rule via a representative body with lawmaking power that controls the executive government. Public power needs to be divided between different institutions, with the executive being democratically accountable, and its exercise legally circumscribed, while guaranteeing strong rights of the individual against the state, i.e. negative freedoms[39] (cf. Held

[39] This refers to freedoms such as freedom of thought, conscience and religion, freedom of expression and information and freedom of assembly and association (cf. Art. 6-19 Charter of Fundamental Rights of the EU).

2006:64; Puntscher Riekmann 2008:19) that are protected by an independent judiciary (cf. Held 2006:68).

The liberal democratic tradition thus constructs a political system which balances the demands of security and liberty. The executive holds "the monopoly on the legitimate use of force" (Weber 1948:78, cited in Anderson 1995:89) but is also constrained by the constitutional order. In a nation-state shaped by liberal democratic values, the police and similar law enforcement authorities have the powers to lawfully interfere with civil liberties in order to fulfil the government's mandate to provide internal security and enforce the law. Following Montesquieu's understanding of human nature, their position of authority needs to be strictly regulated by law and controlled by public oversight in order to prevent arbitrary actions.

From this perspective, data protection laws and mechanisms are a manifestation of the checks and balances so inherent to the liberal democratic system. The police necessarily infringe individual civil liberties when collecting and transferring data such as fingerprints, DNA samples or any kind of personal information, as this constitutes an interference with the right to privacy and family life, which is a core civil right, as well as an interference with the right to protection of personal data, which is derived from the right to privacy and which is explicitly recognized for instance in the Charter of Fundamental Rights of the European Union and in the constitutions of several member states[40].

On the national level, this civil rights infringement is safeguarded by robust data protection laws, whose observance is controlled by national parliaments and independent data protection authorities, and whose enforcement is the task of national courts. This status quo of data protection is challenged by the ongoing Europeanization of law enforcement (cf. Mitsilegas et al. 2003:164). Increasing volumes of personal data cross the borders between member states, while national parliaments and judiciaries are bound to their respective territory. Therefore, it appears vital that the strengthening of national law enforcement authorities through European anti-terrorism legislation is accompanied by a simultaneous strengthening of fundamental rights and civil liberties on the EU level in order to protect the liberal democratic balance between security and liberty (cf. Mitsilegas et al 2003:164).

[40] Member states in which data protection is a constitutionally protected right include Germany, the Netherlands, Austria, Portugal and Sweden (see Sule 1999:55-71).

3.2 The National Data Protection Framework in Europe

In the national context, the processing of personal data by public authorities is subject to the general institutional mechanisms constraining the executive as well as to more specific safeguards in the form of data protection laws and independent supervisory bodies.

The more general safeguards concern judicial and democratic control. Individuals have the right to seek redress against unlawful processing of their personal data before the national courts, invoking data protection laws which were adopted by the national parliaments. New legislative initiatives which affect data protection are subjected to parliamentary debate and scrutiny, with NGOs, lobby groups and the media aggregating opinions and driving the public discourse. The judiciary also has the right to review laws and repeal them in case of undue infringement of individual rights and existing data protection laws.

The most significant constraint is derived from the principle of the rule of law; the executive has to adhere to the specific data protection laws that define which actions related to the processing of data are lawful and which are penalized. These data protection laws distinguish between data processing done by private actors and by public bodies, with the later being subject to more rigorous provisions.

National data protection laws differ in their specific arrangements, and one can identify two different approaches to data protection. In most states, data protection is in the Anglo-American tradition seen as the protection of an individual's private sphere against infringement by either the state or private parties, with different kind of information being protected more or less intensively, depending on their significance for individual privacy. In Germany, data protection is approached differently, as an individual's right to decide which data to make public (right to informational self-determination). As a consequence, German data protection laws emphasize individual rights and strictly restrict data collection and processing in general, while most other European data protection laws focus on certain kinds of data which are especially protected (cf. Sule 1999:49-50).

Despite these two different rationalizations, national data protections laws in Europe share a common minimum standard that can be explained by the influence supranational agreements had on the development of data protection (see Sule 1999:71). The legal protection of personal data is a relatively recent phenomenon that has its origins

in the United States, not least because data protection is closely linked to the emergence of computerized processing of information which started in the USA (see Sule 1999:46). In Europe, it was the Council of Europe (CoE) that took the leading role in recognising the necessity of improving the protection of personal data. In 1981, the member states of the CoE adopted the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, known as 'Convention 108'. The Convention made it mandatory for the signatories to develop a national body of law that guaranteed the protection of the principles enshrined in Convention 108, which consequently had the effect that despite all the differences in the specific modalities, national data protection laws at their core reflect the principles established by Convention 108, which thus forms a common denominator of data protection in Europe (Sule 1999:71).

The general principles of data protection expressed by Convention 108 promulgate that personal data should only be used for the purpose for which it was collected and not retained for longer than absolutely necessary[41]; data processing should be done fairly and lawfully; data collection has to be necessary for the concrete purpose; individuals should be informed about the data held on them, when the data is passed on to third parties and the individual should have possibilities of redress to get the collected data corrected or deleted. Also, sensitive data such as the political, religious and sexual orientation, race and health of a person have to be particularly protected, by either a general prohibition on their collection or specific legal provisions. Regarding data transfers across borders, Convention 108 sets out that data may only be transferred on the condition that the protection in the receiving country has to be equivalent to the protection in the originating country (Art. 12(3)[a]), a formulation that is rather vague and is interpreted differently by the national data protection laws, with some on principle allowing data transfers (e.g. France) and others prohibiting transfers if there is reason to suspect that the data protection standards of the receiving country are lower than in the originating country (e.g. Germany) and making any transfer dependent on judicial authorisation (e.g. Austria) if there are doubts regarding the equivalence of protection (see Sule 1999:59-59, 66). The adherence of all public bodies processing personal data to the data protection laws is monitored by a system of independent supervisory authorities, which play an especially important role in guaranteeing public oversight in the characteristically intransparent area of internal security in law en-

[41] Principle of purpose limitation.

forcement actors operate. These data protection monitoring bodies usually have the right to access the information held on individuals, have the power to give instructions and recommendations to actors which are processing personal data and can investigate individual complaints of misuse of data. In some countries, these bodies are bound to regularly report to parliament (e.g. in Denmark, Germany and the UK, see Sule 1999:72) and have to approve the establishment of new public databases (e.g. Sweden, see Sule 1999:67).

On the national level, the processing of personal data is thus subject to numerous safeguards, from general judicial and democratic control to the specific protections of the data protection provisions of national law and of public oversight by independent monitoring bodies.

3.3 The Question of Institutional Checks and Balances in the Third Pillar

In the European nation-states shaped by the liberal constitutionalist tradition, the political and social freedoms of individual citizens are safeguarded from undue interference by the public authorities by a differentiated system of safeguards which also covers the processing of personal data by making it subject to judicial and democratic control, public oversight by independent authorities and extensive data protection laws. In recent years, however, internal security issues have begun to shift to the EU level, where national parliamentary scrutiny is much less effective and national courts do not have the jurisdiction to review the legality of executive decision-making. Therefore, it is necessary to first take a closer look at the institutional checks and balances on the European level in order to evaluate whether the shift of security policies to the transnational level is counterbalanced by sufficient constraints on the powers of the executive. In a second step, the specific safeguards for the processing of personal data on the European level will be analyzed (chapter 3.4).

Though built on liberal democratic values (cf. Art 6 TEU), the EU is not a liberal constitutional order comparable to a nation-state[42], particularly as most commentators

[42] There is, however, no consensus on what exactly the EU is. Certainly, the EU's institutional configuration is neither that of a nation-state nor that of an intergovernmental organisation. The argument of the EU being a system *sui generis* has become almost a proverb in European Studies, see inter alias Woyke 1998:113 and Kohler-Koch & Eising 1999: 3.

diagnose that the EU suffers from a clear democratic deficit[43]. The academic discourse on the democratic deficit almost exclusively focuses on the Community pillar, most probably as legislative activity in the intergovernmental Third Pillar[44] was for a long time very technical and negligible in its impact; moreover, the controversial issues of visa, asylum and immigration policy were communitarized with the Treaty of Amsterdam and thus fall under the Community pillar. With the increasing momentum on internal security legislation since 9/11, the legal framework of the Third Pillar is however increasingly coming under criticism (cf. Monar 2007a:311-313).

Legislative acts adopted under Title VI TEU are subject to the consultation procedure according to Article 39(1) TEU, which marginalizes the European Parliament to a purely consultative role; the Parliament's opinion is neither binding to the Council nor has it to be taken into account. This constitutes a clear deficit in terms of democratic accountability.

Judicial control is impaired as well: the European Court of Justice only has the powers granted to it at the member states' discretion. According to Article 35(2) TEU, member states can accept the Court's jurisdiction to give preliminary rulings on the validity and interpretation of Third Pillar legislation[45] as well as of the measures implementing them (Art. 35 (1) TEU) and they have to specify whether any national court of tribunal[46] or only national courts and tribunals against there is no judicial remedy[47] may use the preliminary reference procedure. As so far only seventeen member states have officially granted the ECJ jurisdiction over conferrals, and their position differs on which specific courts may refer cases, this leads to an incoherent

[43] See Hix 2008 for a summary of the academic debate, and Majone 1998, Moravscik 2002, Scharpf 1997, Höreth 1999, Follesdal & Hix 2006, Weiler 1995 and Lord & Beetham 2001 for the main positions in the debate.

[44] The second pillar, Common Foreign and Security Policy, also falls in this category.

[45] Framework decisions, decisions and conventions (Art. 34 (2) TEU). Common positions are excluded as they are simply statements of common strategy devoid of any binding character. In 2003, the Court gave its first judgment under Title VI TEU with Gözütok and Brügge (Judgement of 11 February 2003, Case 187/01, ECR (2003) I-5689).

[46] Under Article 35 (3) [b].

[47] Under Article 35 (3) [a].

legal situation that hinders effective judicial control over Third Pillar matters[48]. Most importantly, the ECJ has no jurisdiction regarding national law enforcement operations which have the purpose to maintain law and order and safeguard internal security according to Article 35(5) TEU and thus cannot review the validity and proportionality of cross-border police activities.

As counterterrorism measures as for instance information sharing may be very invasive and infringe on civil liberties and human rights to a considerable degree, the impaired democratic and judicial control in EU Third Pillar decision-making "casts a shadow over the legitimacy of EU measures" (Monar 2007b:281). The exceptionality and unpredictability of the terrorist threat tends to justify unnecessarily invasive security measures, overriding human rights concerns (cf. International Commission of Jurists 2009:18); the fact that the power of EU executive law-making in security issues is not sufficiently restricted by effective democratic and judicial control threatens the protection of civil liberties.

3.4 The Data Protection Framework at the European Level

On the national level, the processing of personal data by public bodies is subject to the specific safeguards of extensive data protection laws and public oversight by independent monitoring bodies. On the European level, data protection is of a much more fragmented nature, with the pillar division and the number of Third Pillar information systems, agencies and other bodies with their own respective data protection rules clearly rendering the data protection regime incoherent and even incomprehensible at times.

Very significant for data protection is the role of independent supervisory bodies, of which there a multitude due to the fragmented landscape of European data protection. In the Community pillar, the Article 29 Working Party[49] is the main actor regarding

[48] UK, Ireland and Denmark have not granted the ECJ jurisdiction; for Bulgaria, Cyprus, Estonia, Malta, Poland, Romania and Slovakia, there is no official information available according to the Research and Documentation Service of the ECJ (cf. ECJ 2008)

[49] Properly named Working party on the Protection of Individuals with regard to the Processing of Personal Data, established by Article 29 of the 1995 data Protection Directive (Directive 95/46/EC) and formed by national supervisory authorities, the Commission and Community supranational authorities such as the European data Protection Supervisor.

issues of data protection, while the European Data Protection Supervisor (EDPS) has the mandate to monitor data protection in all three EU pillars. Both have advisory as well as controlling functions, with the views of the Article 29 WP important in particular regarding data transfers to third countries, as it assesses whether the level of data protection in the receiving country is adequate and thus may be lawfully transferred (see Gonzalez Fuster & Paepe 2008:132). In the Third Pillar, the fragmentation of data protection rules is apparent in the number of actors, with separate Joint Supervisory Authorities responsible for every actors operating in the pillar and no coordination between them, a situation that is criticised as harmful for effective data protection (see Gonzalez Fuster & Paepe 2008:133).

Similar to the independent supervisory bodies, the data protection laws on the European level are also affected by the pillar division and the fragmentation of the Third Pillar. In the First Pillar, the 1995 EC Data Protection Directive provides a harmonized legislative framework that is, like national data protection laws, inspired by CoE Convention 108. However, while the police were also effectively exempted from the CoE Convention[50] (see Hayes 2005:33), the EC Directive goes one step further by explicitly excluding all "processing operations concerning public security, defense, State security (…) and the activities of the State in areas of criminal law" as well as not covering any activities "which fall outside the scope of Community law" [51]. Therefore, the Directive only applies to First Pillar matters[52].

In the Third Pillar, different rules apply depending on the context the data is being processed in. When data is transferred to European bodies such as Europol and Eurojust or when it is submitted to European information systems such as SIS, CIS and

---

[50] Convention 108 has a derogation clause for "protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences" (Art. 9(2)[a]).

[51] The practical effect of the pillar division is illustrated by one interesting example: a EU customs officer opening a suspicious box operates under different data protection laws depending whether the box, once opened, contains vegetables or weapons, as data entered into the CIS under first pillar rules is subject to different legal provisions than data entered under third pillar rules (see Lang 2008:268).

[52] As the ECJ judgement on the PNR Agreement with the USA recognizes (Joined Cases C-317/04 and C-138/04, 30 May 2006), this constitutes a legal loophole. Personal data, in the PNR case passenger information, can be collected in the context of commercial activities falling under the first pillar, but then accessed by national law enforcement authorities for public security reasons; while the collection of data is covered by the 1995 Directive, the further use for security purposes is not (cf. Kosta et al. 2007:3).

EURODAC, their respective data protection provisions apply. Concerning data that is exchanged between the member states, Prüm and the Swedish Framework Decision explicitly regulate which national laws apply to the transferred information[53], a system that is so complex to be nearly incomprehensible. Both the Swedish Framework Decision and the Prüm Decision also contain provisions on data protection. While they do not have direct effect[54], the duty of consistent interpretation developed by the ECJ case law states that national courts are required to interpret national law, and in particular legislation implementing EU directives, in light of the wording and the purpose of Community law. With the Pupino judgement in 2005 (C-106/03) this duty of consistent interpretation was applied to Third Pillar framework decisions[55]. Also, general human rights principles offer a certain degree of protection for individuals. The ECHR and therefore Article 8 on the right to privacy forms part of the EU legal order[56], and the Charter of Fundamental Rights of the European Union[57] even explicitly recognizes data protection in Article 8, which gives everyone the right to the protection of personal data (Article 8(1)) and reflects CoE Convention 108 and the 1995 Directive data in laying down the principles of purpose limitation and right of access[58] as well as independent oversight (Article 8(3)). In principle, these fundamental

---

[53] Under the Swedish framework decision, transmitted data is subject to the rules of the receiving member state (cf. Art. 8[2]), while the Prüm Decision regulates that transmitted data is protected according to the specific provisions of the Decision (Chapter 6) and the data protection regime of the supplying member state respectively, if there is no specific Prüm provision (cf. e.g. Art 28(3) [b] Prüm Decision).

[54] Meaning that framework decisions and decisions do not directly confer rights on individuals, see Article 34[b] and Article 34[c] TEU.

[55] The indirect effect of directives and framework decisions is based on Article 10 TEC, known as the loyalty clause; the principle gives individuals the possibility to seek redress for rights infringed by a member state failing to implement or wrongly implementing a directive (*Francovich* ,C-6 and 9/90; *Brasserie/Factortame,* C-46 and C-48/93) or a framework decision (Pupino judgement, C-106/03).

[56] The case law of the European Court of Justice shows that the ECHR has a special status as a source of law for the European legal order (see Chalmers & Tomkins 2007:237, 260).

[57] 2000/C 364/01. The Charter is not yet legally binding, but is consistently referred to by the ECJ (see Chalmers & Tomkins 2007:248-251).

[58] Data must be processed "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." (Art. 8(2)).

rights enshrined in the ECHR and the Charter bind member states when they act in the context of Community law (cf. Chalmers & Tomkins 2007:263-270).

However, all the data protection regimes situated on the European level have one serious weakness: the European Court of Justice does not have the jurisdiction to review actions taken by the member states when maintaining public order, according to Article 35(5) TEU. Consequently, the enforcement of data protection rules solely is the task of national courts, which leads to an uncertain legal situation, as there is no uniformity of interpretation of European data protection law. An individual might be able to seek redress before a national court, with the court bound to interpret the national implementing laws in the light of the data protection provisions of the Swedish Framework Decision and the Prüm Decision and the general principles of Community law, namely fundamental rights as expressed by the ECHR and the Charter. This however does not replace a coherent and substantive data protection framework with effective judicial control as it exists on the national level. The fragmentation of data protection regimes at the European level consequently harms the civil rights of the individual.

There is also an additional, similarly problematic effect of this incoherent framework of data protection. When exchanging information, law enforcement authorities face a particularly differentiated legal situation, in which it is consistently unclear which rules on data protection apply to the case at hand. This lack of legal certainty undermines the effectiveness of information exchange (McGinley & Parkes 2007:13). The practice of case-by-case authorisation of data exchange as used in the Prüm system implies that the data protection situation in the specific case is checked a priori (before the transfer) by the involved security officials. Coupled with their discretionary powers to refuse a request for information, security officials may exploit the argument of insufficient data protection and refuse requests for information in order to maintain their informational advantage over other security actors. For individual security officials, the transfer of data to other law enforcement bodies may not be in their own interests: "by sharing information, they lose clout" (McGinley & Parkes 2007:13). Therefore, the lack of legal certainty which characterizes data transfers between law enforcement authorities due to the confusing number of different data protection rules is a serious problem not only for individual rights protection but also for the effectiveness of information exchange.

4. Data Protection in the Third Pillar: Analysing the Data Protection Framework Decision

Aware of the negative effects of the incoherent data protection regime in the Third Pillar for both individual rights protection and the effectiveness of law enforcement cooperation, the Commission proposed a draft *Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Co-operation in Criminal Matters*[59] that is supposed to provide a coherent data protection framework for the Third Pillar and that was intended to be discussed simultaneously to the initiatives implementing the availability principle. The framework decision went through several revisions, with it being considerably altered by the German Presidency in early 2007. Curiously, the draft was prepared not by the Council Working Party on Data Protection, as may be expected, but by the Multidisciplinary Group on Organised Crime, which is composed of representatives of national law enforcement agencies and Interior Ministries (cf. Bunyan 2009:50) and who might presumably have a greater personal interest in improving the effectiveness of information sharing than in improving the protection of individual rights.

The framework decision has been seriously criticised by the European Parliament, the European Data Protection Authorities[60], national parliaments and civil society organisations for not offering an adequate level of data protection. As Tony Bunyan, director of *Statewatch* bluntly puts it: "Everyone but the Council is opposed to its content" (Bunyan, 2009:51). The European Parliament extensively amended the Council draft three times, in September 2006, in June 2007 and in September 2008. However, on 27 November 2008, the Council adopted the Data Protection Framework Decision[61] (DPFD) without taking the changes proposed by the European Parliament resolutions into account.

International agreements such as the Council of Europe Convention 108 and the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal*

---

[59] COM (2005) 475.

[60] On the EU level, the national Data Protection Commissioners are organized as the `Article 29 Working Party`, which also consists of one representative of the European Commission and of the European Data Protection Supervisor (named after Art 29 of the 1995 Directive on data protection). The Working Party gives (non-binding) advice to the European Commission on data protection issues.

[61] 2008/977/JHA.

Data have developed data protection standards for transnational data processing and information sharing, and the 1995 Directive reflected these core principles. Does the DPFD take into account data protection principles such as purpose limitation, data quality, independent oversight, strong rights to individuals, and does it have sufficient scope to provide a high level of protection? Admittedly, law enforcement activity is subject to derogations[62], but nevertheless, as the OECD Guidelines say, "exceptions to the Principles […] should be as few as possible" (§4 [a]).

4.1 Purpose Limitation

The 1995 Directive, the CoE Convention 108 as well as the OECD *Guidelines* all emphasize the principle of purpose limitation: personal data may only be stored for specific and legitimate purposes and not used in a way incompatible with those purposes[63]. Applied to information exchange, this means that transmitted data may not be used for any other purpose than the one for which it was originally requested. Article 3(2)[a] of the DPFD, however, allows further processing of transmitted data for another purpose, as long as the new purpose "is not incompatible with the purposes for which the data were collected". This wording is "vague" (McGinley & Parkes 2009: 16) and "far too broad" (EDPS 2007, part 22). Article 11 of the DPFD then lists a number of purposes for which derogations from the purpose limitation principle are allowed; the wording again is very vague, referring to "the prevention, investigation, detection or prosecution of criminal offences" (Art. 11[a]), "other judicial and administrative proceedings" directly related to the former (Art. 11[b]) and the "prevention of an immediate and serious threat to public security" (Art. 11[c]). Article 11[d] allows further processing "for any other purpose", under the condition of the transmitting authority giving its consent. Peter Hustinx, the European Data Protection Supervisor, points out that the "consent of the transmitting authority cannot be considered under any circumstances as replacing the consent of the data subject or providing le-

[62] Cf. §4 of the OECD Guidelines, Art. 9 §2 of the COE Convention 108.

[63] CoE Convention 108, Article 5(b); similiar to the purpose specification principle of the OECD Guidelines and Article 6(1)[b] of the 1995 Directive, which states: … *personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*, a formulation that was part of the original Commission proposal (Article 4(1)[b]) and then eliminated from the adopted framework decision.

gal grounds to derogate from the purpose limitation principle" (EDPS 2007, part 23). In his Third Opinion, Hustinx concludes that the framework decision in its parts on further data processing "does not fulfil the basic requirements of adequate data protection and even contradicts the basic principles of Convention 108" (EDPS 2007, part 23).

4.2 Principles Ensuring the Quality of Data

While the Commission proposal of 2005 explicitly distinguished between different categories of data subjects as well as between different types of data, these provisions are not part of the final version of the framework decision. The obligation to distinguish between the personal data of convicted criminals, suspects, witnesses, victims and associates of suspects was laid out in Article 4(3) of the Commission proposal; the failure of the adopted framework decision to follow the Commission draft in this aspect harms the rights of individuals who are neither criminals nor suspects and whose data nevertheless may be transmitted to other law enforcement authorities without special safeguards. Also, the DPFD does not differentiate between serious crime and any crime, however minor.

Similarly, Article 4(1)[d] of the Commission draft committed member states to make a clear distinction between data based on facts and data based on opinions and personal assessments. Differentiating hard data such as information on convictions from information based on speculation (intelligence) is very significant for the reliability and accuracy of transmitted data, and by it not being included in the framework decision, the receiving member state may have difficulties in assessing the reliability of the data it received, which may harm ongoing investigations, the work of courts and negatively influence trust between law enforcement authorities (cf. EDPS 2007, part 32) as well as violating the rights of the concerned individuals. Moreover, the need for accuracy of data used by law enforcement authorities is not sufficiently taken into account: there is no provision that would make periodic verification of the accuracy of data obligatory, merely making member states responsible for assuring that data are reasonable accurate prior to transmission (Article 8(1)). The European Data Protection Supervisor criticises the lack of provisions that would ensure „that police files are purged of superfluous or inaccurate data and kept up to date" (EDPS 2007, part 32), and comes to the conclusion that "the provisions relating to data quality of the

current proposal are neither appropriate nor complete" and that "they even fall below the level of protection required by Convention 108". As far as the quality of transmitted data is concerned, the DPFD adopted by the Council merely states that "As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability" (Article 8(1)); however, the FD fails to specify common categories of how to indicate the degree of reliability or accuracy, which may lead to considerable miscommunications due to the different law enforcement practices and cultures in the EU.

4.3 Rights of the Individual

Data protection laws do not merely protect an individual's private sphere from undue infringement by the state and other parties; data protection can also be understood as broadly analogous to the concept of information privacy, which Westin (1967)[64] in a commonly accepted definition describes as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (14), an approach to data protection that is emphasized as `right to informational self-determination` for instance in the German data protection regime. Following this approach, data protection legislation should enable the individuals to ascertain if information is held on them as well as for what purpose data is being held, and giving them the right to know what data is held on them, when that data is being transmitted, to whom it is being transmitted, and to get wrong information deleted and inaccurate information corrected[65] (often summarized as 'right of access'). Moreover, an individual should have the right to seek redress for misuse of personal data[66]. The right of the data subject to be informed is subject to exceptions as far as law enforcement activities are concerned, in order to protect "State security, public safety, the monetary interests of the State or the suppression of criminal of-

[64] Westin, A.F. (1967) `Privacy and Freedom`. New York. p.7, cited in Bennett 1992:14.

[65] Cf. Article 8 of CoE Convention 108; Article 12 and Article 14 of the 1995 EC Directive; §13 of the OECD Guidelines (Individual Participation Principle).

[66] Cf. Article 8[d] of Convention 108; Article 22 of the 1995 EC Directive.

fences" (Convention 108, Art. 9(2)[a]). However, security concerns cannot completely negate the subject's right to information privacy.

Individual rights in the context of data sharing should allow data subjects to access and if necessary challenge the data held by law enforcement on themselves, subject to certain exceptions safeguarding essential security interests. Article 16 (Information for the data subject), Article 17 (Right of access) and Article 18 (Right to rectification, erasure or blocking) address these principles; however, the relevant provisions are very vague in their wording and therefore open to misinterpretation. The right of access is severely restricted, allowing only for the data subject to receive confirmation that data has been transmitted and to whom (Art 17(1)[a]) or to receive confirmation that "all necessary verifications have taken place" (Art 17(1)[b]); the individual has no right to have access to the data itself, which makes it in practice impossible to challenge incorrect data, and the individual has no right to be informed about the purpose for which data has been transmitted. Moreover, according to Article 16(2), each of the member states party to the transmission of data can ask the other member state not to inform the data subject of the transmission. Even considering the concessions made necessary by the confidential nature of police activity, the framework decision fails to offer clear and robust individual rights.

Moreover, as McGinley and Parkes (2009) argue, an individual's right to be informed about data held on him and to challenge this data even "constitutes a useful mechanism to ensure that accurate information is exchanged" (13), with the lack of mechanisms to verify personal data undermining the effectiveness of law enforcement work. Therefore, the lack of substantive individual rights harms both of the arguments in favour of a coherent data protection framework: neither civil rights protection nor effectiveness of law enforcement cooperation is furthered by the failure to establish robust individual rights for access to and verification of personal data.

4.4 The Scope of Application

Especially crucial is the scope of the framework decision: it only covers the transmission and making available of personal data in the context of the Third Pillar[67]. It does

[67] I.e. between member states as well as between member states and the European authorities established under Title VI TEU (Europol, Eurojust) and from member states to information systems under

not cover the processing of data at the national level or the transmission of data to third parties, i.e. third states or private entities. It also is "without prejudice to essential national security interests and specific intelligence activities in the field of national security" (Article 1(4)) and thus excludes the activity of secret services and other intelligence agencies.

Hustinx (EDPS 2007, part 16) points out that:

> *"(...)the European Parliament, the Conference of data protection authorities, and even the Council of Europe's T-PD Consultative Committee — consisting of data protection representatives of European governments — have all made clear in various occasions that the applicability of the Framework Decision to domestic processing of personal data is an essential condition not only to ensure a sufficient protection of personal data but also to allow an efficient cooperation between law enforcement authorities".*

By excluding domestic data processing, the different levels of data protection in the member states will continue to coexist, and considering the fact that the principle of availability, once fully implemented, would make nationally held data directly accessible to other member states, the limited scope of the DPFD is a serious gap in protection.

A further controversial issue prior to the adoption of the DPFD was the transfer of data to third states, e.g. the USA. The framework decision as of now regulates the transfer in Article 13, one provision of which is cause for much criticism: Article (3)[b] allows information received from another member state to be transferred to a third state insofar "the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law". Apparently, the prior consent of the member state originally holding the data is not necessary for this data to be further transmitted outside of the European Union. Moreover, the DPFD fails to sufficiently regulate which authorities may have access to data stored in the diverse databases of other member states, instead defining 'competent authorities' so vaguely that there is no obligation to explicitly deny secret services access to data held by law enforcement; this undermines the separation between law enforcement and intelligence services which is constitutionally guaranteed in Germany and Great Britain.

---

the third pillar (VIS, SIS, Eurodac etc.). Once transferred to these European bodies, their respective data protection rules continue to apply (see recital 39).

Also, the fragmented landscape of Third Pillar data protection is not merged into one coherent framework, as the respective data protection regimes of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS) as well as the data protection provisions of the Prüm Decision are not affected, according to recital (39) of the DPFD.
The DPFD fails to provide a comprehensible data protection regime covering data processing for security purposes on the national and the transnational level, and thus does neither provide individuals nor security actors with legal certainty regarding the data protection rules which apply when data is being processed.

4.5 Independent Oversight

The original Commission proposal established a Working Party which was supposed to monitor the implementation of the data protection framework decision. The respective provisions[68] have been dropped. National supervisory authorities are still referred to, and their powers of investigation and intervention as well as their legal competencies are strong (Article 25). However, the framework decision drops the provisions on cooperation between different authorities and on the obligation to make a public annual report[69]. Seen together with the cut of the Working Party, the adopted text of the framework decision seems awkward in regard to guaranteeing effective independent oversight and transparency. Cross-border exchange of information should, by common sense, be accompanied by a similarly transnational oversight body, especially considering the difficulties of parliamentary and judicial oversight in the Third Pillar.

4.6 The DPFD: Failing to Create a Harmonized Framework and Guarantee Legal Certainty

The DPFD consistently refers to 'national law' providing specific modalities and exceptions to the provisions of the framework decision; to name a few of the instances, Article 9 refers back to national time limits for the retention of data, Article 12 regu-

[68] Article 31 and Article 32 of COM(2005)475 final.

[69] Article 31 (5) and (7) of COM(2005)474 final.

lates that the receiving member state has to comply with the specific processing restrictions of the transmitting member state and Article 16 leaves the modalities on the right of the data subject to be informed up to the member states.
This reliance on the provisions of national law has the effect that personal data transferred to another member state continues to be subject to the data protection safeguards of the originating member state; however, this is practically impossible to guarantee. As the European Data Protection Supervisor Peter Hustinx describes (EDPS 2007, part 46):

> *"this would mean that a law enforcement body at national or EU level when dealing with a criminal file – consisting of information from various, national, other Member States' and EU authorities – would have to apply different processing rules for different pieces of information depending on whether: personal data have been gathered domestically or not; each of the transmitting bodies has given its consent for the envisaged purpose; the storage is compliant with time limits laid down by the applicable laws of each of the transmitting bodies; further processing restrictions requested by each of the transmitting bodies do not prohibit the processing; in case of a request from a third country, each transmitting body has given its consent according to its own evaluation of adequacy and/or international commitments."*

Consequently, the framework decision "makes exchange of information still subject to different national 'rules of origin' and 'double standards'" (EDPS 2007, part 5). This shows that despite initial attempts to harmonize data protection laws, the final version of the DPFD reflects the approach of mutual recognition of national laws, which is the chosen organizing principle for police and judicial cooperation in criminal matters (see Guild & Geyer 2008:7). This principle allows member states to maintain national rules, but facilitates cooperation by making it mandatory for them to accept the rules of the other member states as equivalent to their own and thus legally obliges member states to mutually trust each other's decisions and practices (cf. Guild & Geyer 2008:7). Concerning the issue of data protection, the application of the principle of mutual recognition does not manage to offer the legal certainty that information sharing needs as it causes the fragmentation of data protection under the Third Pillar to continue. Therefore, despite the adoption of this framework decision, information sharing will continue to suffer from a lack of effectiveness and patchy fundamental rights protection. The legitimacy of information sharing initiatives under the Third Pillar is already weak due to the lack of democratic accountability and effective judicial control (input legitimacy); by undermining the effectiveness of information

sharing, the data protection framework decision furthermore fails to improve output legitimacy.

5. Conclusion

The terrorist attacks of 9/11, and then in particular of those in Madrid and London in 2004 and 2005 acted as catalysts for the rapid acceleration of EU policies related to internal security. Since then, the European Union has been very active in building a European security regime that is far from being limited to counterterrorism but spans the range of security policies, with legislation regulating border controls, visa, immigration and asylum laws, data retention, data exchange and the mutual recognition of criminal law. The threat of terrorism provides the context for this promotion of "a much broader criminal law enforcement agenda" (Andreas & Nadelmann 2008:189) which aims at making law enforcement in Europe more effective, employing a hybrid strategy of strengthening intergovernmental cross-border police and criminal law cooperation as well as creating supranational security actors such as Europol, Eurojust and Frontex.

Under the umbrella of the 'area of freedom, security and justice', the European Union promotes the principle of availability, which in its fullest implementation would abolish the concept of information being the property of a specific authority and create "a EU-wide right of use of data" (Balzacq et al. 2006:116). The principle of availability has been partially implemented by the Swedish Framework Decision of 2006 and the Prüm Decision of 2008, which both created new information exchange regimes, with their particular communication channels, types of information exchanged, authorities authorised to access the system and data protection provisions. In December 2009, the European Council will adopt a new five-year strategy for justice and home affairs and security policy for 2010-2014, following the Tampere Programme (1999-2004) and the Hague Programme (2005-2009). This 'Stockholm Programme' will further develop the central role of information technology in today's security environment; the Future Group Report, which can be seen as a blueprint for the later programme, is permeated with references to the opportunities public security actors are provided with by the 'digital tsunami', i.e. the increasing amount of data generated about a per-

son in daily life[70]. The free flow of information between security actors is seen as a key component of European security, and therefore, the Stockholm Programme will most probably extend the principle of availability to the exchange of additional categories of data (Future Group 2008:9), such as communications data, ballistics, data from civil registers, photographs and income information.

Indubitably, the EU is on its way to become an active provider of security, motivated by the cross-border character of many of today's security threats such as terrorism, organised crime and drugs trafficking. This shift of decision-making in security matters to the European level may lead to a safer Europe - however, this trend also threatens citizens' civil liberties.

In the member states of the EU, the balance between security and liberty is safeguarded by the checks and balances so central to liberal democracy. On the EU level, these safeguards are deficient: national parliaments are less effective in scrutinizing legislative proposals, and under the current legal framework of the Third Pillar, democratic accountability by the European Parliament and judicial control by the ECJ are severely impaired. Most importantly, the increased exchange of personal data between law enforcement authorities is not accompanied by a coherent and robust legal framework for data protection.

The Data Protection Framework Decision of November 2008 most probably will form the core document for data protection in law enforcement cooperation for the foreseeable future. It suffers from serious deficits regarding central principles of data protection, as it provides insufficient purpose limitation, only weak individual rights, has an insufficient scope and harms effective cooperation by neither guaranteeing acceptable data quality nor providing a harmonized framework.

All in all, it clearly bears the marks of being a lowest-common-denominator agreement, with all controversial issues being watered down to achieve unanimity in the Council and thus sacrificing a high level of data protection. It does not provide satisfactory protection of civil liberties and in many aspects, it weakens data protection in

[70] In a concept paper presented at the October 2007 meeting of the Future Group, the representative of the government of Portugal elaborated on the potential information available to law enforcement: "In the next few years billions of items in the physical world will be connected, using technologies such as radio-frequency identification (RFID), broadband wireless (WiFi, WiMAX), satellite and small area wireless (Bluetooth, wireless USB, ZigBee). This means it will be possible to trace more and more objects in real-time and to analyse their movement and activity retrospectively." (Portugal 2007, part 5) This also implies the real-time tracking of persons by using the GPS imbedded in mobile phones.

Europe by falling below the standard of protection established by the CoE Convention 108. The Data Protection Framework Decision also fails to fulfil its intended aim of improving the effectiveness of law enforcement cooperation, as its organising principle of mutually recognizing national rules does not manage to guarantee the legal certainty and comprehensibility that regular data exchange needs. At a time when information sharing is decisively promoted, this is disappointing and cause for concern.

As the analysis of the data protection framework in Third Pillar matters shows, the development of extensive security regimes is not sufficiently counterbalanced by a strong fundamental rights regime and effective institutional safeguards, leading to an imbalance which will shape the relation between security and liberty for the foreseeable future. Security threats are increasingly perceived to be of a transnational nature, and therefore demanding a corresponding shift of policing to the European level, while checks and balances largely are bound by the national context, a situation that allows national ministers to play the two-level game of sidestepping domestic constraints by choosing the venue of the EU Council to realize disputed security policies. One can only hope that the resulting primacy of the security rationale in EU policy-making does not lead to an accelerating trend of weakening civil liberties protection in order to guarantee an illusion of security. The Treaty of Lisbon may help in preventing such an undermining of the central values of human rights and fundamental freedoms on which the European Union is allegedly built. Even though not alleviating all points of concern, the Treaty of Lisbon would significantly strengthen the safeguards on the European level by strengthening the legal status of civil rights protection[71] and improving democratic and judicial oversight[72]. However, it is also the continuing lack of public scrutiny regarding security policy that makes the building of an extensive European security regime out of the public's eye possible. One therefore has to hope that the public discourse will shift to the threat to individual liberty posed by the securitization of EU policy fields, and that public actors will realize their responsibility to protect the values the European Union stands for.

---

[71] The Charter of Fundamental Rights of the EU would be elevated to primary law (Article 6(1)) and the EU would accede to the ECHR (Article 6(2)).

[72] The extension of the co-decision procedure would make the European Parliament a true co-legislator, and extend the competencies of the European Court of Justice, though its jurisdiction remains limited by the exception clause regarding public security matters (Article 240b).

Bibliography:

Anderson, M. et al. (1995) *Policing the European Union*. Oxford.

Anderson, M. & Apap, J. (2002) *Striking a Balance between Freedom, Security and Justice in an Enlarged European Union*. Brussels.

Andreas, P. & Nadelmann, E. (2006) *Policing the Globe. Criminalization and Crime Control in International Relations*. Oxford and New York.

Balzacq, T. & Carrera, S. (2005). 'The EU's Fight against International Terrorism. Security Problems, Insecure Solutions'. CEPS Policy Brief 80.

Balzacq, T. & Carrera, S. (eds.) (2006) *Security Versus Freedom? A Challenge for Europe's Future*. Aldershot, UK and Burlington, VT.

Balzacq, T., Bigo, D., Carrera, S. & Guild, E. (2006) 'The Treaty of Prüm and EC Treaty: Two Competing Models for EU Internal Security', in: Balzacq, T. & Carrera, S. (eds.) (2006) *Security Versus Freedom? A Challenge for Europe's Future*. Aldershot, UK and Burlington, VT.

Bennett, C.J. (1992) *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*. New York.

Baird, Z. & Barksdale, J. (2006) 'Building a Trusted Information-Sharing Environment', in Northouse, C. (ed.) (2006) *Protecting What Matters. Technology, Security and Liberty since 9/11*. Baltimore, pp. 51-62.

Bellanova, R. (2008) 'the "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange?', in: Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.

Bendiek, A. (2006) 'Cross-Pillar Security Regime Building in the European Union: Effects of the European Security Strategy of December 2003'. *European Integration online Papers*, Vol. 10, 9.

Bigo, D. (2000) 'Liaison Officers in Europe: New Actors in the European Security Field', in Sheptycki, J. E. (ed.) (2000) *Issues in Transnational Policing*, London and New York, pp. 67-100.

Bigo, D., Bruggeman, W., Burgess, P. & Mitsilegas, V. (2007) 'The principle of information availability'. Available at http://www.libertysecurity.org/article1376.html?var_recherche=Bigo%20information (accessed 4 May 2009).

Bigo, D. (2008) 'EU Police Cooperation: National Sovereignty Framed by European Security?', in: Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.

Bertelsmann Stiftung (ed.) (2005) *Securing the European homeland: The EU, terrorism and homeland security*. Gütersloh.

Bos, E. & Helmerich, A. (eds.) (2002) *Neue Bedrohung Terrorismus. Der 11. September und die Folgen*. Münster.

Bunyan, T. (2006) 'The "principle of availability"'. *Statewatch Analysis*. Statewatch Organisation. Available at http://www.statewatch.org/analyses/no-59-p-of-a-art.pdf (accessed 6 May 2009).

Bunyan, T. (2009) 'The Shape of Things to Come – EU Future Group'. *Statewatch Analysis*. Statewatch Organisation.

Chalmers, D. & Tomkins, A. (2007) *European Union Public Law*. Cambridge and New York.

Commission of the European Communities (2005) 'Proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.' COM (2005)475 final, 04 October 2005.

Council of the European Union (2001) 'Council Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism'. OJ L 344/93, 28 December 2001.

Council of the European Union (2002a) 'Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism'. OJ L 164/3, 22 June 2002.

Council of the European Union (2002b) 'Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States'. OJ L 190/1, 18 July 2002.

Council of the European Union (2004a) 'Council Declaration of 25 March 2004 on Combating Terrorism '. Brussels.

Council of the European Union (2004b) 'The Hague Programme. Strengthening Freedom, Security and Justice in the European Union'. Presidency Conclusions, November 2004.

Council of the EU (2005a) 'Prüm Convention'. Note from the Council Secretariat, No. 10900/05, 7 July 2005.

Council of the European Union (2005b) 'The European Union counter-terrorism strategy', Council document 14469/4/05 REV 4, 30 November 2005, Brussels.

Council of the European Union (2006a) 'Revised action plan on terrorism: update June 2006'. Commission document SEC(2006) 686, EU Council document 10043/06, 31 May 2006, Brussels.

Council of the European Union (2006b) 'Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and

intelligence between law enforcement authorities of the Member States of the European Union'. OJ L 386, 29 December 2006.

Council of the European Union (2008a) 'Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime'. OJ L 210, 6 August 2008.

Council of the European Union (2008b) 'Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime'. OJ L 210, 6 August 2008.

Council of the European Union (2008c) 'Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters'. OJ L 350, 30 December 2008.

Den Boer, M. & Monar, J. (2002) 'Keynote Article: 11 September and the Challenge of Global Terrorism to the EU as a Security Actor'. *Journal of Common Market Studies* Vol. 40: pp. 11-28.

De Hert, P. & Gutwirth, S. (2006) 'Interoperability of police databases within the EU: an accountable political choice?' *TILT Law & Technology Working Paper*, No. 001/2006. A April 2006. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=971855 (accessed 5 May 2009).

Eder, F. & Senn, M. (2009) *Europe and Transnational Terrorism. Assessing Threats and Countermeasures.* Baden-Baden.

Eder, F. & Senn, M. (2009) 'The Art of the Impossible? Deterring Measures in Europe's Fight Against Transnational Terrorism', in: Eder, F. & Senn, M. (2009) *Europe and Transnational Terrorism. Assessing Threats and Countermeasures.* Baden-Baden.

European Council (2003) 'A secure Europe in a better world: the European security strategy', 12 December 2003, Council of the EU, Brussels.

European Court of Justice (2008)'Jurisdiction of the Court of Justice to give preliminary rulings on police and judicial cooperation in criminal matters', March 2008. Available at http://curia.europa.eu/jcms/jcms/Jo2_7031/procedure (accessed 15 May 2009)

European Data Protection Supervisor (2007) 'Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters`. 2007/C 139/01, 27 April. OJ C 139/1, 23 June 2007.

European Parliament, Council and Commission of the European Union (2000) 'Charter of Fundamental Rights of the European Union'. 2000/C 364/01, OJ C 364/5, 18 December 2001.

European Parliament (2008) 'Combating terrorism / protection of personal data - MEPs underline freedom of expression'. Press Release, 22 September 2008.

European Union Council Secretariat (2007) 'European Union Factsheet: EU and the Fight against Terrorism', available at http://www.consilium.europa.eu/uedocs/cmsUpload/Factsheet-fight%20against%20terrorism%20ENMarch2007.pdf#_ (accessed 29 April, 2009).

Follesdal, A. & Hix, S. (2006) 'Why there is a democratic deficit in the EU: a response to Majone and Moravcsik'. *Journal of Common Market Studies, Vol. 44*, 3: pp.533-562.

Future Group, Portugal (2008) 'Public Security, privacy and Technology in Europe: Moving Forward. Concept paper on the European strategy to transform Public security organizations in a Connected World'. Paper for the 4th Meeting of the Future Group, December 2007.

Guiraudon, V. (2000) 'European Integration and Migration Policy: Vertical Policy-making as Venue Shopping'. *Journal of Common Market Studies*, Vol. 38, 2: pp.251-71.

Gonzalez Fuster, G. & Paepe, P. (2008) 'Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects', in: Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.

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

Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.

Guild, E. & Geyer, F. (2008) 'Introduction: The Search for EU Criminal Law – Where is it Headed?', in: Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.

Haftendorn, H., Keohane, R. O. & Wallander, C. A. (1999) *Imperfect Unions. Security Institutions over Time and Space*. Oxford and New York.

Hayes, B. (2005) 'A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe'. *Statewatch News Online*, June 2005. Available at www.statewatch.org/news/2005/jun/ben-hayes-A-Fai.pdf (accessed 06 May 2009).

Held, D. (2006) *Models of Democracy*. Cambridge and Malden, MA.

Hix, S. (2008) *What's Wrong with the European Union and How to Fix It.* Cambridge and Malden, MA.

Hempel, L., Carius, M. & Ilten, C. (2009) 'Exchange of Information and Data between Law Enforcement Authorities within the European Union'. Study requested by

the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. Brussels.

Höreth, M. (1999) 'No way out for the beast? The unsolved legitimacy problem of European governance'. *Journal of European Public Policy,* Vol. 6, 2: pp. 1350-1763.

Howorth, J. (2006) 'European Security and Counter-Terrorism'. Working Paper, Ford Institute for Human Security. Available at http://www.ridgway.pitt.edu/docs/working_papers/HoworthFormatted.pdf (accessed 27 April, 2009).

International Commission of Jurists (2009) *Assessing Damage, Urging Action. Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights*. Geneva.

Keohane, D. (2005) ‚The EU and international terrorism', in: Bertelsmann Stiftung (ed.) (2005) *Securing the European homeland: The EU, terrorism and homeland security*. Gütersloh.

Kohler-Koch, B. & Eising, R. (eds.) (1999) *The Transformation of Governance in the European Union*. London.

Kosta, E., Coudert, F. & Dumortier, J. (2007) 'Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive'. Paper presented at the 2007 Annual Conference of the British & Irish Law, Education and technology Association, April 2007.

Kratochwil, F. (2003) 'Der 11. September 2001 – Das Ende des Hobbes'schen Projekts?', in: Bos, E. & Helmerich, A. (eds.) (2002) *Neue Bedrohung Terrorismus. Der 11. September und die Folgen*. Münster.

Lang, R. (2008) 'Third Pillar Developments from a Practitioner's Perspective', in: Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.

Lord, C. & Beetham, D. (2001) 'Legitimizing the EU: Is there a "post-parliamentary basis" for its legitimization?' *Journal of Common Market Studies*, Vol. 39, 3: pp. 443-462.

Majone, G. (1998) 'Europe's "democratic deficit": the question of standards'. *European Law Journal,* Vol. 4, 1: pp. 5-28.

Maurer, A. & Parkes, R. (2005) 'Democracy and European Justice and Home Affairs Policies under the Shadow of September 11'. SWP *Working Paper*. Berlin.

Maurer, V. (2009) 'Politics and the Threat of Transnational Terrorism in Germany', in Eder, F. & Senn, M. (eds.) (2009) *Europe and Transnational Terrorism. Assessing threats and Countermeasures*. Baden-Baden, pp. 75-105.

McGinely, M. & Parkes, R (2007) 'Data Protection in the EU's Internal Security Co-operation. Fundamental Rights vs. Effective Cooperation?'. *SWP Research Paper*. Berlin.

Mitsilegas, V., Monar, J. & Rees, W. (2003) *The European Union and Internal Security. Guardian of the People?* Basingstoke and New York.

Mitsilegas, V. (2007) 'Police Co-operation: What are the main Obstacles to Police Co-operation in the EU?' Available at http://www.libertysecurity.org/article1379.html?var_recherche=availability (accessed 4 May 2009).

Monar, J. (2007a) 'Common Threat and Common Response? The European Union's Counter-Terrorism Strategy and its Problems'. *Government and Opposition*, Vol. 42, 3: pp. 292–313.

Monar, J. (2007b) 'The EU's approach post-September 11: global terrorism as a multidimensional law enforcement challenge.' *Cambridge Review of International Affairs*, Vol. 20,2: pp. 267-283.

Moravcsik, A. (2002) 'In defence of the "democratic deficit": reassessing legitimacy in the European Union'. *Journal of Common Market Studies,* Vol. 40, 4: pp. 603-624.

Northouse, C. (ed.) (2006) *Protecting What Matters. Technology, Security and Liberty since 9/11*. Baltimore.

Portugal (2007) 'Public Security, Privacy and Technology in Europe: Moving Forward'. Concept paper presented at the Future Group meeting in October 2007. Available at http://www.statewatch.org/stockholm-programme.htm (accessed May 28th).

Puntscher Riekmann, S. (2008) 'Security, Freedom and Accountability: Europol and Frontex', in: Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.
Sanfrutos Cano, E. (2008) 'The Third Pillar and the Court of Justice: A "Praetorian Communitarization" of Police and Judicial Cooperation in Criminal Matters?', in: Guild, E. & Geyer, F. (eds.) (2008) *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot, UK and Burlington, VT.

Scharpf, F. W. (1997) 'Economic integration, democracy and the welfare state'. *Journal of European Public Policy,* Vol. 4, 1: pp. 18-36.

Sheptycki, J. E. (ed.) (2000) *Issues in Transnational Policing*, London and New York.

Soria, J. M. (2006) 'Nachrichtendienste und Polizei. Die Zusammenarbeit in Deutschland und in der EU im Lichte des Trennungsgebots.' *Göttinger Online-Beiträge zum Europarecht*, Vol. 1: pp. 1-17. Available at http://www.europarecht.uni-goettingen.de/Paper44.pdf (accessed 28 May 2009).

Sule, S. (1999) *Europol und europäischer Datenschutz*. Baden-Baden.

Wallander, C. A. & Keohane, R. O. (1999) 'Risk, Threat, and Security Institutions', in: Haftendorn, H., Keohane, R. O. & Wallander, C. A. (1999) *Imperfect Unions. Security Institutions over Time and Space*. Oxford and New York.

Walsh, J. I. (2006) 'Intelligence-Sharing in the European Union: Institutions Are Not Enough`. *Journal of Common Market Studies*, Vol. 44, 3: pp. 625-43.

Weidenfeld, W. (2004) 'Für ein System kooperativer Sicherheit', in Weidenfeld, W. (ed.) (2004*) Herausforderung Terrorismus. Die Zukunft der Sicherheit*. Wiesbaden, pp. 11-25.

Weidenfeld, W. (ed.) (2004*) Herausforderung Terrorismus. Die Zukunft der Sicherheit*. Wiesbaden

Weiler, J. H. H., Haltern, U. & Mayer, F. (1995) 'European Democracy and its critique. Five uneasy pieces'. *EUI Working Paper RSC, 95/11*.

Wiegand, I. (2008) *The Protection of Human Rights and Fundamental Freedoms in the Fight against Terrorism. The Case of the European Union after September 11, 2001*. Stuttgart.

Woyke, W. (1998) *Europäische Union*. Wien.