

The third pillar in practice: coping with inadequacies*

Information sharing between Member States

*Hielke Hijmans***

1. Introduction and issues raised

1. Even aside from the Constitutional Treaty, the European Union has considerable aspirations for an area of freedom, security and justice. The Hague programme¹ was produced with a view to subsequent entry into force of the Constitutional Treaty (the programme having been adopted over six months before the referendums in France and the Netherlands), on the assumption that it was possible to anticipate that Treaty. According to its introduction, the programme reflects the aspirations avowed in the Constitutional Treaty. Its legal basis is to be found in the existing Treaties². The Hague programme, the various Commission policy papers aimed at implementing it³ and the (proposed) legal provisions for the third pillar make for the denationalisation of criminal law, in what René Barents has classed as an irreversible process.

2. This discussion paper goes on from Barents' conclusions to look at the practice of cooperation: where will it get us in practice if we try and build a European criminal justice area in spite of the lack of a Constitutional Treaty which was supposed to bring a necessary strengthening of the contractual framework in just this field? Can the EU live up to the aspirations set out in the Hague programme, particularly as regards police and judicial cooperation in criminal matters?

* The original paper in Dutch was published in the Dutch legal journal SEW and can be cited as follows: Hielke Hijmans 'De derde pijler in de praktijk : leven met gebreken over de uitwisseling van informatie tussen de lidstaten' SEW 2006.91

** Hielke Hijmans is an adviser to the European Data Protection Supervisor. His previous positions include acting as an adviser at the Ministry of Justice and as a law clerk at the Court of Justice of the European Communities (in Mr Geelhoed's office). This discussion paper is, of course, written in a personal capacity.

¹ The Hague programme: strengthening freedom, security and justice in the European Union, OJ C 53, 2005, p. 1.
² Section II.1 of the Hague programme.

³ See the package of measures proposed by the Commission on 28 June 2006 as a result of a political assessment of implementation of the Hague programme, in particular the Commission communications of that date entitled "Implementing the Hague programme: the way forward" (COM(2006) 331 final) and "Report on the implementation of the Hague programme for 2005" (COM(2006) 333 final).

3. Let me focus on a few important issues concerned with improving exchange of information between Member States⁴. This is of interest because third-pillar cooperation to bring about a European criminal justice area will need above all to involve easier information sharing. The basic premise here is that (partly as a result of the removal of internal borders within the European Union) crime is becoming increasingly transnational, whereas action to tackle it is constrained by national borders. Under the EU Treaty, there is no European law enforcement authority, and national authorities are not normally empowered to take action within other Member States' territory. Information sharing is thus of the essence. A criminal moving from one Member State to another must not be allowed to go unpunished⁵. The threat of terrorist attacks also creates a more pressing need for information sharing. That threat is at any rate often adduced as a reason for introducing new EU legal instruments. An apt example, highly topical at the time of writing, is Commissioner Frattini's reaction to the foiled plans for aircraft hijackings in the United Kingdom: a proposal to require national authorities to be supplied with passenger data for all flights to, from or within Europe⁶.
4. Exchange of police and judicial information⁷ is thus seen as a key cooperation tool. If that tool is to work, however, authorities in the Member States (there may be two or more involved) have to be able to trust one another. The information concerned is usually sensitive and confidential, in many cases gleaned by dint of considerable police and judicial effort, in order to solve a particular crime. This in itself provides two reasons why readiness to share information cannot be taken for granted. Trust is not just important in dealings between authorities, though; data subjects also need to be able to rely on their rights not being infringed when information is shared between Member States. Trust also involves constitutional aspects. (Mutual) trust is considered in section 2.
5. The European legal armoury must help make information sharing possible on a basis of mutual trust. This in any case requires that the Treaties provide an adequate legal basis for cooperation and that EU action satisfy criteria of effectiveness and proportionality. Effective, proportionate EU action is not, on the face of it, easy to achieve, however, in view of the considerable differences between countries in substantive and procedural criminal law. The European legislature will need both to take steps limiting the adverse implications of such

⁴ As referred to in section III.2.1 of the Hague programme. The choice of focus is also due to my own involvement in the matter as an adviser to the European Data Protection Supervisor.

⁵ See also the reference to the 1980 Convention in Barents, paragraph 4.

⁶ See, for instance, The Guardian of 17 August 2006 and EDRI-gram of 30 August 2006 (European Digital Rights, on www.edri.org).

⁷ And also of information available from third parties, for police and judicial purposes.

differences for information sharing and to make allowance for the impossibility of completely eliminating the differences themselves. I would lastly point out that EU action must, of course, fulfil prerequisites for democracy and the rule of law. The problems encountered by the European Union within the third pillar are discussed in section 3.

6. Section 4 deals with a more specific consequence of the Treaty architecture, demarcation between the first and the third pillars, with the PNR judgment given by the Court of Justice on 30 May 2006⁸ playing a key part here.
7. How the EU legislature is to bring about an improvement in information sharing is discussed in section 5. Mutual recognition as a reflection of mutual trust is the basis for action and should make it possible to live up to the Hague programme aspirations. However, mutual recognition in itself is not sufficient. Additional provisions are required. Three kinds of additional provisions, as included in recent Commission proposals, are discussed by way of example. The proposal for a Framework Decision on data protection within the third pillar⁹ serves as an example of minimum-level harmonisation of ground rules, the proposal on exchange of information under the principle of availability¹⁰ as an example of a requirement for active cooperation between Member States, and the proposals for a second-generation Schengen Information System (SIS II)¹¹ as an example of a partly centralised technical structure to support information sharing between Member States.
8. Section 6 considers ways of getting around third-pillar decision-making difficulties. It looks at the Prüm Convention and at renewed interest in the bridging clause. Section 7 concludes the discussion paper, by putting some points to the meeting.

⁸ Judgment in joined Cases C-317/04, *European Parliament v. Council of the European Union* and C-318/04, *European Parliament v. Commission of the European Communities* (not yet published). PNR stands for passenger name record, i.e. passenger data held by airlines.

⁹ Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final). See also the European Data Protection Supervisor's opinion, OJ C 47, 2006, p. 12.

¹⁰ Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final). See also the European Data Protection Supervisor's opinion, OJ C 116, 2006, p. 8.

¹¹ Proposal for a Council Decision on the establishment, operation and use of the second-generation Schengen Information System (SIS II) (COM(2005) 230 final), proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second-generation Schengen Information System (SIS II) (COM(2005) 236 final) and proposal for a Regulation of the European Parliament and of the Council regarding access to the second-generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final). See also the European Data Protection Supervisor's opinion, OJ C 91, 2006, p. 38. In contrast to the proposals referred to in footnotes 9 and 10, decisions on these proposals are currently (in August 2006) to be expected soon.

2. (Mutual) trust

2.1. Trust between authorities

9. Police and judicial cooperation requires mutual trust. It is no accident that the Constitutional Treaty¹² regards promoting mutual confidence between authorities as a foundation stone of an area of freedom, security and justice. The Court of Justice saw mutual confidence as lying at the heart of the Gözütok and Brügge judgment concerning application of the double-jeopardy bar. The Court found it necessary "that the Member States have mutual trust in their criminal justice systems and that each of them recognises the criminal law in force in the other Member States even when the outcome would be different if its own national law were applied"¹³. That finding by the Court raises the question of whether the mutual trust which the Court considers necessary is actually forthcoming from Member States. Unfortunately, it often is not. Even leaving aside the restrictions in Title VI of the EU Treaty, themselves in turn stemming from distrust which makes Member States reluctant to give up sovereignty in criminal justice, strong action by the EU under that title is in fact hampered above all by a lack of mutual trust.

It has been pointed out by Weyembergh "how difficult the realisation of the mutual trust implied by mutual recognition in fact is. The daily practice of judicial cooperation offers many examples of the prevalence of mutual distrust"¹⁴. A good example, to which she also refers here, is implementation under national law of the Framework Decision on the European arrest warrant¹⁵. The Framework Decision not only requires acceptance of the application of another country's criminal law¹⁶ but also presupposes a Member State's active assistance in the enforcement of judgments given in other Member States, even if those other Member States have different criminal justice systems¹⁷.

10. Lack of trust is, in my view, also one of the reasons for criminal law practitioners' reluctance

¹² Article I-42.

¹³ Judgment given by the Court of Justice on 11 February 2003 in joined Cases C-187/01, Gözütok, and C-385/01, Klaus Brügge, ECR I-1345, paragraph 33.

¹⁴ Anne Weyembergh, *Approximation of criminal laws, the Constitutional Treaty and the Hague Programme*, Common Market Law Review No 42, pp. 1567-1597, 2005 (p. 1575).

¹⁵ Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, p. 1. The implementation of that Framework Decision was a laborious process (on this point, see: Report on the implementation of the Hague programme in 2005, referred to in footnote 3).

¹⁶ As required under the Gözütok and Brügge judgment.

¹⁷ See, in particular, Article 1(2) of the Framework Decision.

to transfer powers to the European Union. Within their own borders, Member States have a monopoly in the use of coercive measures, including force against individuals. They are also responsible for supervising the use of coercive measures, so as to safeguard against any infringement of fundamental rights. Mutual recognition entails trust by Member States in decisions taken in other Member States in this sensitive area too. The fact that such trust cannot be taken for granted, even between democratic countries governed by the rule of law, can be seen, for instance, from the *ex parte Ramda* judgment given in the United Kingdom, as described by Guild¹⁸, which concerned the extradition to France of an Algerian suspected of terrorism. The evidence against that individual had largely been obtained by the use in France of dubious interrogation techniques and there were thus grounds for opposing extradition. With regard to criminal law practitioners, I would further refer to Barents' discussion paper. In sharing police and judicial information under the third pillar, mutual trust also has a special part to play. This normally involves protected, confidential data, often compiled and processed by the police for a particular criminal case. Sharing those data with another Member State means that they can no longer rely on their own authorities, subject to their own legislation, to ensure such protection and confidentiality. This requires real trust in their counterparts in another Member State, who will often be unknown to them and in addition do not speak the same language.

2.2. *From a data subject perspective*

11. Data subjects must be able to rely on the exercise of their rights not being impaired by information sharing between Member States' police and judicial authorities. The implications of this are twofold. In the first place, this is an area of law in which, as pointed out, there are considerable differences between Member States' legal systems, both in substantive and in procedural criminal law. Information sharing between two or more Member States must not leave the public enjoying only the lowest standard of protection out of those afforded by the Member States involved (which could even lead to the notorious "race to the bottom"¹⁹). That is why the various (proposed) Framework Decisions include conflict-of-law rules determining the law applicable. In an isolated case, information sharing even has to comply with national law in more than one Member State, thus providing data subjects with a high

¹⁸ Elspeth Guild, *Crime and the EU's Constitutional Future in an Area of Freedom, Security and Justice*, *European Law Journal*, 2004, pp. 218-234 (in particular, p. 227).

¹⁹ See Barents, paragraph 19 (on having to accept substandard law from other Member States) and paragraph 22 (on the "race to the bottom").

standard of protection²⁰. In the second place, information sharing itself entails risk for the public. It is not immediately evident which Member State is responsible for the quality and security of information and for supervision of these matters. Nor is it clear in which Member State the public can actually take legal action. The case behind the *Commission v. Spain* judgment²¹ will serve to illustrate this point. It involved two Algerian nationals refused entry into the Schengen area by the Spanish authorities on account of an alert for them in the SIS. The judgment shows that one of them was refused entry after landing at Barcelona airport. Under the Schengen Convention, the alert-issuing state, in this case Germany, bears sole responsibility for the accuracy and up-to-dateness of the data and for their lawful entry in the SIS and is the only one empowered to amend, add to, correct or delete those data. Other contracting states are automatically required to deny entry to the alien concerned. That automatic effect, as the Court also states, reflects the principle of cooperation between contracting states. In short, those concerned are not allowed into Spain and cannot actually do anything about that vis-à-vis the Spanish authorities.

2.3. *The constitutional dimension*

12. Article 1(3) of the Framework Decision on the European arrest warrant²² shows that mutual trust is directly related to observance of fundamental rights and basic legal principles. In 2005 the German Federal Constitutional Court annulled Germany's implementing legislation on the grounds that it did not fully respect the country's constitutional ban on extradition of German nationals²³. As that judgment shows, third-pillar cooperation between Member States may come up against constitutionally enshrined distrust of another country's legal system. Exchange of information under the principle of availability²⁴ might also, for similar reasons, meet with constitutional objections in Germany or in other Member States, since in such information sharing a Member State has no control over access to and use of personal data compiled by police and judicial authorities. The German Federal Constitutional

²⁰ See, for instance, Article 7 of the proposal for a Council Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States (COM(2005) 690 final). As the European Data Protection Supervisor explains (in paragraph 38 of the opinion of 29 May 2006, published on www.edps.europa.eu), where information from criminal records is used for purposes other than criminal proceedings, the law of three Member States may be cumulatively applicable.

²¹ Judgment given by the Court of Justice on 31 January 2006 in Case C-503/03 (not yet published), in particular paragraphs 29-37. As the third-country nationals concerned were married to EU citizens, the Court ultimately came down in their favour. See also paragraph 13.

²² Referred to in footnote 15. The provision serves to safeguard against any infringement of the rights and principles laid down in Article 6 of the EU Treaty. On that provision, see also paragraph 43.

²³ Judgment of 18 July 2005, 2 BvR 2236/04.

²⁴ See also paragraphs 52 and 53. The point is that, in unqualified application of that principle, the source Member

Court has ruled that the taking and testing of bodily samples (DNA) clashes with Germany's constitutionally enshrined right of self-determination as regards personal information. This means that such samples may be used in criminal proceedings only under strict conditions. There is at any rate a need to fulfil requirements of proportionality, which makes it impossible to use such samples in the case of less serious offences²⁵.

13. For data subjects, the constitutional dimension means that they must be able to rely upon protection of their fundamental rights as laid down, in particular, in the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights. Protection of those rights seems also to be figuring increasingly prominently in the case-law of the Court of Justice²⁶. For information sharing between Member States, the following come to mind in particular:

- the right to effective protection in law, as laid down in Article 6 of the ECHR and Article 47 of the Charter. The significance of this is suitably illustrated by the case behind the *Commission v. Spain* judgment (see paragraph 11 above). Article 111 of the Schengen Convention also contains a specific provision designed to afford effective legal protection. Anyone may apply to the courts in any Schengen country with regard to an SIS alert concerning that person, with the issuing state being required to enforce a final decision by another state's courts²⁷. That is an interesting provision, but it does not entirely eliminate the problem outlined in paragraph 11;
- the right to respect for privacy (Article 8 of the ECHR and Article 7 of the Charter) and to protection of personal data (Article 8 of the Charter). Mention may be made, by way of illustration, of the individual rights forming part of the fundamental right to protection of personal data, such as people's right to have access to data processed concerning them and their right to oppose processing of data²⁸. In the police and judicial sphere, as is only natural, those rights are subject to the necessary restrictions.

State has no say in the use made of data in other Member States.

²⁵ Inter alia, the judgment of 14 December 2000, BvR 1741/99.

²⁶ See here, for instance, the judgment in Case C-540/03, *European Parliament v. Council*, concerning the Directive on the right to family reunification. In that judgment the Court carried out a detailed examination of compatibility with the ECHR and attached some legal force to the Charter. Reference should also be made to Douglas-Scott, *A tale of two Courts: Luxembourg, Strasbourg and the growing European human rights acquis*, *Common Market Law Review* No 43, pp. 629-665, 2006.

²⁷ This provision has recently been applied by the courts in Haarlem (decision of 6 December 2005, 111842/HA RK 05-44) and Alkmaar (decision of 10 November 2005, 79543/HA RK 05-14). The decisions required Spain to withdraw alerts for certain individuals.

²⁸ See, for instance, Articles 12 and 14 respectively of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, p. 31.

The judgments given by the Court of First Instance concerning restrictive measures in combating terrorism show how far those restrictions may go in some cases. In the Ahmed Ali Yusuf judgment, the Court found that "any opportunity for the applicants effectively to make known their views on the correctness and relevance of the facts in consideration of which their funds have been frozen and on the evidence adduced against them appears to be definitively excluded". It nonetheless considered that "observance of the fundamental rights of the persons concerned does not require the facts and evidence adduced against them to be communicated to them" ²⁹.

Paradoxically enough, that reasoning by the Court brings out the importance of protecting fundamental rights. If such a far-reaching restriction of those rights is allowed, it must at any rate actually be possible to ensure that this does not result in them being completely eroded.

3. Main third-pillar inadequacies

14. In its communication of 28 June 2006 ³⁰ the Commission lists the third pillar's inadequacies as follows: specific legislative instruments which complicate implementation, insufficient powers for the European Parliament, the need for unanimity, a right of initiative shared between the Commission and Member States, limited jurisdiction for the Court of Justice and non-availability of Treaty infringement proceedings (under Article 226 EC). That summation basically stems from a comparison between the third pillar and the first pillar ³¹. The account given below is mainly concerned with the third pillar's special need: to what extent can the third-pillar armoury help make cooperation possible on a basis of mutual trust (see paragraph 5 above)?

3.1. A broad legal basis

15. Powers for third-pillar legislative action are couched in narrow terms in Articles 29 to 32 EU. This applies especially to powers explicitly providing for harmonisation of national legislation, such as Article 31(1)(e), which is confined to "minimum rules relating to the

²⁹ Judgment given by the Court of First Instance on 21 September 2005 in Case T-306/01, Ahmed Ali Yusuf et al. v. Commission and Council, paragraphs 319 and 320. The Court's findings do not actually refer to European data protection rules, but do relate to them in substance. That judgment is also discussed by C. Tomuschat in Common Market Law Review No 43, pp. 537-551, 2006 (though mainly as regards the impact of UN decisions on EU law).

³⁰ "Implementing the Hague programme: the way forward", referred to in footnote 3, section 3.1.

³¹ The customary Community instruments, aside from any specific restrictions in the EC treaty itself, such as in Title IV of Part Three.

constituent elements of criminal acts and to penalties in the fields of organised crime, terrorism and illicit drug trafficking". Third-pillar powers thus seem wholly different in nature from the broadly worded powers in the EC Treaty. Reference need only be made to Article 95 EC (internal market), although environmental regulatory powers under Articles 174 and 175 EC, for instance, are also very broad. Third-pillar powers seem more like powers under Article 63 EC for legislative action in the area of asylum and immigration, where it needs to be considered in each case whether there is a sufficient legal basis for proposed regulation. Upon closer inspection, however, third-pillar powers extend somewhat further than is apparent at first sight, as I have previously argued in my contribution to the collection of essays "*De EU, de interstatelijkheid voorbij?*" [The EU, beyond the inter-state nexus?]³². Articles 29 to 32 EU do not provide a platform for legislation³³, as can be seen in practice. A good example is provided by the Framework Decision on the standing of victims in criminal proceedings³⁴. The Framework Decision is not attributable to any particular part of Article 31 EU, as shown by the general reference to that article in the preamble.

16. In the Pupino case, Advocate-General Kokott made a few brief points³⁵ explaining why, in her view, that Framework Decision had an adequate legal basis. To start with, the list in Article 31 EU is not exhaustive and heed must be paid to the general objectives of police and judicial cooperation in criminal matters, which is intended to provide citizens with a high level of safety. She went on to give three reasons why, to her mind, there was a legal basis for rules to protect victims in criminal proceedings. Firstly, protection of victims is important for the safety of citizens³⁶. Secondly, Community rules may encourage judicial cooperation, since the evidence provided by victims in criminal proceedings can be used in all Member States. Thirdly, the third-pillar need for unanimity prevents Member States from being bound by EU legislation without their consent. Frankly, I find the Advocate-General's arguments somewhat contrived (especially her third reason), but I do agree with her initial premises, namely that there is a broad legal basis and the content of Article 29 EU is determinant. Articles 29 et seq. confer general powers to legislate with regard to cooperation between Member States' authorities, as a means of fostering mutual trust and for the purposes of the

³² H. Hijmans, "*Interstatelijkheid in ontwikkeling: de 'zuiver interne situatie' verliest aan betekenis*" [Moving on from the inter-state nexus: the declining meaningfulness of a "purely domestic" situation], in "*De EU, de interstatelijkheid voorbij?*" [The EU, beyond the inter-state nexus?], E.R. Manunza and L.A.J. Senden (ed.), Wolf Legal Publisher, 2006. I am here further developing the thinking behind that article.

³³ Article 63 EC could be seen as one.

³⁴ Council Framework Decision of 15 March 2001 on the standing of victims in criminal proceedings, OJ L 82, p. 1

³⁵ See paragraphs 48 to 52 of the opinion in Case C-105/03 (see footnote 50). The Court did not consider the legal basis in its judgment.

³⁶ The objective mentioned in the first paragraph of Article 29 EU.

objective in the first paragraph of Article 29.

17. With regard to harmonisation of substantive and procedural criminal law, Weyembergh draws a pertinent distinction between the supporting and the autonomous roles of harmonisation ³⁷. In my view, harmonisation of legislation within the third pillar is possible in support of measures for closer cooperation under Article 29 EU. The third pillar also makes provision for autonomous harmonisation. This applies primarily, of course, to Article 31(1)(e), as explicitly referred to in Article 29. However, Article 31(1)(c) and Article 30(1)(b) also involve explicit harmonisation powers. Where the European legislature gives effect to those provisions, Article 29 EU can be presumed to be complied with.
- It may, of course, be objected that such a broad interpretation of third-pillar powers runs counter to the (treaty-making) Member States' reluctance to transfer powers to the EU in this area. Yet the EU legislature itself has given an even broader interpretation in adopting a Framework Decision on the standing of victims in criminal proceedings. For the nub of that Framework Decision is harmonisation of an area of criminal procedure, something for which there is no explicit provision in the EU Treaty.
18. I would lastly also point to the limitation in Article 29 EU to cooperation between Member States' authorities. Clearly, Article 29 applies not only to police, judicial and customs authorities but also to Member States' other authorities insofar as they are assigned responsibilities or (have to) provide assistance in criminal law enforcement. Examples which spring to mind are special investigators or tax inspectors. It is less clear, however, whether Article 29 EU is also considered to cover cooperation between authorities within a Member State, cooperation with authorities in non-member countries and cooperation with private parties involved in criminal law enforcement. A few brief comments here:
- there is a slowly evolving consensus that it is possible, within the third pillar, to enact provisions relating to Member States' domestic situations, where this plays a part in criminal law cooperation ³⁸;
 - cooperation with non-member countries is an important issue in discussion of the proposed Framework Decision on third-pillar data protection. The Commission proposal includes a provision on the subject and there is no reason to challenge the legal basis, given some connection with cooperation between Member States. Title VI of the

³⁷ Weyembergh, *op. cit.*, pp. 1574 et seq.

³⁸ As opined by the Council Legal Service in discussion of the proposal for a Framework Decision on third-pillar data protection.

EU Treaty also explicitly provides power to conclude agreements with non-member countries³⁹;

- cooperation with private parties raises issues concerning demarcation between the first and third pillars and will be considered below in that context.

3.2. *Legal bases: lack of any European enforcement system*

19. There is no European enforcement system. As European integration currently stands, European Union law enforcement is a matter for Member States. In this there is no difference between third-pillar law and Community law. It is only natural that law enforcement should not be transferred to a central, European level. That would hardly fit in with a Europe actually needing to be brought closer to its citizens and would substantially upset the balance between the powers of the Member States and those of the European Union⁴⁰. In criminal justice it would also have to be accompanied by power to use coercive measures, including force, and would thus breach the nation-state monopoly in use of force, a core feature of national sovereignty⁴¹.
20. The lack of any European enforcement system does not make for effectiveness in the EU legislature's action. It thus comes as no surprise that initial steps have been taken towards European structures, at present in fact mainly designed to facilitate cooperation between Member States' authorities. The tasks of Europol and Eurojust⁴², as referred to in the EU Treaty, are directed to that end and include exchanging information⁴³. Other major information systems have been (and are being) set up as well, with European and national components (the SIS, Eurodac and the planned Visa Information System⁴⁴), to support

³⁹ On the scope also available to Member States, see the discussion of the Prüm Convention below.

⁴⁰ For a more extensive discussion of this, see L.A. Geelhoed and H. Hijmans, "*Het rechterlijk toezicht op de uitvoering van het gemeenschapsrecht in een Europabrede Unie*" [Judicial review of implementation of Community law in a Europe-wide Union], SEW [Socio-Economic Legislation, a European and economic law journal] (2002), pp. 407 et seq.

⁴¹ See also paragraph 10.

⁴² Plans for the eventual expansion of Eurojust into a European public prosecutor's office, as laid down in particular in Article III-274 of the Constitutional Treaty, will not be discussed here.

⁴³ See, for instance, Article 3 of the Europol Convention, OJ C 316, 1995, p. 2, and Article 13 of the Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, p. 1.

⁴⁴ The SIS is currently governed by the Schengen Convention (for SIS II, see the proposals referred to in footnote 11). Eurodac was set up under Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, p. 1. The VIS is to be set up under the proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (COM(2004) 835 final).

information sharing between Member States. Only to a limited extent, however, can those systems make good the lack of any European enforcement authority⁴⁵.

3.3. *Effectiveness and proportionality: limited use of legal bases*

21. Despite the lofty ambitions shown at Tampere⁴⁶ and subsequently in the Hague programme, limited use has been made of the legal instruments available under the third pillar. This seems to stem from Member States' reluctance actually to transfer legislative powers in sensitive areas. The third-pillar need for unanimity does not help either. To judge from the Commission communications of 28 June 2006⁴⁷, Council decision-making tends to be sluggish and result in a lowest common denominator. The Commission instances the course taken by proceedings on the European evidence warrant⁴⁸. The Framework Decision on third-pillar data protection seems to face a similar fate⁴⁹. Even the level of implementation of legislation already adopted is described by the Commission as disappointing. What the Commission finds even more disappointing, of course, is that, if Member States fail to deliver, it has no means of taking legal action at the Court of Justice (see also paragraph 26).
22. This picture contrasts with the way in which the third pillar has increasingly become a normal area of European law, as shown by the Pupino judgment⁵⁰. Prechal refers in this connection to the communitarisation of the third pillar⁵¹. Looking at what is in fact being achieved, two points stand out. Firstly, there some inconsistency with the avowed aspirations, which set their sights mainly on mutual recognition, whereas the Framework Decisions enacted are in large part actually concerned with harmonisation of substantive criminal law⁵². Secondly, fulfilment of some of the legislative programme seems to be strongly driven by current events, often in the aftermath of terrorist attacks. Mos here rightly asks whether the European evidence warrant is really a worthwhile instrument, when it might be better first to bring into

⁴⁵ On the SIS in particular, see also paragraphs 55 et seq.

⁴⁶ See the European Council conclusions of 15 and 16 October 1999.

⁴⁷ See the two communications referred to in footnote 3.

⁴⁸ Proposal for a Council Framework Decision on the European evidence warrant for obtaining objects, documents and data for use in proceedings in criminal matters (COM(2003) 688 final).

⁴⁹ The dilatoriness shown by the Council is a constant source of annoyance to the European Parliament's LIBE Committee and in particular the rapporteur, Ms Roure. Within the third pillar, however, the European Parliament has little power.

⁵⁰ Judgment of 16 June 2005 in Case C-105/03, Pupino. That judgment plays an important part in the discussion papers by Barents (see, for instance, section 5, Community nature of third-pillar law) and myself.

⁵¹ S. Prechal, *Juridisch cement voor de Europese Unie* [Legal cement for the European Union], European Law Publishing, Groningen, 2006, p. 22.

⁵² According to EURLEX, there have been eighteen Framework Decisions adopted to date (August 2006). Eleven of them serve in whole and one in part to give effect to Article 31(1)(e) EU.

operation the instruments already adopted but not yet in force⁵³.

3.4. *Background: divergent national law*

23. There are considerable differences between Member States in both substantive and procedural criminal law, with those in criminal procedure being far greater than for substantive criminal law. In substantive criminal law, the principle of double criminality has often acted as an obstacle, but its significance is declining for two reasons. Firstly, Member States are less inclined to cling to the principle of double criminality, which has been dispensed with in the Framework Decision on the European arrest warrant. Secondly, there is a need for criminal law cooperation for offences which do constitute a crime in all Member States, such as those listed in Article 2(2) of that Framework Decision.
24. In procedural criminal law, differences between legal systems give rise to a need for additional measures for information sharing. A recent Commission proposal on exchange of information from criminal records provides a good example⁵⁴. There are considerable differences between Member States in the content of criminal records and in the use which may be made of them, especially outside judicial proceedings. One example coming to mind is whether information from criminal records may be sought for the purposes of a job selection procedure. There is thus a need to establish procedural rules for sharing information from criminal records with another Member State. Among other things, those rules must specify the law applicable to use of that information, the Member State whose authority is responsible for the updating of information and the supervisory arrangements to which data are subject. Apart from differences between national legal systems, of course, the matter is further complicated by the use of different languages, which may make another Member State's criminal records difficult to understand, and different technical systems, which hamper on-line interchange.

3.5. *Prerequisites for democracy and the rule of law: limited powers for the Commission, the European Parliament and the Court of Justice*

25. The EC Treaty makes provision for checks and balances ("institutional equilibrium") which the third pillar lacks. The powers of the institutions supposed to keep the Community interest

⁵³ M.R.B. Mos, *Is het kaderbesluit betreffende het Europees bewijsverkrijgingsbevel doeltreffend?* [Does the Framework Decision on the European evidence warrant serve any useful purpose?], NTER [Netherlands Journal for European Law], 2005, p. 191.

in sight or at any rate represent Europe's citizens (the Commission, the European Parliament and the Court of Justice) are limited. Authority lies with the Council or, in other words, the Member States.

26. In the Commission's case, the limitations are apparent in two ways. Firstly, the Commission shares the right of initiative with the Member States, which in fact often make use of that right. Unlike under the provisions on an area of freedom, security and justice for the first pillar⁵⁵, Member States' right of initiative is permanent in nature. Secondly, infringement proceedings under Article 226 EC are not available, which leaves the Commission toothless when overseeing Member States' implementation. As mentioned earlier, then, the Commission considers the level and pace of implementation generally to be disappointing. It cannot itself really do anything about that, however, except publicly draw Member States' attention to their failure to deliver and, for instance, point to the importance of proper implementation in combating terrorism⁵⁶.
27. Democratic political scrutiny is also inadequate, as the European Parliament has only a consultative role. Article 39 EU requires the Council to consult the European Parliament before taking any binding decisions of the kind referred to in Article 34(2)(b), (c) and (d). This requirement does not apply in concluding an agreement with one or more non-member countries or an international organisation, under Article 38 EU. Strangely enough, the latter provision is precisely the legal basis chosen for the new PNR agreement with the United States of America⁵⁷. The upshot of the finding by the Court of Justice in favour of the European Parliament's applications, with the resultant annulment of the original PNR decisions, is thus to leave the European Parliament completely bypassed. This also applies to the Court itself, as the preliminary ruling procedure laid down in Article 35(1) EU does not seem to be applicable to agreements referred to in Article 38 EU⁵⁸.
28. Turning lastly to the prerequisites for the rule of law, the third pillar is not well served here. The powers of the Court of Justice under Article 35 EU are far more limited than for the first pillar. By mid-2006 only 14 Member States had, under Article 35(2), declared their acceptance of the Court's jurisdiction. Needless to say, within the third pillar there is actually an especially strong need for legal protection, in view of the fundamental civil rights at stake.

⁵⁴ Referred to in footnote 20.

⁵⁵ Title IV in Part Three of the EC Treaty.

⁵⁶ Commission communication of 28 June 2006, Report on the implementation of the Hague programme for 2005 (see footnote 3), paragraph 73.

⁵⁷ For a fuller account, see paragraphs 31 et seq.

⁵⁸ The Dutch language version is not entirely clear on this point, since both Article 34 EU and Article 38 EU use the term "*overeenkomst*" (for convention and agreement respectively). The same applies to the French language version, which in both cases uses the term "*accord*". A brief survey shows that not only the English but also the

The public are entitled to effective protection, whereas here, of all places, the Treaties leave gaps. Another problem, of course, is that the requirement for Member States to implement legislation is incomplete because, as pointed out, there are no infringement proceedings available. This is all the more galling in areas where the European legislature's action is in fact supposed to be protecting the public ⁵⁹.

3.6. *Conclusion*

29. This section show that Title VI of the EU Treaty forms an adequate legal basis on which to bring about cooperation between Member States' police and judicial authorities and thus, in accordance with Article 29 EU, provide citizens with a high level of safety within an area of freedom, security and justice. However, the section also shows that it still cannot be taken for granted that such a level of safety can actually be achieved. Enforcement is carried out by national authorities constrained by their countries' borders, the use made of legal bases is limited (particularly in view of the avowed aspirations), the background of widely differing national criminal law acts as a complicating factor and, last but not least, the Commission, the European Parliament and the Court of Justice enjoy too few powers.

30. In short, there is every reason to raise the issue of the extent to which criminal justice powers should be transferred to the European level. However, there is first a need at least to make provision for suitable (democratic) scrutiny and legal protection. I do not wish to leave the matter there, though. The EU has set its sights high for criminal law cooperation, rightly so. I referred earlier to Barents, who classes the European approach as irreversible. Here we come up against a key problem: the third-pillar legal framework needs to be used, but that legal framework proves inadequate on grounds of democracy and the rule of law.

4. **Demarcation between the first and the third pillars** ⁶⁰

4.1. *PNR judgment*

German and Italian language versions use different terms.

⁵⁹ As the Pupino judgment shows, victims of improper treatment can sometimes duly avail themselves of EU law, even in the event of non-implementation.

⁶⁰ I shall not here consider the demarcation between the second and the third pillars, although the second pillar certainly has a part to play in police and judicial information sharing. The Council Common Positions implementing the 9/11 Security Council Resolutions were based on both the second and the third pillars. See the Council Common Positions of 27 December 2001 on combating terrorism, OJ L 344, 28.12.2001, p. 90, and on

31. It is tempting to give pride of place in this section to the PNR judgment by the Court of Justice⁶¹. That judgment, firstly, concerns sharing of personal data of relevance in investigating criminal offences (admittedly, not between Member States' authorities but between European firms and the US authorities) and, secondly, makes crystal clear the risk of a legal lacuna emerging in between first-pillar and third-pillar powers⁶².
32. Allow me to succumb to that temptation and focus my argument on the second point. What was all the fuss about? The Court ruled on a Council Decision and a Commission Decision requiring European airlines to pass on passenger data to US customs authorities, or even give those authorities access to their databases⁶³, when flying to, from or over the United States of America. For the USA, this system was important on account of the attacks perpetrated on 11 September 2001 and the ensuing war on terrorism. For the European Union, however, the system gave rise to difficulties, as European airlines were subject to national legislation implementing Directive 95/46/EC on the processing of personal data⁶⁴. That Directive allows data to be passed on to a non-member country only under strict conditions. At any rate, being subject to the Directive was the basis for the complex legal construction put in place by the Council and the Commission so that passenger data could be supplied to the Americans.
- Under Article 25 of the Directive, personal data may be supplied to a non-member country only if it ensures a suitable level of protection. For the purposes of that requirement, the Council and the Commission had adopted a package of measures (including an agreement with the USA) to ensure that the passenger data to be passed on to the US authorities were adequately protected there. The dispute before the Court was in large part concerned with whether that package actually provided the protection required by the Directive.
33. Surprisingly, however, the Court held that the Directive did not apply at all and that airlines could supply the data in question to the US authorities without any problem under European law⁶⁵. That outcome has attracted a great deal of comment, with the European Parliament's

the application of specific measures to combat terrorism, OJ L 344, p. 93.

⁶¹ See footnote 8. I was myself involved in that case, acting for the European Data Protection Supervisor.

⁶² On that judgment (and on the lacuna), see E. Guild and E. Brouwer, *The Political Life of Data*, July 2006, downloadable from www.ceps.be.

⁶³ The distinction between (actively) passing on and (passively) allowing access, known in the jargon as "push" and "pull", featured prominently in the case with regard to protection of personal data. If the US authorities have direct access, there can be no check on precisely what data are shared with them, which considerably weakens European passengers' protection.

⁶⁴ Referred to in footnote 28.

⁶⁵ Such supply may in fact be prohibited by national law, as is actually the case in many Member States.

success in the court proceedings (the Decisions were annulled, as it had argued they should be) being described as a "Pyrrhic victory"⁶⁶ or as the European Parliament "shooting itself in the foot"⁶⁷. The Court based its judgment on the first indent of Article 3(2) of the Directive itself. Under that provision, the Directive's scope excluded "the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities provided for by Titles V and VI of the Treaty on European Union, and in any case to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law"⁶⁸. The Court went on to find that processing of passenger data for the US authorities was aimed solely at public security and state activities in areas of criminal law. The processing was not necessary for supply of a service and it was immaterial that the passenger data had originally been collected from passengers by airlines so that they could supply a service, namely air transport to the USA⁶⁹.

34. In view of that broad finding by the Court, it may legitimately be asked to what extent the judgment also means that Article 95 or even the EC Treaty itself does not confer any powers to regulate information sharing for the purposes of state criminal law activities, even in the case of data obtained in the course of a commercial business. I would refer here to the Court's case law, such as the British American Tobacco judgment⁷⁰, on the legal basis for Community acts serving two purposes or involving two components. If "one of these is identifiable as main or predominant, whereas the other is merely incidental, the act must be founded on a sole legal basis, that is, the one required by the main or predominant purpose or component". In spite of that established case-law, I remain unconvinced as to the broad scope of the PNR judgment. For the main purpose and the predominant component of provisions need not coincide. Let me again take the example of the British American Tobacco judgment, which concerned the validity of a Directive primarily designed to combat smoking and thus protect public health. That Directive could nevertheless be based on Article 95 EC, as the provisions laid down related inter alia to trade in cigarettes on the internal market. In short, the main purpose fell outside Article 95 EC, while the predominant component came within it. For the Court, that was sufficient. Had the Court followed a similar line of reasoning in the PNR case, a different result would have been possible. The main purpose of the package

⁶⁶ Including by a number of the European Parliament's own members at its LIBE Committee meeting on 2 June 2006.

⁶⁷ Hirsch Ballin at the annual meeting of the Netherlands Legal Association (NJV) on 9 June 2006 in Maastricht.
⁶⁸ Paragraph 54 of the judgment.

⁶⁹ Paragraphs 55 to 58 of the judgment.

⁷⁰ Judgment given by the Court of Justice on 10 December 2002 in Case C-491/01, British American Tobacco and Imperial Tobacco, ECR I-11453, paragraph 94.

of measures was criminal law enforcement, whereas the predominant component was the treatment of commercial data. However, the Court did not follow that line of reasoning. The answer to the above question would thus seem to be that there are in fact no powers within the first pillar. This also brings to light a lacuna in between the first and the third pillars.

35. The situation is that private airlines are providing assistance with criminal law enforcement. Recent practice shows such assistance also to be imposed in other areas. Firstly, Directive 2006/24/EC⁷¹ requires telecommunications companies and Internet service providers to retain data generated or processed by them, for use in detecting, investigating and prosecuting serious crime. Secondly, in June 2006 Europeans were startled to learn that US authorities apparently have access to all manner of European payment data held by SWIFT in Belgium (and possibly also in the Netherlands)⁷². Thirdly, there seems to be a general tendency increasingly to involve the business world in tackling serious crime, with the Commission work programme for 2006⁷³ announcing an EU action plan for public-private partnership in combating crime and terrorism.
36. Such activities by private firms in connection with the performance of criminal law tasks cannot simply be brought within the scope of the third pillar and hence covered by action by the European Union legislature under Article 34 EU. The only question is whether requirements for private firms to provide police and judicial authorities with access to their databases, or to retain data for those authorities, are measures concerning closer cooperation between Member States' authorities, as referred to in Article 29 EU. This is an even more moot question where firms prove to be processing or retaining data for authorities in a non-member country, such as the USA.
37. The question could in fact arguably, in my view, be answered in the affirmative. As I maintained earlier, Articles 29 to 32 EU provide a broad legal basis. Third-pillar powers to impose rules on private firms' activities with regard to law enforcement could also be based

⁷¹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, p. 54. See also paragraphs 39 and 44. On that Directive, see too: De Hert et al., *Iedereen wordt er slechter van* [Everyone will be hurt], NJB [Netherlands Legal Journal] (2006) No 24, p. 1318.

⁷² Society for Worldwide Interbank Financial Telecommunications (SWIFT). See the European Parliament Resolution of 6 July 2006 on the interception of bank transfer data from the SWIFT system by the US secret services (www.europarl.europa.eu, under "Texts adopted by Parliament").

⁷³ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unlocking Europe's full potential: Commission legislative and work programme for 2006 (COM(2005) 531 final).

on a line of reasoning mirroring that followed by the Court of Justice in its judgment in the case between the Commission and the Council concerning the environment and criminal law⁷⁴. In paragraphs 47 and 48 of that judgment the Court held that:

- "As a general rule, neither criminal law nor the rules of criminal procedure fall within the Community's competence".
- This point "does not prevent the Community legislature, when the application of effective, proportionate and dissuasive criminal penalties by the competent national authorities is an essential measure for combating serious environmental offences, from taking measures which relate to the criminal law of the Member States which it considers necessary in order to ensure that the rules which it lays down on environmental protection are fully effective".

38. For private firms' activities, the reasoning might run as follows:

- As a general rule, private firms' activities do not fall within the EU legislature's third-pillar powers.
- However, this point does not prevent that legislature, where this is essential for closer cooperation between Member States' authorities, as referred to in Article 29 EU, from imposing on private firms any requirements necessary for achievement of the objectives in Article 29 EU (or, to put it another way, necessary for the effectiveness of that cooperation).

Such a line of reasoning could largely plug the gap brought about by the PNR judgment, leaving just the special situation in which European firms lend a helping hand with criminal law enforcement in a non-member country. I shall not go on to consider that special situation, which raises extremely interesting issues with regard to the principle of territoriality and to the global nature of terrorism and of action to combat it, issues which go beyond the bounds of this discussion paper.

4.2. *Retention of data*

39. It is unclear more generally where the border between the first and the third pillars lies. There was a clash between interested parties on this point in adopting Directive 2006/24/EC on the retention of data⁷⁵. The first issue raised was within which pillar those provisions should be enacted. A Directive was opted for, despite an earlier initiative by four Member States to

⁷⁴ Judgment of 13 September 2005 in Case C-176/03, *Commission v. Council*, ECR I-7879.

⁷⁵ See also paragraph 35 and footnote 71.

have the matter dealt with in a Framework Decision. One of those four Member States, Ireland, did not go along with that legal basis and applied to the Court of Justice for annulment of the Directive⁷⁶. The second issue raised was whether the aspects to be covered could or should all be regulated within the same pillar. Data are to be retained by private firms but subsequently used by police and judicial authorities. From a data protection angle, it is important to impose restrictions not only on retention of but also on access to and use of such sensitive data in privacy terms. The European Data Protection Supervisor therefore argued in his opinion⁷⁷ that both aspects were inseparably linked and that, if the Community legislature were not empowered to impose rules on access and use, it would be unable to fulfil its obligation under Article 6 EU to respect fundamental rights. Failing such powers, the Directive could not ensure that data retained for the purpose of combating serious crime were not also used for other, less weighty purposes. Examples coming to mind here include not just combating minor criminal or other offences but also use for commercial purposes. Needless to say, this could encroach upon the right to privacy, as protected by Article 8 of the ECHR. That line of argument was not followed by the Community legislature, although the final version of the Directive did include a rather generally worded provision on access to traffic data⁷⁸. That provision is in fact not devoid of significance, since it allows access only in specific cases, lest law-enforcement authorities engage in non-specific searching of records. It also includes a reference to the ECHR. Use of data is not regulated.

4.3. Conclusion

40. This section has brought out one of the possible implications of the PNR judgment. Between the first and the third pillars, there seems to be a borderline area in which, unintentionally to my mind, the European Union is left with no powers to act. The third pillar is concerned with cooperation between Member States' authorities, the key point being between *whom* cooperation is engaged in. The PNR judgment applies a different criterion, making the purpose of a particular act (*why*) the determining point. It may be possible to plug that gap by means of the line of reasoning set out in paragraph 38, mirroring the judgment concerning the environment and criminal law⁷⁹. That judgment also brings to light an area in which there seem to be overlapping powers under the first *and* the third pillars. Within the first pillar it is

⁷⁶ Application of 5 July 2006, Ireland v. Council and European Parliament (not yet published in the Official Journal).

⁷⁷ Opinion of 26 September 2005, OJ C 298, p. 1, paragraph 40.

⁷⁸ Article 4 of the Directive.

⁷⁹ Referred to in footnote 74.

possible, under specified conditions, to impose penalties, which is of course also possible, under different conditions, within the third pillar. I would lastly now point here to SIS II, which throws up another demarcation problem. That system is to share information from both the first pillar and the third pillar. The difference in legal framework has implications in law, but it will not always be clear within which legal framework a particular activity comes.

5. Means of improving information sharing

5.1. *Mutual recognition as a basis for cooperation*

41. Mutual recognition of criminal justice systems forms the basis for cooperation between Member States' authorities. Mutual recognition presupposes mutual trust. This can be seen, for instance, from the case law concerning the double-jeopardy bar, such as the Gözütok and Brügge judgment referred to earlier⁸⁰. Should a criminal case in the Netherlands be settled with the public prosecution service, without going to court, the same occurrence cannot be judged in another Member State, even if its criminal justice system makes no provision for out-of-court settlement in respect of such offences. In the third pillar, too, the legislature uses mutual recognition as a basis, drawing on examples from the internal market⁸¹. On its own, however, mutual recognition does not bring improved information sharing. Further legislative action by the European Union is required and is indeed being taken.

5.2. *Minimum-level harmonisation of ground rules: proposal for a Framework Decision on data protection*

What public interests?

42. Mutual recognition presupposes minimum-level harmonisation of ground rules, so that the effectiveness of cooperation is not undermined by excessive differences between Member States⁸². Within the first pillar, harmonisation of ground rules normally involves the differing public interests referred to in Article 30 EC or recognised by the Court of Justice in its case-law concerning the rule of reason⁸³. Within the third pillar, the range of interests to be protected is far more limited.

⁸⁰ Referred to in footnote 13. The line taken in that judgment has been confirmed in various subsequent rulings by the Court of Justice.

⁸¹ On this, see Barents at various points in his discussion paper.

⁸² For a more extensive discussion of this point, see Barents, paragraph 19.

⁸³ See Kapteyn/VerLoren van Themaat, *Het recht van de Europese Unie en de Europese Gemeenschappen* [The law of the European Union and the European Communities], Sixth Edition, pp. 559 et seq.

43. Firstly, Member States are, of course, required to respect fundamental rights, as laid down in the ECHR and in other human rights conventions ratified by all Member States. For the EU institutions, that obligation is entailed by Article 6 EU. Those obligations for Member States and for the EU cannot be infringed in secondary legislation. Article 1(3) of the Framework Decision on the arrest warrant ⁸⁴ explicitly, though no doubt unnecessarily, stipulates as much for the matters dealt with in that Framework Decision.
44. Secondly, effective law enforcement is in fact also to be classed as a substantial public interest warranting harmonisation. In this way, third-pillar cooperation differs from the customary weighing of interests to be performed in the first pillar as between market interests and specific public interests. Third-pillar action involves a balance *between* public interests. In her article, Weyembergh finds fault with the EU legislature for a lack of even-handedness in practising harmonisation. Adducing various examples, she argues that the main thrust of criminal law harmonisation in the European Union is punitive ⁸⁵. In a nutshell, she is arguing that, in the framing of legislation, the instrumental function of criminal justice gains the upper hand over its safeguard function. That argument is borne out by the process of adoption of Directive 2006/24/EC (retention of data) ⁸⁶.
Swift enactment of an instrument serving (in part) to combat terrorism took precedence over and seemed more important than a balanced outcome incorporating privacy safeguards ⁸⁷. On the other hand, the proposal for a Framework Decision on data protection, designed precisely to provide safeguards, is not being dealt with by the Council as a matter of similar urgency, even though its importance is constantly pointed out by all concerned ⁸⁸.
45. Thirdly, Article 30(1)(b) EU makes provision for very specific harmonisation of ground rules, in that measures for the collection, storage, processing, analysis and exchange of information may be adopted only subject to appropriate provisions on protection of personal data. The question is, of course, to what extent the EU legislature is actually complying with that. The Commission proposal for a Framework Decision on data protection is, admittedly, under discussion within the Council. However, the enactment of various legal instruments

⁸⁴ Referred to in footnote 15. On that provision, see also paragraph 12.

⁸⁵ For instance, by imposing not maximum sentences but minimum levels for maximum sentences (*op. cit.*, p. 1588). She refers to wielding the sword rather than the shield (protection from the authorities).

⁸⁶ See footnote 71; strictly speaking, of course, this is not a third-pillar decision.

⁸⁷ The Directive was adopted extremely quickly. Political decisions were reached in the Council and the European Parliament within three months following submission of the Commission proposal. Significantly, the LIBE Committee's report, regarded as being more balanced, was not put to a vote in the full house of the European Parliament. This prompted the rapporteur, Mr Alvaro, a German Liberal, to vote against the proposal (see also De Hert et al., referred to in footnote 71).

concerned with the collection (etc.) of information has not been made conditional upon the Council's adoption of that Framework Decision ⁸⁹.

Framework Decision in context

46. Let me begin by outlining the setting in which the Framework Decision on data protection is to be adopted. Partly as a result of the various (proposed) European provisions to facilitate information sharing, themselves in turn resulting from the removal of internal borders, increasing amounts of information are being compiled and shared. This then has further implications. On the one hand, there is a special need for a high level of data protection within the third pillar, not least because of the sensitive nature of data compiled and shared for criminal law enforcement purposes. On the other hand, that is exactly where data protection comes under great strain, with any information available also needing to be exploitable. For the sake of effective action, police and judicial authorities will want to have easy access to personal data and to be able to combine them with other data or with data on other people.
47. That strain is particularly evident as regards the principle of purpose limitation, meaning in short that personal data may be used only for the purpose for which they have been collected. The Commission has submitted a proposal for a special legal instrument to allow access, for law-enforcement purposes, to data entered in the (first-pillar) Visa Information System and compiled with the aim of establishing a common visa policy ⁹⁰. That information system is not a law-enforcement tool, but is still to be usable for the purpose. At any rate, that is the intended effect of the Commission proposal. It should be pointed out, though, that the Commission proposal would not give police and judicial authorities unlimited access. Access would be allowed only in connection with serious crime and would not be provided routinely, just in specific cases. Another example is the increasing part played by biometric data, such as DNA and fingerprints, in criminal justice. There is much law-enforcement appeal in large-scale collection and use of such data, but this involves considerable risks for data subjects. As regards DNA, mention should be made of the difficulty of correctly interpreting

⁸⁸ See also paragraph 21.

⁸⁹ Nor is the Council willing to do so. As Statewatch has pointed out: "The Council is not prepared to wait for the proposed Framework Decision on the protection of personal data in police and judicial matters to be in place before going ahead" (www.statewatch.org/news/2006/aug/01eu-convictions.htm). That point was made with regard to the Framework Decision on exchange of information from criminal records.

⁹⁰ Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final). See also the European Data Protection Supervisor's opinion, OJ C 97, 2006, p. 6.

DNA data⁹¹ and the necessity and difficulty of confining data collection to DNA material from which no sensitive details of individuals, such as hereditary characteristics, can be derived⁹².

48. To conclude, the need for harmonisation of ground rules, which must of course make balanced allowance for the various public interests involved, thus seems also on substantive grounds to be a *sine qua non* for information sharing based on mutual recognition.

Article 1(2) of the Commission proposal

49. Article 1(2) of the Commission proposal is a remarkable provision, reading as follows:

"Member States shall ensure that the disclosure of personal data to the competent authorities of other Member States is neither restricted nor prohibited for reasons connected with the protection of personal data as provided for in this Framework Decision". That provision is clearly based on the mutual recognition clauses customarily found in internal market legislation, such as the one in the Directive on electronic commerce⁹³. This stipulates that Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide certain services from another Member State.

50. It would seem that, in drawing up the proposed Framework Decision, the Commission meant Article 1(2) to make for unhindered exchange of data between Member States' competent authorities⁹⁴. In the European Parliament, that provision was brought up by Ms Buitenweg⁹⁵, who wondered whether it did not breach protection of personal data. As such provisions in internal market legislation reflect the home-country principle⁹⁶ (ensuring that services meeting the requirements in the supplier's country of origin are allowed in), Article 1(2) of the Commission proposal seems to have a mirror-image effect. The supply of

⁹¹ See, for instance, the letter of 13 September 2005 from the Minister for Justice concerning the Schiedammer Park murder (*Kamerstukken* [Parliamentary papers] 2004-2005, 29 800 VI, No 168).

⁹² See the European Data Protection Supervisor's opinion on the Framework Decision on the exchange of information under the principle of availability (referred to in footnote 10), paragraphs 55-64.

⁹³ Article 3(2) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce"), OJ L 178, p. 1. On this, see also B.J. Drijber, *De richtlijn elektronische handel op de snijtafel* [The Electronic Commerce Directive dissected], SEW [Socio-Economic Legislation, a European and economic law journal] (2001), pp. 122-138.

⁹⁴ The explanatory memorandum accompanying the proposal points to that intention (under "Legal basis"), but does not give any explanation of Article 1(2).

⁹⁵ During public discussion of the Commission proposal in the LIBE Committee on 12 June 2006.

⁹⁶ I shall not go here into the conceptual distinction between the home-country principle and mutual recognition. On that point, see inter alia H. Hijmans, *De Europese Unie, verdwijnende grenzen en elektronische diensten* [The European Union, disappearing borders and electronic services], SEW (2004), p. 52.

data to other Member States' authorities cannot be refused if the receiving Member State's data protection requirements are fulfilled. This applies even where the source Member State imposes more stringent data protection rules and would not allow a particular use of data under its own national legislation. The question raised by Ms Buitenweg is thus a pertinent one⁹⁷.

5.3. *Requirement for active cooperation as part of the Framework Decision on the exchange of information under the principle of availability*

51. There are a number of legal instruments requiring Member States' authorities to cooperate actively across the board. This section focuses on the putting into practice of the principle of availability in a Framework Decision⁹⁸. However, there are other instruments designed to make information available to authorities in other Member States, such as the proposed provisions on exchange of information from criminal records⁹⁹.
52. The Hague programme ambitiously presents the principle of availability as an innovative approach needed in order to underpin an area of freedom, security and justice. Police information sharing no longer stops at EU internal borders. Free sharing of information between authorities is an important step in tackling territorial restrictions in combating crime, as a result of internal borders remaining in place for investigation. Availability is more than mutual recognition of national legislation. Member States' authorities have to provide active cooperation. They must firstly ensure that other Member States' authorities actually have access, preferably (according to the Commission proposal for a Framework Decision) on line. To put it rather more specifically, if police information is accessible on line to another police force within a Member State, other Member States' forces are also to be given access. As this is protected information, there will be a need, without going into the technical details, to interconnect police networks. If information is not available on line within a Member State, it will have to ensure by other means that authorities from another Member State can ascertain whether specific relevant information, e.g. on a particular suspect, is available from a police force¹⁰⁰. What counts as being available, though, is not clearly defined. Does the principle

⁹⁷ The practical significance of this point has in fact diminished, as it seems to be the Council's intention to delete the provisions in question (at any rate, that is what I gather from the Council working party's non-public reports).

⁹⁸ See footnote 10.

⁹⁹ See paragraph 24 and footnote 20.

¹⁰⁰ The Commission proposal requires Member States to provide index data which can be consulted using a hit/no-hit system. In the event of a hit, e.g. showing a particular individual to be known to the police, the requesting Member State can then ask for further information.

of availability , for instance, relate only to data included in police records (on line or otherwise) or does it also apply to information not held by the police but to which they do have direct access (such as telecommunications data ¹⁰¹)?

53. Availability, of course, presupposes strong mutual trust. This is most obvious where other Member States' authorities have direct access to information. In such cases, source Member States lose control of access, which is available automatically and so cannot normally be refused, and of subsequent use of data. The Commission proposal is in fact internally inconsistent on this point. It allows a source Member State to require prior authorisation for the provision of information and to refuse to provide information, on specified grounds ¹⁰². It is unclear how those powers are to be exercised where other Member States' authorities have direct access. As pointed out, the Member State has no control, at any rate not *ex ante*. Technology does make it possible to keep a record of which foreign authorities have obtained access to particular information.
54. Active cooperation between Member States is to result in a European information-sharing network. That network will be available to authorities in a number of Member States, normally without any involvement of European bodies. Oversight of that network, too, can only be carried out by Member States' authorities. This applies to supervision by a data watchdog, such as the Netherlands' Data Protection Authority, and to oversight by the courts ¹⁰³. Oversight is therefore confined to action by a country's own police forces within that network. Effective protection of individuals concerned is thus not necessarily ensured. Information is to be shared and will hence be available in a number of Member States. There will thus be a need for additional provisions to specify the law applicable and assign responsibilities for management of information within the network, including removal of information, and for (judicial) oversight of this. Such additional provisions are in fact all the more necessary in that the proposal allows even potentially very sensitive information, such as DNA and fingerprints, to be shared. The Commission proposal expressly mentions those types of data. I have already alluded earlier to the special risks involved in sharing DNA data.

¹⁰¹ As referred to in Directive 2006/24/EC (see footnote 71). Telecommunications data are explicitly included in Annex II to the Commission proposal.

¹⁰² Articles 13 and 14 of the Commission proposal.

¹⁰³ The possibility of national courts seeking preliminary rulings on the interpretation of the Framework Decision makes no difference in this respect.

5.4. *Partly centralised technical structures to support information sharing between Member States: the major information systems, particularly SIS II*

55. One of the types of action taken by the EU legislature is the establishment of major Europe-wide information system to support information sharing between Member States ¹⁰⁴. The SIS is regarded as a necessary tool in doing away with internal borders. A second-generation system, including improved technical facilities, is required if internal borders are also to be removed for the new Member States ¹⁰⁵. The existing system is not equipped for that purpose. The SIS calls for an even more active form of information sharing between Member States than for the principle of availability. Member States have to ensure that data are available, in accordance with certain protocols, for automatic searching by other Member States' authorities. This includes, for instance, data on individuals to be arrested and data on aliens to be refused entry into the area, as they pose a threat to public policy and public security (or national security) ¹⁰⁶.
56. It is a feature of all the existing or planned major information systems within the area of freedom, security and justice that they do not create a separate European structure. They comprise national sections, run by Member States, and a central section. Member States are responsible for supplying data, keeping those data up to date and erasing them. The central section is mainly necessary in order to ensure that data can actually be exchanged between Member States. In the SIS, the central section is mostly regarded as a technical support function maintaining a central database and providing the communications infrastructure for the network of national authorities ¹⁰⁷. Management of SIS II is to be entrusted to a central management authority. Despite its limited role, the central section is bound to entail a complicated apportionment of responsibility and supervision. The problem is even more acute in that the SIS comes partly within the first pillar and partly within the third pillar. The other (planned) systems are somewhat simpler. They come entirely within either the first pillar (Eurodac and the Visa Information System) or the third pillar (Europol and Eurojust).

¹⁰⁴ Those systems are referred to in paragraph 20.

¹⁰⁵ EU enlargement is consistently given as the main reason why SIS II needs to be introduced quickly; see, for instance, the conclusions of and press release for the JHA Council meeting on 24 July 2006.

¹⁰⁶ See Title IV of the Schengen Convention.

¹⁰⁷ Article 92(3) of the Schengen Convention defines the central section merely as a technical support function. The proposals for SIS II (see Article 4 of the proposals referred to in footnote 11) seem to posit a slightly broader function for the central section.

57. The proposals providing a legal framework for SIS II ¹⁰⁸ point out that the fact that the legislative basis consists of separate instruments does not affect the principle that SIS II constitutes a single information system, which should operate as such. Watching over that unified system, however, will not always be easy. For instance, data protection, an important subject with the SIS being largely a collection of personal data, will be subject to differing arrangements. The legal framework for the SIS lays down some rules in that area and there are also general arrangements applying. However, the general arrangements applicable depend on the level of responsibility, national or central, and on the pillar within which a given activity comes. The central authority's action is subject to the arrangements laid down, under Article 286 EC, in Regulation (EC) No 45/2001 ¹⁰⁹. Where that central authority takes action with regard to personal data compiled within the third pillar, however, it is open to question whether the Regulation can be applied just so. Action by Member States' authorities within the first pillar, such as supplying data with a view to refusal of entry into and residence in the EU by nationals of non-member countries, is subject to the arrangements in Directive 95/46/EC ¹¹⁰. Action within the third pillar is not covered by any arrangements under EU law ¹¹¹. All of this gives rise to a rather opaque system. For the various supervisors having to deal with SIS II, this will presumably be manageable; the system does also make provision for coordination mechanisms. The situation would be different should betrayed members of the public want someone to turn to if they think their data have been wrongfully entered in the SIS, or if their data in the SIS have been inadequately protected and as a result disclosed to third parties. Not to mention the case behind the *Commission v. Spain* judgment ¹¹², nor the limited powers of the Court of Justice within the third pillar and also under Article 68 EC.

5.5. *Conclusion*

58. In paragraph 2, I asked whether the EU can live up to its aspirations within the existing Treaties. To this end, the legal instruments available need to help step up information sharing, based on mutual trust, with the fullest possible attention being paid to the problems pointed out within the third pillar (see paragraphs 29 and 30). Also to be addressed are the implications of the demarcation between the first and the third pillars, especially where

¹⁰⁸ See the fourth recital in the proposals referred to in footnote 11.

¹⁰⁹ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, p. 1.

¹¹⁰ Referred to in footnote 28.

¹¹¹ This may change with the Framework Decision on third-pillar data protection.

¹¹² See paragraph 11.

private parties are involved in criminal law enforcement.

59. For a start, this calls for harmonisation of ground rules, based on balancing the various public interests involved, as borne out by the context in which the proposal for a Framework Decision on data protection is being discussed. Pressure is constantly being exerted to place the emphasis on the instrumental function of criminal justice rather than its safeguard function.
60. The principle of availability is in itself a fine means of actually achieving cooperation between Member States' authorities and thus making further headway in the process of European integration, as also required in response to transnational crime. As can be seen from the description of the system proposed, however, practical implementation of the principle of availability raises many issues. It is thus open to question whether it is not too soon to implement that principle ¹¹³ and whether a number of prerequisites do not first need to be fulfilled. I am not just referring here to a harmonised level of data protection. It is perhaps more important still for a system of availability to be accompanied by legal infrastructure allowing controlled, proportionate information sharing. That infrastructure must in any event provide clarity as to the law applicable, make oversight possible, even where information is shared between a number of Member States, and establish suitable legal remedies for data subjects.
61. What about SIS II? The European legislature can get by, although the result is not entirely satisfactory, given the ambiguities resulting from the pillar structure. What is more, although this also stems from the present state of European integration, SIS II brings out Member States' desire as far as possible to retain powers themselves. It is a major European information system in which the main responsibilities lie with the Member States. I have already pointed to the pressure for personal data collected to be used for other purposes as well and to the increasing significance of biometric data. It is also on account of those risks that data subjects must be able to avail themselves of a legal system in which responsibilities and oversight are clearly regulated.

6. Ways of getting away from the third pillar

6.1. Initiatives outside the EU framework, such as the Prüm Convention

62. On 27 May 2005 seven Member States signed a Convention ¹¹⁴ on various police cooperation

¹¹³ In substance, not procedure, the Prüm Convention might just turn out to be a more suitable instrument here.

¹¹⁴ Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed in Prüm (Germany) on 27 May 2005.

matters¹¹⁵. Although that Convention governs matters of prime relevance to criminal law cooperation, the Member States taking the lead opted for a method circumventing the EU Treaty. The Convention is often compared with the 1985 Schengen Agreement and the 1990 Schengen Convention. The reasons are plain to see: like Schengen, Prüm is a village near where three countries meet (in this case, Germany, Luxembourg and Belgium), much the same countries are involved¹¹⁶, the subject-matter is similar and there is a close link with cooperation within the EU (or, in those days, the EEC).

63. There are, however, important differences. There *is* now a European legal framework within which to regulate the matters concerned and there were actual plans to make use of it for the (main) matters covered by the Prüm Convention. More specifically, the Convention overlaps to a considerable extent with the principle of availability and even clashes with it in significant respects. The Member States concerned nevertheless opted for a multilateral treaty enabling them to sidestep the thorny path of third-pillar legislation by unanimous agreement. That option unquestionably has its drawbacks: multilateral cooperation between a limited number of Member States sits ill with the idea of a single area of freedom, security and justice; the limited part played by the Commission, the European Parliament and the Court of Justice in the third pillar is replaced by an arrangement under which those institutions play no part whatever; moreover, the other Member States are denied any chance of a say in the choice of rules. They can only choose between participating and not participating. The question now is whether those drawbacks are also at variance with Member States' obligations under the EU Treaty. The first point to be considered in replying to that question is the relationship between the Prüm Convention and the principle of availability.

Content of the Prüm Convention and principle of availability

64. The Prüm Convention covers a wide range of matters. At the heart of it, however, lies cross-border sharing of certain personal data, namely DNA profiles and fingerprints¹¹⁷. Broadly speaking, the system in Articles 2 et seq. of the Convention amounts to an undertaking by the contracting states to open and keep national DNA analysis files for the investigation of criminal offences. Other states' authorities have access to only a small part of

¹¹⁵ For a more extensive account of the Prüm Convention, see Balzacq, Bigo, Carrera and Guild, *Security and the Two-Level Game: the Treaty of Prüm, the EU and the Management of Threats*, Centre for European Policy Studies Working Document No 234 (January 2006), downloadable from www.ceps.be.

¹¹⁶ Prüm was reportedly in the first place an initiative by the same Member States as for the Schengen process (Germany, France and the Benelux countries). When France soon dropped out, Austria became involved; shortly before the signing, France and also Spain came (back) on board.

¹¹⁷ I shall not go on to consider the third type of data, concerning vehicle registration.

the DNA profiles held in those files, namely reference data which can be compared with profiles in the enquiring country in order to ascertain whether profiles match up, but from which an individual cannot be identified. Should an enquiry show that profiles match up, the enquiring country can ask for more information. Whether that further information is in fact forthcoming will then be governed by national law. A similar system applies for fingerprints. However, those systems run counter to the very essence of the principle of availability, which requires all national information available also to be directly accessible *on line* to other Member States' authorities. As has been pointed out, the principle of availability is one of the key points in the Hague programme, approved by the European Council in November 2004. In May 2005 seven Member States then went on in a multilateral treaty to establish a different system, although it should be noted that the Commission proposal to implement the principle of availability had not yet been submitted at the time.

Is the Prüm Convention in breach of EU Treaty obligations?

65. Three closely interrelated arguments can be put forward to show that the Prüm Convention is not just undesirable but also possibly incompatible with Treaty obligations.
66. Firstly, it can be argued that the Prüm Convention conflicts with the scheme of the EU Treaty itself, inasmuch as the latter is aimed at establishing an area of freedom, security and justice without internal borders. I would make the following points here:
- the third-pillar provisions are more than a framework for intergovernmental cooperation. They set the course for the EU's development and thus leave Member States no leeway to make those objectives harder to achieve. Criminal law cooperation under the Prüm Convention does not bring about a single area, but rather reinforces internal borders within the area, as between participating and non-participating countries;
 - there is a trend, as borne out by the Pupino judgment, towards communitarisation of the third pillar. Member States' first-pillar obligations are to an increasing extent applicable within the third pillar. For this reason, too, cooperation does not come with no strings attached ¹¹⁸;
 - enhanced cooperation is subject to substantive requirements. It must "have the aim of enabling the Union to develop more rapidly into an area of freedom, security and justice" (Article 40 EU) and be "aimed at furthering the objectives of the Union and of the Community, at protecting and serving their interests and at reinforcing their process

¹¹⁸ The self-evidence of this point is also averred, for instance, by G.J.M. Corstens, *Eerste strafarrest van het Hof van Justitie over een kaderbesluit* [First criminal law judgment by the Court of Justice concerning a Framework

of integration" (Article 43 EU);

- Article 40a EU makes provision for a Council decision (so that the other Member States are automatically involved), with the involvement of the Commission and the European Parliament. The Court of Justice can also provide oversight (Article 40(3) EU);
- Article 43a EU has a bearing on the matter as well. It stipulates that enhanced cooperation may be undertaken only when it has been established within the Council that the objectives of such cooperation cannot be attained within a reasonable period by applying the relevant provisions of the Treaties. In the case of the Prüm Convention, the Council was not brought in beforehand.

This is not to say that the system under Title VI EU prevents two or more Member States from reaching agreements on police cooperation. Title VI does not confer on the EU any exclusive powers preventing bilateral cooperation between a limited number of Member States, not even as a result of the provisions on enhanced cooperation. The third pillar does, however, limit Member States' competence. I would argue that the limit has here been overstepped.

67. Secondly, the principle of sincere cooperation can be said to have been infringed in that the Prüm Convention hampers implementation of the principle of availability. In accordance with the Pupino judgment ¹¹⁹, that principle is fully applicable within the third pillar. It may, of course, be objected that, while this shows the undesirability of concluding the Prüm Convention from an EU law perspective, it can by no means be concluded that the Member States concerned are in breach of any legal obligation. The principle of availability is laid down in an EU programme, but that does not make it part of the *acquis*. Moreover, Member States retain some latitude until such time as a European measure becomes applicable within their national law. Even in the case of a Directive already adopted ¹²⁰, in accordance with the Inter-Environnement Wallonie judgment ¹²¹, they need only, during the period before giving effect to the Directive, refrain from taking any national measures liable to seriously compromise achievement of the result prescribed by it.
68. Yet it may well be argued that the Member States concerned are indeed in breach of the principle of sincere cooperation. They could have acted differently and made use of the scope afforded by the EU Treaty: they could have asked the Commission to submit a proposal for a Framework Decision under Article 34 EU, they could have put forward such a proposal themselves or they could have dealt with the matter under the procedures laid down in the

Decision], NTER [Netherlands Journal for European Law] (2006), No 1/2, pp. 24-28.

¹¹⁹ Paragraphs 41 and 42 of the judgment. On sincere cooperation, see also Barents, paragraphs 46-48.

¹²⁰ In my opinion, the same applies to a Framework Decision.

¹²¹ Judgment given by the Court of Justice on 18 December 1997 in Case C-129/96, Inter-Environnement Wallonie,

EU Treaty for enhanced cooperation. The contracting states were doubtless aware of this, in view of the preamble to the Convention. They regard the Prüm Convention as playing a pioneering role in cooperation and information sharing and seek eventually to have its provisions brought within the framework of the European Union.

69. Thirdly, it is open to question whether Member States are in fact empowered to conclude international agreements with the content of the Prüm Convention in this area. I would argue here as follows:

- the communitarisation of the third pillar, as borne out by the Pupino judgment, also has implications for the application of Community-law principles not explicitly addressed in that judgment. The Court of Justice based its findings primarily on the point that the EU must be able to carry out its tasks effectively in the third pillar. That point also applies to other Community-law principles¹²²;
- reference may thus also be made to the case-law on Member States' powers to conclude international agreements¹²³;
- it is immaterial here that the Prüm Convention is an agreement between Member States and not an agreement with one or more non-member countries;
- the Court of Justice has acknowledged that Member States cannot conclude agreements which are incompatible with the common market and with uniform application of Community law. Whether that is the case has to be seen from a specific analysis of the relationship between the agreement and the Community law in force. The proper functioning of the system established by Community law is a key factor here¹²⁴;
- application of that case law, *mutatis mutandis*, to the third pillar leads to the conclusion that the Prüm Convention impedes the proper functioning of the system established by Articles 29 to 32 EU and so Member States were not allowed to conclude agreement.

This line of argument is, admittedly, open to dispute, being based on questionable premises. However that may be, the argument should make for an interesting debate in the Netherlands Association for European Law.

70. The conclusion to emerge from all this is that the Prüm Convention compromises the objectives of the EU Treaty, for a variety of reasons set out above, and also runs counter to the principle of sincere cooperation. The question then arises of what legal effect that finding

ECR I-7411, paragraph 4.

¹²² See also M. Fletcher, Extending "indirect effect" to the third pillar: the significance of Pupino?, *European Law Review*, 2005, pp. 862-877.

¹²³ The Court's case law – the AETR judgment of 31 March 1971 (Case 22/70, ECR 263) and subsequent rulings – is summarised in Opinion 1/03, given by the Court of Justice on 7 February 2006, paragraphs 114-133.

has. The Commission cannot take the matter to the Court of Justice, as Treaty infringement proceedings under Article 226 EC are not available within the third pillar.

6.2. *Bridging clause*

71. In the absence of a Constitutional Treaty, use of the bridging clause in Article 42 EU could provide an alternative way of making criminal law cooperation decision-making more effective, especially if application of Article 42 EU were accompanied by the introduction of qualified-majority decision-making¹²⁵. The Commission is now pushing hard for a transfer of powers from the third to the first pillar. This is remarkable because that possibility was until recently not taken very seriously¹²⁶.

In parallel with that, the Commission is also proposing extension of the powers of the Court of Justice under Title VI in Part Three of the EC Treaty, by making use of the clause in the second indent of Article 67(2) EC¹²⁷. There are good reasons for resorting to the bridging clause. Many of those reasons relate to shortcomings in third-pillar cooperation, as described at various points in this discussion paper. The Prüm Convention, or at any rate its undesirability, may, though, provide the best reason. Member States evidently do not consider themselves tied to the framework for police and judicial cooperation, as established in the EU Treaty's third pillar. A transfer of powers to the first pillar, coupled with majority decision-making, on the one hand, could reduce Member States' needs and, on the other, would enable action to be taken against Member States. In short, there is every reason to press for use of the bridging clause.

7. **Where does this leave us?**

To sum up, let me draw a few conclusions in the form of points put to the meeting of the Netherlands Association for European Law:

- (1) Information sharing presupposes (mutual) trust. The real challenge for the EU legislature lies in eliminating the distrust harboured for good reasons, or at any rate reducing it to acceptable proportions.
- (2) Articles 29 to 32 EU confer general powers to legislate as a means of fostering mutual trust

¹²⁴ See, in particular, paragraphs 122, 124 and 128 of Opinion 1/03.

¹²⁵ On the nature of the bridging clause, see Barents, paragraph 34.

¹²⁶ Weyembergh, *op. cit.*, p. 1588, for instance, states simply that "such a decision is very unlikely to be adopted by Council".

¹²⁷ See the relevant Commission communication, forming part of the package of 28 June 2006, referred to in footnote 3.

and for the purposes of the objective in the first paragraph of Article 29.

- (3) The European approach should help step up information sharing, based on mutual trust, with the fullest possible attention being paid to third-pillar inadequacies, such as the lack of suitable (democratic) scrutiny and legal protection. In spite of those inadequacies, criminal law powers will increasingly be transferred to a European level.
- (4) As a result of the PNR judgment, there is, between the first and the third pillars, a borderline area in which there may be no powers for action by the European Union.
- (5) Ground rules need to be harmonised on the basis of a balance between the various public interests involved.
- (6) The principle of availability is a premature move towards greater European integration. It is first necessary to put in place legal infrastructure allowing controlled, proportionate information sharing.
- (7) The public are entitled to a legal system in which responsibilities and oversight are clearly regulated. The proposed SIS II does not fulfil those requirements.
- (8) The Prüm Convention is incompatible with Member States' EU Treaty obligations. It conflicts with the scheme of the Treaty itself, it infringes the principle of sincere cooperation and, what is more, Member States cannot unilaterally conclude international agreements in this area.
- (9) There is every reason to urge Member States to make use of the bridging clause. The Prüm Convention, or at any rate its undesirability, best demonstrates the pressing need to resort to the clause.
