OPINION OF ADVOCATE GENERAL
BOT
delivered on 14 October 2008 [1](1)

Case C-301/06

Ireland
v
European Parliament,
Council of the European Union

(Action for annulment – Directive 2006/24/EC – Electronic communications – Retention of data – Choice of legal basis – Article 95 EC – Title VI of the EU Treaty)

1. Disputes concerning the choice of legal basis have recently given rise to a number of judgments in which the Court has had to divide up the areas falling within the competence of the European Community and those falling within the competence of the European Union. (2)

2. The division of areas of competences within a constitutional structure comprising three pillars, namely a Community pillar and two pillars the intergovernmental dimension of which is more marked, generates the type of dispute in which the Court has the delicate and complex task of tracing a line demarcating the areas of activity belonging to the Community legislature and those assigned to the legislature of the European Union.

3. In the present case, the Court is called upon to determine the boundary between the Community pillar and the third pillar, namely Title VI of the EU Treaty relating to police and judicial cooperation in criminal matters.

4. By its action, Ireland asks the Court to annul 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 (3) on the ground that it was not adopted on an appropriate legal basis.

5. Ireland, supported by the Slovak Republic, takes the view that the only legal basis on which the measures contained in Directive 2006/24 may legitimately be based is not Article 95 EC, but in Title VI of the EU Treaty concerning police and judicial cooperation in criminal matters, in particular Articles 30 EU, 31(1)(c) EU and 34(2)(b) EU.

6. In this Opinion, I will set out the reasons why, in my view, the Community legislature acted correctly in choosing to adopt Directive 2006/24 on the basis of Article 95 EC.

I – Legal background

7. Article 47 EU provides:

'Subject to the provisions amending the Treaty establishing the European Economic Community with a view to establishing the European Community, the Treaty establishing the European Coal and Steel Community and the Treaty establishing the European Atomic Energy Community, and to these final provisions, nothing in this Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them.'

8. Article 95(1) EC provides:

'By way of derogation from Article 94 and save where otherwise provided in this Treaty, the following provisions shall apply for the achievement of the objectives set out in Article 14. The Council shall, acting in accordance with the procedure referred to in Article 251 and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.'

9. The following three directives were adopted on the basis of Article 95 EC:

– 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; (4)

– Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); (5) and

– Directive 2006/24.

A – *Directive 95/46*

10. Directive 95/46 lays down rules relating to the processing of personal data in order to protect the fundamental rights and freedoms of natural persons, notably their privacy, while ensuring the free movement of those data within the Community.

11. Article 3(2) of Directive 95/46 lays down the following limitation on the material scope of the directive:

'This Directive shall not apply to the processing of personal data:

– in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and, in any case, to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

…'

12. Under paragraph (1) of Article 13 of Directive 95/46, entitled 'Exemptions and restrictions':

'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.'

B – *Directive 2002/58*

13. Directive 2002/58 was adopted with a view to supplementing Directive 95/46 with provisions specific to the electronic communications sector.

14. As stated in Article 1(1) of Directive 2002/58:

'This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community'.

15. Like Article 3(2) of Directive 95/46, Article 1(3) of Directive 2002/58 lays down a limitation on the scope of that directive as follows:

'This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

16. Articles 5, 6 and 9 of Directive 2002/58 define the rules applicable to the processing, by network and service

providers, of traffic data and location data generated by the use of electronic communications services. Those data must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication, with the exception of data required for billing and interconnection payments. Furthermore, with the agreement of the person concerned, certain data may also be processed for commercial purposes or the provision of value added services.

17. In particular, Article 6(1) of Directive 2002/58 provides:

'Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).'

18. According to Article 15(1) of Directive 2002/58:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.'

C – *Directive 2006/24*

19. Recitals 5 to 11 in the preamble to Directive 2006/24 provide as follows:

'(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.

(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [signed in Rome on 4 November 1950] (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.'

20. It is also stated in recital 15 in the preamble to Directive 2006/24:

'Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. …'

21. According to recital 21 in the preamble to Directive 2006/24:

'Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those

objectives.'

22. Recital 25 in the preamble to Directive 2006/24 is worded as follows:

'This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union. Such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as guaranteed by the ECHR. Under Article 8 of the ECHR, as interpreted by the European Court of Human Rights, interference by public authorities with privacy rights must meet the requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner that is adequate, relevant and not excessive in relation to the purpose of the interference.'

23. Article 1(1) of Directive 2006/24 provides:

'This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.'

24. Article 3 of Directive 2006/24 lays down an obligation to retain data. Article 3(1) is worded as follows:

'By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.'

25. As regards access to retained data, Article 4 of Directive 2006/24 provides:

'Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.'

26. As to the periods of retention of data, Article 6 of Directive 2006/24 provides:

'Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.'

27. Furthermore, as regards the storage requirements for retained data, Article 8 of Directive 2006/24 states:

'Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.'

28. By reason of the obligation to retain data established by Directive 2006/24, Article 11 thereof inserts a new paragraph into Article 15 of Directive 2002/58. That paragraph is worded as follows:

'1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC … to be retained for the purposes referred to in Article 1(1) of that Directive.'

29. Finally, Article 12 of Directive 2006/24 is worded as follows:

'1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.

2. The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.

…'

II – Background to the dispute

30. On 28 April 2004, the French Republic, Ireland, the Kingdom of Sweden, and the United Kingdom of Great Britain and Northern Ireland submitted to the Council a draft of a framework decision based on Articles 31(1)(c) EU and 34(2)(b) EU. The draft concerned the retention of data processed and stored in connection with the provision of publicly available electronic

communications services or data in public communication networks for the purposes of the prevention, investigation, detection and prosecution of criminal offences, including terrorism. (6)

31. Taking the view that this draft framework decision consisted of two parts, namely, obligations on operators to retain traffic data relating to users of their services for a certain period and obligations concerning access to and exchange of those data by the competent authorities in criminal matters, the Commission stated that it favoured Article 95 EC as the legal basis for the continuous measures in the first part of the draft framework decision. In particular, it pointed out that Article 47 EU did not allow an instrument based on the EU Treaty to affect the *acquis communautaire*, in this case Directives 95/46 and 2002/58. Taking the view that the determination of the categories of data to be retained and of the retention period fell within the competence of the Community legislature, the Commission reserved the right to submit a proposal for a directive.

32. On 21 September 2005, the Commission adopted a proposal for a directive of the European Parliament and of the Council, based on Article 95 EC, on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58. (7)

33. During its session on 1 and 2 December 2005, the Council opted for a directive on the legal basis of the EC Treaty, rather than for the adoption of a framework decision.

34. On 28 November 2005, the Civil Liberties, Justice and Home Affairs Committee of the European Parliament approved a report on the proposal for a directive. (8) On 14 December 2005, the Parliament issued its opinion in accordance with the co-decision procedure under Article 251 EC. (9)

35. The Council adopted Directive 2006/24 by qualified majority at its session on 21 February 2006. Ireland and the Slovak Republic voted against it.

III – Forms of order sought

36. Ireland claims that the Court should:

– annul Directive 2006/24 on the ground that it was not adopted on an appropriate legal basis, and

– order the Council and the Parliament to pay the costs.

37. The Parliament contends that the Court should:

– reject the application as unfounded, and

– order the applicant to pay all the costs of the present proceedings,

– or, in the alternative, declare that the effects of the contested Directive are to remain in force until a new measure enters into force.

38. The Council contends that the Court should:

– reject Ireland's application for annulment of Directive 2006/24, and

– order Ireland to pay the costs.

IV – Proceedings before the Court

39. By orders of 1 February 2007, the President of the Court granted leave to the Slovak Republic to intervene in support of the form of order sought by the applicant and to the Kingdom of Spain, the Kingdom of the Netherlands, the Commission and the European Data Protection Supervisor ('EDPS') to intervene in support of the forms of order sought by the defendants.

V – Main arguments of the parties

40. Ireland submits that the choice of Article 95 EC as the legal basis for Directive 2006/24 is incorrect. It argues that neither Article 95 EC nor any other provision of the EC Treaty is capable of providing an appropriate legal basis for that directive.

41. Ireland claims principally that the sole objective or, alternatively, the main or predominant objective of Directive 2006/24 is to facilitate the investigation, detection and prosecution of serious crime, including terrorism. Therefore, it submits that the only legal basis on which the measures contained in that directive may be validly based is to be found in Title VI of the EU Treaty, in particular in Articles 30 EU, 31(1)(c) EU and 34(2)(b) EU.

42. In the view of Ireland, an examination of the recitals in the preamble (in particular recitals 7 to 11 and 21) and of the basic provisions (in particular Article 1(1)) of Directive 2006/24 shows that reliance on Article 95 EC as the legal basis for that directive is inappropriate. The directive, it submits, is clearly directed towards the fight against serious crime.

43. It is established that measures based on Article 95 EC must have as their centre of gravity the harmonisation of national laws in order to improve the functioning of the internal market. The provisions of Directive 2006/24 concern the fight against serious crime and are not intended to address defects in the internal market.

44. Alternatively, even if, contrary to Ireland's main argument, the Court were to hold that Directive 2006/24 is indeed intended, inter alia, to prevent distortions of competition or obstacles to the internal market, Ireland submits that that aim must be regarded as purely incidental to the main or predominant objective of combating crime.

45. Ireland argues that the Community legislature is not competent to use an amending directive adopted on the basis of Article 95 EC in order to incorporate provisions falling outside the competence conferred on the Community under the first pillar. The obligations intended to ensure that data are available for the investigation, detection and prosecution of serious criminal offences fall within an area which may only be the subject of a measure based on Title VI of the EU Treaty. The adoption of such an instrument would therefore not affect the provisions of Directive 2002/58 within the meaning of Article 47 EU.

46. Furthermore, Ireland argues that the first indent of Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58 expressly exclude from their scope activities which fall outside the EC Treaty, activities concerning public security, defence, State security and the activities of the State in areas of criminal law. Directive 2006/24 does not contain any exclusion of that kind. On the contrary, the matters excluded from the scope of Directives 95/46 and 2002/58 are included within the scope of Directive 2006/24, as is shown clearly by the provisions of Article 1(1) of the latter. Even if it is not the case with respect to Directives 95/46 and 2002/58, it is permissible to question the choice of Article 95 EC as the legal basis of Directive 2006/24 on the ground that it contains matters expressly excluded from the earlier directives.

47. The fact that Directive 2006/24 does not contain provisions providing for access to data for purposes of the investigation, detection and prosecution of serious criminal offences is, Ireland contends, not conclusive and does not prevent the Court from following the same reasoning as that which it adopted in its above judgment in *Parliament* v *Council and Commission*.

48. Finally, as regards the Parliament's request that any judgment annulling the contested measure should be limited in time, Ireland submits, first, that such an annulment would not give rise to a risk of serious economic repercussions and, second, that legal certainty does not require that the provisions of Directive 2006/24 be maintained in force despite its invalidity. Accordingly, Ireland takes the view that it would not be appropriate for the Court to apply a limit in time if that directive were to be annulled.

49. The Slovak Republic supports Ireland's position. It takes the view that Article 95 EC cannot serve as the legal basis for Directive 2006/24, since the latter's main objective is not to eliminate barriers and distortions in the internal market. The directive harmonises the retention of personal data in a manner which goes beyond commercial objectives in order to facilitate State action in the area of criminal law. For that reason, it cannot be adopted under Community competence regardless of whether or not the Community act provides for transmission of those data or for other processing by law-enforcement authorities.

50. The retention of personal data to the extent required by Directive 2006/24 would, it argues, amount to an extensive interference in the right of individuals to privacy, as protected by Article 8 of the ECHR. It is also questionable whether such a far-reaching interference could be justified on economic grounds, in this case the enhanced functioning of the internal market. The adoption of an act outside the scope of Community competence, the primary and undisguised purpose of which is the fight against crime and terrorism, would be a more appropriate solution, providing a more proportionate justification for interference in the right of individuals to protection of their privacy.

51. Unlike Ireland, the Slovak Republic takes the view that it would be appropriate, if Directive 2006/24 were annulled, for the Court to suspend the effects of its judgment until the adoption of a replacement instrument.

52. According to the Parliament, Ireland's action is based on an incorrect assessment of the purpose and content of Directive 2006/24 and on a misunderstanding of the powers accorded to the Community under the first pillar and of those of the Union under the third pillar, namely Title VI of the EU Treaty.

53. Thus, the Parliament submits that the applicant is selective in its interpretation of the provisions of Directive 2006/24. Recitals 5 and 6 in the preamble make it clear that the directive's main or predominant purpose is to eliminate obstacles to the internal market for electronic communications services, and recital 25 in the preamble to the directive confirms that the access to and use of the retained data for law-enforcement purposes fall outside the scope of Community competence.

54. Article 3(1) of Directive 2006/24 derogates from Articles 5, 6 and 9 of Directive 2002/58 by requiring the providers of electronic communications to retain data which they were previously required to erase. Such a modification of existing obligations must necessarily be adopted on the basis of the powers under the first pillar, since the use of a third-pillar instrument would infringe Article 47 EU. The Parliament also observes that the main provisions of Directive 2006/24, namely Articles 5 to 8, undeniably seek to harmonise the requirements relating to retained data.

55. The Parliament points out that, following the terrorist attacks of 11 September 2001 in the United States of America and the subsequent attacks in Madrid and London, a number of Member States adopted or were in the process of adopting widely differing rules on the retention of data. Such differences would have been liable to impede the free flow of personal data between the Member States and, therefore, the provision of electronic communications services.

56. The retention of data constitutes a significant cost element for the operators concerned and the existence of different requirements in that field may distort competition within the internal market. The main purpose of Directive 2006/24 is to harmonise the obligations imposed by the Member States on providers of electronic communications concerning data retention. It follows that Article 95 EC is the correct legal basis for that directive. Reliance on Article 95 EC as the legal basis

is not invalidated by the importance attributed to combating crime. While the fight against crime has clearly influenced the choices made in Directive 2006/24, that concern does not invalidate the choice of Article 95 EC as the legal basis for the directive.

57. The Parliament also observes that Directive 2006/24 does not contain any provision the aim or effect of which is to grant access to, or permit the processing of, the retained data for law-enforcement purposes, unlike the cases which gave rise to the judgment in *Parliament* v *Council and Commission*, cited above, in which access was granted to a law-enforcement body from a non-member country. Furthermore, Directive 2006/24 does not contain any provisions on cooperation between law-enforcement services within the meaning of Article 30 EU or cooperation between judicial authorities within the meaning of Article 31 EU. In summary, the directive does not contain any provision relating to 'the activities of the State in areas of criminal law' within the meaning of Article 1(3) of Directive 2002/58.

58. According to the Parliament, although the retention of an individual's personal data may in principle constitute interference within the meaning of Article 8 of the ECHR, that interference may be justified, in terms of that article, by reference to public safety and crime prevention. That justification must be distinguished from the correct choice of the legal basis within the legal system of the Union, that being an unrelated matter.

59. Finally, the Parliament takes the view that, were the Court to annul Directive 2006/24, its effects should be maintained on the basis of Article 231 EC until the adoption of a replacement measure. Although the applicant seeks annulment of the directive on the ground that it was adopted on an inappropriate legal basis, it does not challenge its content. Maintenance of the effects of the directive would be justified on grounds of legal certainty and in order to protect the interests of data subjects.

60. The Council submits that, in the years following the adoption of Directive 2002/58, national law-enforcement authorities were becoming increasingly concerned about the exploitation of developments in the area of electronic communications for the purpose of committing criminal acts. Those new concerns led the Member States to adopt measures to prevent data relating to those communications being erased and to ensure that they were available to law-enforcement authorities. Those measures were divergent and began to affect the proper functioning of the internal market. Recitals 5 and 6 in the preamble to Directive 2006/24 are explicit in that regard. Those circumstances led the Community legislature to lay down precise and harmonised obligations for service providers concerning whether or not the personal data referred to in Article 5 of that directive are to be erased, thereby guaranteeing common Community rules to ensure uniformity in the internal market.

61. The Council also takes the view that, while the need to combat crime, including terrorism, was a determining factor in the decision to amend the scope of the rights and obligations laid down in Articles 5, 6 and 9 of Directive 2002/58, that fact does not preclude Directive 2006/24 from having to be adopted on the basis of Article 95 EC. Neither Articles 30 EU, 31 EU and 34 EU nor any other article in the EU Treaty can, without infringing Article 47 EU, serve as the basis for a measure which amends the obligations imposed on operators by Directive 2002/58.

62. Apart from the constraints imposed by Article 47 EU, the Council denies that the area regulated by Directive 2006/24 may be the subject-matter of a measure which must be adopted under Title VI of the EU Treaty, since nothing in that directive relates to the organisation of cooperation between, inter alia, police forces, customs authorities and judicial authorities or to the harmonisation of the rules of criminal law of the Member States.

63. The Council adds that the rights protected by Article 8 of the ECHR are not absolute and may be subject to restrictions under the conditions laid down in Article 8(2) thereof. As provided in Directive 2006/24, the retention of data serves a legitimate public interest recognised in Article 8(2) of the ECHR and constitutes an appropriate means by which to protect that interest.

64. The Kingdom of Spain and the Kingdom of the Netherlands support the Parliament and the Council, submitting arguments to the Court which are essentially the same as those put forward by the defendants.

65. The Commission recalls that, prior to the adoption of Directive 2006/24, several Member States had adopted national measures on data protection pursuant to Article 15(1) of Directive 2002/58. It highlights the significant divergences which existed between those measures. For example, the retention period varied from three months in the Netherlands to four years in Ireland. The obligations relating to data protection have serious economic repercussions for service providers. A divergence in those obligations could lead to significant market distortions. In that context, it was legitimate to adopt Directive 2006/24 on the basis of Article 95 EC.

66. Directive 2006/24 limits, in a manner harmonised at Community level, the obligations laid down by Directive 2002/58. Since the latter was based on Article 95 EC, Directive 2006/24, which amended it, must be based on the same article of the EC Treaty.

67. The Commission also takes the view that, contrary to arguments put forward by Ireland, Directive 2006/24 must be understood as a data protection measure which forms part of the regulatory framework established by Directives 95/46 and 2002/58. In particular, a distinction must be made, from the point of view of data protection, between operations which do not come within the scope of Community law by reason of an exclusion clause and those which come under Community law but which may be subject to certain limits that are justified and proportionate by reason of a restrictive clause.

68. Admittedly, Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58 exclude from the scope of those directives, inter alia, State activities in areas of criminal law. However, Directive 2006/24 does not cover activities of the State as such, but data processing by telecommunications operators for commercial purposes related to the provision of electronic communications services on public communications networks. That activity falls clearly within the scope of Community law and in particular that of Directives 95/46 and 2002/58.

69. Furthermore, if the possibility for a Member State to limit the scope of data-protection rights for the purposes of the investigation, detection and prosecution of serious crime was indeed an issue which fell outside the scope of Community law, Article 13(1) of Directive 95/46 and Article 15(1) of Directive 2002/58 would be redundant and, therefore, ineffective in regard to Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58.

70. Finally, the Commission submits that the mention of the investigation, detection and prosecution of serious crime in Article 1(1) of Directive 2006/24 falls under Community law because it indicates the legitimate objective of the restrictions imposed by that directive on the rights of individuals with regard to the protection of their personal data. Such an indication is necessary in order to comply both with the requirements of Directives 95/46 and 2002/58 and with those of Article 8 of the ECHR.

71. As regards the EDPS, his arguments consist, inter alia, in demonstrating the impact of the choice of legal basis on the Community system for the protection of personal data. According to the EDPS, if the EC Treaty could not serve as the basis for Directive 2006/24, the provisions of Community law relating to data protection would not protect citizens when the processing of their personal data would facilitate the prevention and combating of crime. In such a situation, the general system of data protection under Community law, stemming in particular from Directives 95/46 and 2002/58, would apply to data processing for commercial purposes but not to the processing of those data for the purposes of crime prevention. That would give rise to difficult distinctions for service providers and a reduction in the level of protection for data subjects. Such a situation should be avoided. The need for consistency justifies the adoption of Directive 2006/24 under the EC Treaty.

VI – Analysis

72. In order to mark out the boundary, in the context of a dispute relating to the choice of legal basis, between the spheres of action belonging to the Community legislature and those allocated to the legislature of the European Union, the Court has indicated the scope to be given to Article 47 EU, which acts as a pivot between matters covered by Community law and those covered by the law of the Union.

73. I would point out that, under Article 47 EU, no provisions of the EC Treaty may be affected by a provision of the EU Treaty. That requirement also appears in the first paragraph of Article 29 EU, which introduces Title VI of the EU Treaty dealing with police and judicial cooperation in criminal matters.

74. In guaranteeing a link between the areas falling with the respective scopes of the EC and EU Treaties in accordance with the rule laid down in Article 47 EU, the Court's role is to ensure that acts which a party claims fall within the scope of Title V or Title VI of the EU Treaty do not encroach upon the powers conferred on the Community by the EC Treaty. (10)

75. In that context, the powers enjoyed by the Community under the EC Treaty must be regarded as being affected within the meaning of Article 47 EU where the provisions of an act adopted on the basis of the EU Treaty could have been adopted on the basis of an article of the EC Treaty. (11) According to the Court, Article 47 EU thus seeks, in accordance with the fifth indent of Article 2 EU and the first paragraph of Article 3 EU, to maintain and build on the *acquis communautaire*. (12)

76. As far as concerns the method used to determine whether an act adopted on the basis of the EU Treaty could have been adopted on the basis of the EC Treaty, the Court examines whether, by reason of its aim and content, such an act has as its main purpose the implementation of a policy conferred on the Community by the EC Treaty. (13) The Court thereby applies its settled case-law, according to which the choice of legal basis for a measure must rest on objective factors which are amenable to judicial review, including in particular the aim and the content of that measure. (14)

77. In the present case, the issue is not, of course, whether a measure adopted on the basis of the EU Treaty should have been adopted on the basis of the EC Treaty, but whether a measure was correctly adopted on the basis of the EC Treaty and not that of the EU Treaty, as the applicant claims. The method to be used is, however, identical. It consists in determining whether or not, having regard to the centre of gravity of the measure in issue, Article 47 EU would have authorised the adoption of that measure on the basis of the EU Treaty.

78. The issue in this case consists, therefore, in determining whether Ireland's argument, namely that Directive 2006/24 should have been adopted on the basis of Articles 30 EU, 31(1)(c) EU and 34(2)(b) EU, is compatible with the provisions of Article 47 EU. In other words, would the adoption under the EU Treaty of the measures contained in that directive have amounted to an infringement of Article 47 EU? In order to answer that question it is first necessary to ascertain whether, regard being had to its purpose and its content, Directive 2006/24 does in fact fall within the area covered by Article 95 EC.

79. As regards the use of Article 95 EC as the legal basis for a Community act, it follows from the case-law of the Court that, while a finding that disparities exist between national rules is not sufficient in itself to justify recourse to that article, the situation is otherwise where differences exist between the laws, regulations or administrative provisions of the Member States which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market. (15) It is also clear from settled case-law that, although recourse to Article 95 EC as a legal basis is possible if the aim is to prevent the emergence of future obstacles to trade resulting from multifarious development of national laws, the emergence of such obstacles must be likely and the measure in question must be designed to prevent them. (16) In summary, in order to justify recourse to Article 95 EC as the legal basis, what matters is that the measure adopted on that basis must actually be intended to improve the conditions for the establishment and functioning of the internal market. (17)

80. The adoption of Directive 2006/24 on the basis of Article 95 EC appears to me to satisfy the requirements thus laid down by the Court.

81. It is quite clear from recitals 4 to 6 in the preamble to Directive 2006/24 that the Community legislature started from the finding that there were legislative and technical disparities between the national provisions relating to data retention by service providers. Several Member States, exercising the powers conferred on them by Article 15(1) of Directive 2002/58,

had legislated on data retention by service providers for the purposes of the prevention, investigation, detection and prosecution of criminal offences. Those national provisions varied substantially, particularly in regard to the retention period required and the types of data to be retained. (18)

82. Such disparities could therefore make it necessary to harmonise national provisions relating to the obligations of providers of publicly available electronic communications services or public communications networks in respect of data retention.

83. It is appropriate, however, to ascertain whether the disparities found were in fact capable of affecting the establishment and functioning of the internal market, with the result that the Community legislature was entitled to use Article 95 EC in order to adopt the measures contained in Directive 2006/24.

84. From that perspective, it is important to note that the retention of data by the providers of electronic communications services represents a significant financial burden on them, and that that burden is proportionate to the amount of data to be retained and the retention period. (19) The costs concerned are attributable not only to the upgrading of the technology required to retain and archive the data in a secure manner, but also to the maintenance and operation of systems allowing the retention of data.

85. It follows that, in the absence of harmonisation, a provider of electronic communications services would be faced with costs related to the retention of data which differ according to the Member State in which he wishes to provide those services. Such differences may constitute obstacles to the free movement of electronic communications services between the Member States and may therefore create obstacles to the establishment and functioning of the internal market in electronic communications. They may, in particular, slow down the cross-border development of new electronic communications services which are regularly introduced in the information society. They may also give rise to distortions in competition between undertakings operating on the electronic communications market.

86. As is clear from recital 6 in the preamble to Directive 2006/24, such disparities between the laws of the Member States 'present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention'.

87. In so far as Directive 2006/24 proceeds with harmonisation of national laws on the obligation to retain data (Article 3), the categories of data to be retained (Article 5), periods of retention of data (Article 6), and data protection and data security (Article 7), I take the view that it facilitates the development of the internal market for electronic communications by providing common requirements for service providers.

88. I would add that the impact which differences between national laws on data retention have on the functioning of the internal market is also taken into consideration in Article 12(2) of Directive 2006/24. When evaluating national measures providing for an extension of the maximum data retention period in particular circumstances and for a limited period, the Commission must ascertain whether such measures amount to a means of arbitrary discrimination or a disguised restriction on trade between the Member States, and whether they constitute an obstacle to the functioning of the internal market.

89. In the light of those factors, the intervention of the Community legislature on the basis of Article 95 EC appears to me to be justified.

90. Ireland, supported by the Slovak Republic, takes the contrary view that Directive 2006/24 cannot be based on Article 95 EC inasmuch as its centre of gravity is not the establishment and functioning of the internal market. The directive, it submits, has as its sole, or at least its main purpose, the investigation, detection and prosecution of serious crime. Ireland relies, in that connection, on a number of provisions of the directive which do in fact emphasise that objective.

91. Among those provisions is recital 11 in the preamble to Directive 2006/24, according to which, it will be recalled, '[g]iven the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive'. Also, according to Article 1(1), Directive 2006/24 'aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law'.

92. It has not been disputed by any party during these proceedings, and it appears to me to be unarguable, that the rationale of the obligation to retain data which is imposed on providers of electronic communications services lies in the fact that it facilitates the investigation, detection and prosecution of serious crimes. It cannot be denied that it is because the retention of data constitutes an effective investigative tool in inquiries undertaken by the law-enforcement authorities of the Member States, and particularly in cases of organised crime and terrorism, that the Community legislature wished to make general the obligation to retain traffic and location data generated or processed by the providers of electronic communications services or public communications networks.

93. The Community legislature therefore sought to go a stage further than is provided for in Article 15(1) of Directive 2002/58. That provision, it will be recalled, gives Member States the possibility to 'adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13 (1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention

of data for a limited period justified on the grounds laid down in this paragraph.' By adopting Directive 2006/24, the Community legislature sought to go further, first, by transforming that option available to Member States into an obligation to require data retention and, second, by harmonising the categories of data to be retained and their retention period.

94. Among the grounds cited in Article 15(1) of Directive 2002/58, the Community legislature adopted only that relating to the investigation, detection and prosecution of serious crime. In so doing, it indicated the legitimate objective of the restrictions imposed by Directive 2006/24 on the rights of persons concerning the protection of their personal data. One of the particular features of that directive is that it must be understood as forming part of the system for the protection of personal data which has been gradually introduced by the Community legislature. As that directive introduces an exception to a number of protective measures laid down by Directive 2002/58, it was necessary for the legislature to mention such a public-interest objective in order to demonstrate the need to adopt an instrument on data retention in the light of the requirements of Article 8 of the ECHR.

95. Must the mention of such a ground justifying interference in the right of individuals to privacy protected by Article 8 of the ECHR, as well as the statement that the retention of data is an effective tool in the area of law enforcement for the purposes of investigation, detection and prosecution of serious crime, none the less be regarded as incompatible with the use of Article 95 EC as a legal basis for a Community act such as Directive 2006/24?

96. I think not for the following reasons.

97. First of all, the Court has already had occasion to state that if the conditions for recourse to Article 95 EC as a legal basis are fulfilled, the Community legislature cannot be prevented from relying on that legal basis on the ground that a public interest is a decisive factor in the choices to be made. (20) In that connection, sight must not be lost of the fact that Article 95(3) EC explicitly requires that, in achieving harmonisation, a certain number of overriding requirements of public interest must be taken into account and that these must be the subject of a high level of protection. (21) In my view, those overriding requirements include the requirement of security. A measure such as Directive 2006/24, which harmonises the conditions on the retention of certain data for the purposes of the investigation, detection and prosecution of serious crime, contributes to this requirement that a high level of security be guaranteed within the internal market. Thus, in my view, Article 95(3) EC authorises measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market and which also pursue a public-interest objective such as guaranteeing a high level of security within the Community.

98. Next, contrary to Ireland's submissions, I take the view that the mere fact that a measure refers to an objective such as the investigation, detection and prosecution of serious crime is not sufficient to shift such a measure from the first to the third pillar. In other words, the existence of such a purpose is not, in my view, sufficient to constitute an act coming within the area covered by 'police and judicial cooperation in criminal matters' within the meaning of Title VI of the EU Treaty.

99. It follows from Article 29 EU that, without prejudice to the powers of the European Community, the Union's objective of providing citizens with a high level of safety within an area of freedom, security and justice is achieved by preventing and combating crime through three types of action: first, through closer cooperation between police forces, customs authorities and other competent authorities in the Member States, both directly and through the European Police Office (Europol), in accordance with the provisions of Articles 30 EU and 32 EU; second, through closer cooperation between judicial and other competent authorities of the Member States, including cooperation through the European Judicial Cooperation Unit (Eurojust), in accordance with the provisions of Articles 31 EU and 32 EU; and, finally, through approximation, where necessary, of rules on criminal matters in the Member States, in accordance with the provisions of Article 31(e) EU.

100. In my opinion, the obligation to retain data generated or processed in connection with the provision of communications services does not correspond to any of those three types of action. It does not, therefore, have the characteristics necessary for its inclusion within the scope of Title VI of the EU Treaty.

101. It is true that the objective of investigating, detecting and prosecuting serious crime has a criminal aspect which suggests that all measures pursuing that objective should be brought under the third pillar. Such an approach would, however, amount to extending unduly the scope of Title VI of the EU Treaty, which, as I have indicated, does not merely state an objective but lists the kinds of action which give expression to the concept of 'police and judicial cooperation in criminal matters' within the meaning of that title.

102. I would observe in this regard that the measures provided for by Directive 2006/24 do not involve any direct intervention by the law-enforcement authorities of the Member States. It is merely envisaged that the providers of publicly available electronic communications services or public communications networks must retain the data which are generated or processed when the communications services in question are being supplied, that is to say, only those data which are closely related to the commercial activities of those providers.

103. In summary, Directive 2006/24 contains measures which relate to a stage prior to the implementation of police and judicial cooperation in criminal matters. It does not harmonise either the issue of access to data by the competent national law-enforcement authorities or that relating to the use and exchange of those data by such authorities, for example in the context of criminal investigations. Those matters, which come, in my view, within the area covered by Title VI of the EU Treaty, were properly excluded from the provisions of Directive 2006/24. (22)

104. Furthermore, it is expressly stated in recital 25 in the preamble to Directive 2006/24 that the latter 'is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. *Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union*'. (23) The only requirement as to data access which the Community legislature wished to highlight, and which is more akin to a warning that a harmonisation measure, appears in Article 4 of Directive 2006/24, which provides that 'Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national

authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights'.

105. The boundary between measures coming under the Community pillar and those which must be adopted within the framework of Title VI of the EU Treaty may therefore, in my view, be drawn as follows.

106. Measures which harmonise the conditions under which providers of communications services must retain traffic and location data which are generated or processed in the course of their commercial activities belong to the Community pillar. Such an approximation of national laws on data retention reduces the risk of obstacles to the development of the internal market in electronic communications by presenting operators with common requirements. The fact that the Community legislature deemed it necessary to impose an obligation to retain data by reason of the efficacy of this tool for the investigation, detection and prosecution of serious offences is not sufficient to remove such a measure from the Community pillar, since that overriding requirement of public interest may be taken into account by a harmonisation measure adopted on the basis of Article 95 EC. Furthermore, the mention of such an overriding requirement of public interest is vital in order to justify the interference by the Community legislature in the right to privacy of the users of electronic communications services.

107. On the other hand, measures harmonising the conditions under which the competent national law-enforcement authorities may access, use and exchange retained data in the discharge of their duties belong to the third pillar. The direct involvement of such authorities with private operators and the mandatory transmission by the latter of data for law-enforcement purposes fall, in my view, within the scope of 'police and judicial cooperation in criminal matters' within the meaning of Title VI of the EU Treaty. At that stage, the participation of private operators in a criminal investigation and their collaboration with the competent national authorities acquire a specific and certain character.

108. This dividing line is certainly not exempt from criticism and may appear artificial in some respects. I agree that it would be more satisfactory if the overall issue of data retention by the providers of electronic communications services and the detailed rules on their cooperation with the competent national law-enforcement authorities were the subject of a single measure which would ensure coherence between those two aspects. Although it is regrettable, the constitutional architecture consisting of three pillars nevertheless requires that the areas of action be split up. The priority in this context is to guarantee legal certainty by clarifying as far as possible the respective boundaries between the spheres of action covered by the different pillars.

109. The analysis that I suggest here does not appear to me to be at variance with the Court's findings in its judgment in *Parliament* v *Council and Commission*, cited above. On the contrary, in my view it serves to clarify the scope to be given to that judgment.

110. I would point out that, in the cases which gave rise to that judgment, the Parliament sought, first, the annulment of Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (24) and, second, the annulment of Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection. (25)

111. In its judgment, the Court first considered the legality of the decision on adequacy in the light of the first indent of Article 3(2) of Directive 95/46. That provision, it will be recalled, excludes from the scope of Directive 95/46 the processing of personal data 'in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case … processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State-security matters) and the activities of the State in areas of criminal law'.

112. The Court held that the transfer of personal data contained in the passenger name records ('PNR data') to the Bureau of Customs and Border Protection of the American Department of Homeland Security ('CBP') was a processing operation concerning public safety and the activities of the State in the areas of criminal law. It ruled that the decision on adequacy did not concern data processing necessary for a supply of services, but did concern data processing regarded as necessary for safeguarding public security and for law-enforcement purposes. Furthermore, while it follows from the judgment in *Lindqvist* (26) that the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 are, in any event, activities of the State or of State authorities unrelated to the fields of activity of individuals, the Court held that it none the less does not follow that the fact that the PNR data were collected by private operators for commercial purposes and it was they who arranged for the transfer of those data to a non-member country has the consequence of excluding the transfer concerned from the scope of that provision. The Court observed that that transfer fell within a framework established by the pubic authorities and relating to public safety.

113. From this the Court inferred that the decision on adequacy concerned the processing of personal data within the meaning of the first indent of Article 3(2) of Directive 95/46 and that therefore it did not come within the scope of that directive. The Court concluded that it was necessary to annul the decision on adequacy.

114. Next, in examining the legality of the Council decision, the Court simply ruled on the plea alleging that the choice of Article 95 EC as the legal basis for that decision was wrong. It held that Article 95 EC, read in conjunction with Article 25 of Directive 95/46, could not justify Community competence to conclude the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection ('the Agreement'), approved on behalf of the Community by that decision. (27) In support of that finding, the Court held that the Agreement related to the same transfer of data as the decision on adequacy, and therefore to data-processing operations which are excluded from the scope of Directive 95/46. It inferred from this that the Council decision could not have been validly adopted on the basis of Article 95 EC.

115. Ireland relies on the judgment in *Parliament* v *Council and Commission* to support the arguments which it puts forward in this case, that is, essentially, that, on account of the single, or at least the principal, objective pursued by Directive 2006/24, consisting in the investigation, detection and prosecution of serious crime, that directive should have been adopted under Title VI of the EU Treaty. However, that judgment was delivered in a context the principal characteristics of which distinguish it from the present case.

116. In the case which gave rise to the judgment in *Parliament* v *Council and Commission*, the Agreement principally required air carriers providing international passenger transport services to or from the United States of America to provide the CBP with electronic access to PNR data collected and stored in the air carriers' automated reservation/departure control systems. The Agreement thus established a form of international cooperation between the contracting parties which was intended to achieve the objective of combating terrorism and other serious crimes while attempting to reconcile that objective with the objective of protecting airline passengers' personal data. (28) The existence of such a form of international cooperation with the public authorities of a non-member country already constitutes a substantial difference from the present case.

117. Next, the data processing in question in the cases which gave rise to the judgment in *Parliament* v *Council and Commission* concerned a stage subsequent to the initial collection of the data by airline companies. That processing concerned the consultation, use by the CBP, and the making available to the latter of air passenger data from the air carriers' reservation systems located in the territory of the Member States. (29) It was therefore a form of cooperation involving not only private operators but also a public authority, in that case the CBP, for the purpose of combating terrorism and other serious crimes.

118. In such a context, an act which provides for the consultation and use of personal data by an entity tasked with safeguarding a State's internal security, and for the making available of those data to such an entity, must, in my view, be treated as constituting an act of cooperation between public authorities. In particular, in such a situation of compulsory disclosure of data to a national body for security and law-enforcement purposes, requiring a legal person to transfer data does not appear to be fundamentally different from a direct exchange of data between public authorities, for example in criminal investigations. (30)

119. The international dimension of the cooperation put in place and the methods of collaboration established between air carriers and the CBP, methods which bring it, in my view, within the area covered by Title VI of the EU Treaty, thus constitute two fundamental differences vis-à-vis the situation at issue in the present case.

120. It is, moreover, precisely because of the characteristics which have just been identified that Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) (31) was adopted on the basis of Articles 24 EU and 38 EU.

121. The differences that have been highlighted also help to clarify the scope of the judgment in *Parliament* v *Council and Commission*.

122. In my view, that judgment does not mean that only the examination of the objective pursued by the processing of personal data is relevant for the purpose of including or excluding such processing from the scope of the system of data protection instituted by Directive 95/46. It is also necessary to ascertain in the course of which type of activity data processing is carried out. It is only where it is undertaken in the course of activities specific to States or to State authorities and unrelated to the fields of activity of individuals that it is excluded from the Community system of personal data protection arising from Directive 95/46 pursuant to the first indent of Article 3(2) thereof. It is therefore left to the legislature of the European Union to take over and establish a general system of data protection designed to cover data processing carried out in the course of such State-specific activities. (32)

123. In the judgment in *Parliament* v *Council and Commission*, the Court held that the transfer of data by air carriers to the CBP in order to safeguard public security and for the purposes of law enforcement could be treated as data processing in the course of activities specific to the State or State authorities and unrelated to the fields of activity of individuals. That is why the Court held that it was excluded from the scope of Directive 95/46.

124. Construed thus, the judgment in *Parliament* v *Council and Commission* clarifies the distinction to be drawn between the exclusion clauses and the restrictive clauses which appear in Directive 95/46 and Directive 2002/58.

125. As the Commission explained clearly during the present proceedings, the first indent of Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58 are exclusion clauses, in so far as they exclude from the scope of those two directives data processing carried out in the course of activities which fall outside the EC Treaty, such as those envisaged in Titles V and VI of the EU Treaty, and in any case processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

126. By contrast, the scope of the restrictive clauses in Article 13(1) of Directive 95/46 and in Article 15(1) of Directive 2002/58 is entirely different. Under those clauses, the Member States alone are authorised to restrict the scope of certain rights and obligations defined in those two directives where such a restriction is a measure necessary to safeguard a public-interest objective such as national security, defence and public health and the prevention, investigation, detection and prosecution of criminal offences. The data processing concerned continues, however, to be covered by the Community system of protection of personal data.

127. The fact that those two types of clauses mention similar public-interest objectives undoubtedly maintains the confusion as to their respective scopes. That confusion is probably one of the reasons for Ireland's contentions, inasmuch as that Member State relies only on the exclusion clauses, which it interprets as meaning that the mere fact that a measure refers to a public-interest objective, such as the investigation, detection and prosecution of serious crime mentioned in Article 1(1) of

Directive 2006/24, is sufficient for it to be excluded from the scope of Community law.

128. The very existence of the restrictive clauses in Directives 95/46 and 2002/58, which set out the public-interest grounds pursuant to which the scope of the rights and obligations relating to data protection may be restricted, demonstrates, however, that that argument is flawed and that the mere mention of a public-interest objective, such as that relating to the investigation, detection and prosecution of serious crime in Article 1(1) of Directive 2006/24, is insufficient in itself to identify what is or is not covered by Community law, or, more precisely, by the Community system for the protection of personal data.

129. In order to preserve the effectiveness of restrictive clauses and to ensure that they are not merely a repetition of exclusion clauses, it is thus necessary to take the view that under the exclusion clauses contained in the first indent of Article 3(2) of Directive 95/46 and in Article 1(3) of Directive 2002/58 it is only data-processing operations pertaining to activities specific to the State or to State authorities and unrelated to the fields of activity of individuals, to repeat the formula first used by the Court in its judgment in *Lindqvist* and subsequently in its judgment in *Parliament* v *Council and Commission*, that are excluded from the Community system of personal data protection.

130. Bearing in mind those factors, I would therefore submit, in so far as Directive 2006/24 does not contain any provisions harmonising the conditions for access to data and their use for activities specific to the State or to State authorities and unrelated to the fields of activity of individuals and, in particular, does not contain any provisions liable to come within the notion of 'police and judicial cooperation in criminal matters' within the meaning of Title VI of the EU Treaty, that Directive 2006/24 was correctly adopted under the Community pillar and, more specifically, on the basis of Article 95 EC.

131. Were it to have been accepted, Ireland's argument that Directive 2006/24 should have been adopted on the basis of Articles 30 EU, 31(1)(c) EU and 34(2) EU would thus have led to an infringement of Article 47 EU.

132. Finally, it is necessary to state that, even if it were held that Directive 2006/24 has a twofold component covering both the establishment and functioning of the internal market, in accordance with the provision of Article 95 EC, and 'police and judicial cooperation in criminal matters' within the meaning of Title VI of the EU Treaty, without one being ancillary to the other, Article 47 EU would continue to stand in the way of the use of a legal basis under Title VI of the EU Treaty.

133. The Court, in its judgment in Case C-91/05 *Commission* v *Council*, indicated the scope of Article 47 EU in the case where the examination of a measure reveals that it pursues a twofold aim or that it has a twofold component, falling respectively within the EC and the EU Treaties, without one being ancillary to the other. In such circumstances, the Court held that, since Article 47 EU precludes the Union from adopting, on the basis of the EU Treaty, a measure which could properly be adopted on the basis of the EC Treaty, the Union cannot have recourse to a legal basis coming within an area covered by the EU Treaty in order to adopt provisions which also come within an area of competence conferred by the EC Treaty on the Community.

134. Thus, where a measure has a twofold component, with the result that it could be covered by both the EC Treaty and the EU Treaty, Article 47 EU gives priority, in any event, to the EC Treaty.

VII – Conclusion

135. Having regard to all of the foregoing considerations, I propose that the Court should:

(1) dismiss the action;

(2) order Ireland to pay the costs;

(3) order the Kingdom of Spain, the Kingdom of the Netherlands, the Slovak Republic, the Commission of the European Communities and the European Data Protection Supervisor to bear their own respective costs.

---

1 – Original language: French.

---

2 – In particular, Case C-176/03 *Commission* v *Council* [2005] ECR I-7879; Joined Cases C-317/04 and C-318/04 *Parliament* v *Council and Commission* [2006] ECR I-4721; Case C-440/-05 *Commission* v *Council* [2007] ECR I-9097; and Case C-91/05 *Commission* v *Council* [2008] ECR I-0000.

---

3 – OJ 2006 L 105, p. 54.

---

4 – OJ 1995 L 281, p. 31.

---

5 – OJ 2002 L 201, p. 37.

6 – Council Document No 8958/04, CRIMORG 36 TELECOM 82.

7 – COM(2005) 438 final.

8 – A6-0365/2005.

9 – T6-0512/2005.

10 – See, in that regard, Case C-91/05 *Commission* v *Council*, paragraph 33 and the case-law cited.

11 – Ibidem, paragraph 58 and the case-law cited.

12 – Ibidem, paragraph 59.

13 – Ibidem, paragraph 60.

14 – Case C-440/05 *Commission* v *Council*, paragraph 61.

15 – Case C-380/03 *Germany* v *Parliament and Council* [2006] ECR I-11573, paragraph 37 and the case-law cited.

16 – Ibidem, paragraph 38 and the case-law cited.

17 – Ibidem, paragraph 80 and the case-law cited.

18 – See, in that connection, Annex I to the rejoinder lodged by the Parliament and the Commission working document of 21 September 2005 in the annex to its proposal for a directive (SEC(2005) 1131, paragraph 1.4).

19 – See, in particular, the estimates given in the abovementioned Commission working document of 21 September 2005 (paragraph 4.3.4).

20 – See, to that effect, in the area of public health, *Germany* v *Parliament and Council*, paragraph 39 and the case-law cited.

21 – Ibidem, paragraph 40 and the case-law cited.

22 – Among the proposals for framework directives which deal with the issues relating to the consultation, use and exchange of information by the competent law-enforcement authorities, see, in particular, the proposal of 12 October 2005 for a Council framework decision on the exchange of information under the principle of availability (COM(2005) 490 final), and the proposal of 6 November 2007 for a Council framework decision on the use of Passenger Name Record data (Passenger Name Record – PNR) for law-enforcement purposes (COM(2007) 654 final).

23 – Emphasis added.

24 – OJ 2004 L 183, p. 83, 'the Council decision'.

25 – OJ 2004 L 235, p. 11, 'the decision on adequacy'.

26 – Case C-101/01 [2003] ECR I-12971.

27 – This agreement was later the subject of a corrigendum (OJ 2005 L 255, p. 168).

28 – See point 139 of the Opinion of Advocate General Léger in *Parliament* v *Council and Commission*.

29 – Ibidem, point 102.

30 – Ibidem, points 159 and 160.

31 – OJ 2007 L 204, p. 16.

32 – See, in that connection, the proposal of 4 October 2005 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).