European Court of Justice

The Legal Basis of Internal Market Measures With a Security Dimension. Comment on Case C-301/06 of 10/02/2009, *Ireland* v. *Parliament/Council*, nyr

Sara Poli*

Introduction

Each time users connect to the internet or make a phone call, they leave 'digital fingerprints'[1] which may turn out to be useful for identifying people involved in a crime or an act of terrorism. This is why there is great interest by law enforcement authorities in gaining access to traffic and location data, relying on the forced co-operation of telecommunication and internet providers. However, the effectiveness of compelling these service providers to retain such data for the purpose of fighting crime has been questioned.[2] Moreover, data retention obligations interfere with the right to privacy of individuals, as protected by Article 8 European Convention of Human Rights (ECHR); therefore, they may be imposed only for a legitimate objective, i.e., to protect citizens' safety, and in full respect of the principle of proportionality.

In recent years, a few member states – bearing the advantages of virtual fingerprints in mind – have become active in this area. Taking the view that the disparity of national measures affected the internal market of electronic communication, in 2006 the Council and the European Parliament adopted Directive 2006/24 (the contested Directive).[3] This act obliges private companies to collaborate with law

* University of Rome Tor Vergata. This research was supported by a Marie Curie Intra-European Fellowship within the 7th European Community Framework Programme and was carried out at the Robert Schuman Centre of the European University Institute. I wish to thank Marise Cremona for a discussion on an earlier draft of this note. The usual disclaimer applies.

[1] T.J. McIntyre, 'Data retention in Ireland, privacy, policy and proportionality', 24 *Computer law and security report* (2008) 4, p. 327.

[2] P. Breyer, 'Telecommunications data retention and human rights: the compatibility of the blanket traffic data retention with the ECHR', 11 3 *ELJ* (2005) p. 365.

[3] Directive 2006/24 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* [2006] L 105/54.

European Constitutional Law Review, 6: 137–157, 2010
 doi:10.1017/S157401961010008X

enforcement authorities to fight crime and terrorism.[4] The legal basis is Article 95 EC, now Article 114 of the Treaty on the Functioning of the European Union (TFEU), after the entry into force of the Lisbon Treaty. However, it is clear that this is not a purely internal market instrument but a measure that, prior to the Lisbon Treaty could be defined as 'cross-pillar', since it simultaneously pursues third-pillar objectives.

Ireland, which had enacted strict legislation on 'data retention'[5] before the European initiative was taken, challenged the Directive on the basis of an allegedly inappropriate legal basis. The choice of the latter in the context of cross-pillar measures boils down to deciding whether the Union or the Community is empowered to act. Hence, choosing the correct legal foundation for this kind of measure was necessary in order to safeguard the pillar structure of the EU Treaties. In the pre-Lisbon age, the Irish challenge was designed to preserve the EU's powers *vis-à-vis* the Community ones.

Both Advocate-General (AG) Bot and the Court considered this piece of legislation, which is in a grey area between the first and third pillar, to fall within Community law. This is in stark contrast to a previous ruling,[6] involving an international Treaty concluded by the EC and the United States on the transfer of passenger name record information by air carriers (the so-called 'PNR agreement') – which was, in a similar fashion, on the borders between the Community and an intergovernmental pillar – where the opposite position was taken by the Court.[7]

Had the Treaty of Lisbon not entered into force, one could have said that the Court's position in the present case assuaged the concerns generated by the PNR ruling.[8]

In particular, the Irish case cleared the lingering doubts of the PNR case as to the possibility of adopting Community measures on the basis of first-pillar provi-

[4] The two objectives are both mentioned in the Directive.

[5] This legislation provided for a retention period of three years. *See* Part 7 of the Criminal Justice (Terrorist offences Act) of 2005 reported in McIntyre, *supra* n. 1, p. 331.

[6] Joined Cases C-317/04 and C-318/04, *European Parliament* v. *Council and Commission* [2006] *ECR* I-4721.

[7] Here, the Court considered that Directive 95/46, based on art. 95 of the TEC, was not an appropriate legal basis for the so called 'adequacy decision'. The decision concluding the PNR agreement was also annulled given its links with the mentioned decision. The PNR agreement was found to be excluded from the scope of Directive 95/46, in the same way as the 'adequacy decision'; for that fact the former could not have been validly adopted on the basis of Art. 95. The agreement had to be terminated and re-negotiated with the USA. A new Treaty was concluded on the basis of Art. 24 and 38 of the TEU in 2007 (*OJ* L 204/18).

[8] The criticism levelled to the PNR ruling were the following: it raised the threshold to adopt first pillar measures having a security dimension (G. Gilmore, J.J. Rijpma, 44 *CMLRev.* (2007), p. 1099); it excluded the European Parliament from the decision-making leading to the adoption of the PNR agreement; it left a loophole in terms of data protection in the third pillar (M. Mendez, *EuConst* (2007), p. 137 and also EDPS Press Release of 30 May 2006).

sions, despite their links to third-pillar objectives. Hence, the present ruling moved in the same direction as the 'environmental crime'[9] and *Ecowas*[10] cases, in expanding the breath of the Community's pillar. However, in contrast to the latter, where the hierarchical predominance of the Treaty on the European Community *vis-à-vis* the EU had made the Common Foreign and Security Policy almost nugatory,[11] the green light to the use Article 95 EC has not jeopardised member states' action in the context of criminal and police cooperation in order to combat crime.[12]

Following the entry into force of the Treaty of Lisbon and the abolition of the pillars,[13] it may be wondered whether this case has a mere historic interest. Certainly, member states no longer need to take annulment actions against Community acts in order to safeguard the Union's powers since the Community was superseded by the Union and now we only have Union acts. In this respect, the choice of the legal basis for measures that affect different (old) pillars is no longer problematic. For example, it is now possible to adopt a measure aiming on the one hand, at protecting the environment and on the other, at establishing minimum rules in the area of criminal law, without worrying about the borders between Community and Union powers. However, problems related to the use of multiple legal bases will not cease to exist. On the contrary, the new Treaty poses new ones.[14] Be as it may, the ruling which is commented on here maintains its relevance for appreciating the evolution of the case-law on the choice of legal basis. Indeed, the Luxembourg Court applies the 'centre of gravity' test, which is used to allocate the legal basis of measures pursuing different objectives, in a selective manner. In light of this, one might think that the Court has changed this test.

The comment on this intriguing case is organised as follows. First, it clarifies the legal and political context in which the impugned directive was adopted. Sec-

[9] Case C-176/03, *Commission* v. *Council* [2005] *ECR* I-7879.

[10] Case C-91/05 *Commission* v. *Council* [2008] *ECR* I-3651.

[11] On this issue *see* B. Van Vooren, 'EU–EC External Competences after the Small Arms Judgment,' 14 *Eur. Foreign Aff. Rev.* (2009), p. 13.

[12] On the contrary, there are signs that they do not feel at all inhibited: the body of EU measures designed to facilitate the exchange of information between law enforcement authorities has grown quickly and a cross-border 'dialogue' between intelligence and police authorities and wider access to data are being established as ordinary phenomena.

[13] It should be noted that in the Treaty of Lisbon, the ghost of the second pillar still haunts the fundamental law of the EU. For remarks on the distinctive nature of the CFSP, *see* M. Cremona, 'Coherence through Law: What difference will the Treaty of Lisbon make?', *Hamburg review of social sciences*, Vol. 3, 1 (2008), p. 32.

[14] For example, one of these problems is the following: should the emergency brake procedure be allowed when an act is based on a Treaty provision that enables a member state to rely on this procedure (say Art. 82(3) of the TFEU on judicial cooperation in criminal matters) but also on another provision (say Art. 114 TFEU the provision on the internal market) which does not provide for this possibility? I thank R.H Lauwaars and R.H. van Ooik for this suggestion, taken from their as yet unpublished paper.

ond, the grounds for the challenge will be explained before examining the opinion of AG Bot and the Court's ruling. In the comment, emphasis will be placed on the Court's criteria to allocate the legal basis in order to criticise the way it carries out the 'centre of gravity' test. Subsequently, the differences between the present ruling and the PNR judgment will be highlighted; the contention of this note is that the Data Retention directive is not concerned with the fight against crime or terrorism in the same way as the PNR agreement and therefore Article 95 was the correct legal basis. Finally, the question of whether there are alternative grounds for attacking the legality of the impugned Directive will be explored.

The political and legal context

The principle of confidentiality of data is the tenet of two directives enacted in 1995 and the 2002 and also of Regulation 45/2001 protecting the right to privacy of persons whose personal data are processed by Community institutions or bodies and setting up the European Data Protection Supervisor.[15] For the purposes of this note, the text of the directives is the most interesting. The former, Directive 95/46,[16] is the general Community instrument on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Its legal basis is Article 95 EC. The latter, Directive 2002/58,[17] is a *lex specialis* with respect to the previous one since it was enacted (on the same legal basis) with the double purpose of protecting the right to privacy in the processing of personal data in the specific context of electronic communications,[18] and to ensure the free movement of such data and electronic communications equipment and services in the Community.

Both directives excluded from their scope of application the processing of personal data related 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 of the State concerning, amongst other things, areas of criminal law.'[19]

Both pieces of legislation provided for restrictions to the right to privacy of individuals for the purpose of preventing, investigating, detecting and prosecut-

[15] *OJ* [2001] L 8/1.

[16] *OJ* [1995] L 281/31.

[17] Directive 2002/58 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, *OJ* [2002] L 201/37.

[18] The key principle of the Directive is that traffic data relating to subscribers or users must be erased or made anonymous by the providers of the concerned services when they are no longer needed for the purpose of the transmission of the communication. Art. 6(1).

[19] Art. 3(2) of Directive 95/46 and 1(3) of Directive 2002/58.

ing criminal offences.[20] A specific limit was devised by the 2002 Directive. In particular, under its Article 15(1), *member states* were left free to enact measures, amongst other things on data retention, when this was necessary, *inter alia*, to 'prevent, investigate, detect and prosecute of criminal offences […].'[21] In other words, national authorities were allowed to impose data retention obligations.

The idea of using data collected by electronic communication providers for criminal investigation purposes was put forward by the European Council in its conclusions reacting to the terrorist attacks of 2001.[22] It was reinforced after the Madrid bombings of 2004[23] and became a priority after the tragic London events of 3 July 2005.[24] The legal context, in which action at EU level should have been framed (first pillar v. third pillar), was not specified.

On 28 April 2004, France, the United Kingdom, Ireland and Sweden took advantage of the favourable European mindset towards an instrument compelling electronic communication providers to retain traffic data. They tabled a proposal for a third-pillar measure (a framework decision).[25] The adoption of this new instrument was considered necessary to make police and judicial co-operation more effective in fighting against crime and to enable competent authorities of other member states to have access to this data.[26] The draft framework decision explicitly made cross-border access to the data regulated by this measure possible.[27] A further reason for passing EU legislation in this area was to avoid the loss of this source of information, given its usefulness as an investigative tool. Much data was likely to become unavailable due to the technological and market changes in this sector.[28]

On 26 September 2005 the Commission submitted a proposal for a directive on the same subject-matter of the draft framework decision.[29] It was based on Article 95 and intended to amend Directive 2002/58. For a while the two drafts co-existed. In December 2005 the Council decided to support the Directive.

[20] Art. 13(1)d.

[21] Art. 15(1).

[22] Conclusions of 20/09/2001.

[23] The Council was requested to put forward proposals for measures on data retention by service providers. *See* declaration on combating terrorism of 25/03/2004.

[24] The need to swiftly adopt common rules in the area of data retention was emphasised in the Council declaration of 13/07/2005.

[25] The legal bases were Art. 31(1)c and 34(2)b. *See* Council document 8958/04 of 28/04/2004, available at the Council's register.

[26] Ibid.

[27] Art. 5.

[28] For example, as a result of consumers' requests for flat-rate services, the need to store traffic data was decreasing to the extent that it was becoming superfluous for companies to retain traffic data. *See* Council document 8958/04, *supra* n. 25.

[29] COM (2005) 438 final.

The Commission took the view that the correct legal basis for imposing obligations on electronic communication service providers lay in the first pillar.[30] By somewhat changing the wording of Article 15(1) of Directive 2002/58, it stated that the latter had already dealt with the retention of traffic data. In reality, as previously mentioned, that Directive gave discretion to national authorities in this respect and no action at EC level was envisaged. This was due to the fact that the member states at that time could not agree on the terms of a measure at EC level in this area.[31]

According to the Commission, any further initiative on the retention of traffic data should be adopted through a first-pillar measure, lest Article 47 TEU be breached.[32] The concession was made that access to and exchange of personal data by law enforcement authorities could be regulated through a third-pillar initiative. It also was made clear that international co-operation between law enforcement authorities, which was an essential aspect of the draft framework decision, did not come within the scope of the proposed directive but should be regulated separately via a third-pillar measure or in the framework of existing mutual legal assistance Treaties (this was the favoured option).[33]

The Commission's proposal differed from the draft framework decision in many respects. Quite naturally, emphasis was placed on the negative impact that different national legislations have on the electronic communication market.[34] For instance, the retention period of data held by electronic communication providers was shorter than that envisaged by the third-pillar draft measure.[35] It furthermore held a reimbursement scheme: compliance by the electronic communication providers with the Directive would be beneficial to 'public security' (recital 13) but implied significant additional costs[36] for them which the member states would be obliged to compensate (Article 10). This provision, as well as the one limiting the retention period to a maximum of one year, were considered to be essential to the respect of the principle of proportionality.[37]

[30] Annex to the proposal for a directive of the European Parliament and the Council on the retention of data processed in connection with the public electronic communication services and amending directive 2002/58, SEC (2005) 1131, of 27/09/2005, available at the Council's register.

[31] Ibid., p. 10.

[32] Ibid., p. 10-11.

[33] Ibid., p. 11.

[34] Recital n. 6 of the proposal for a directive.

[35] It is between 6 months and 1 year in the Commission's proposal whereas the draft framework decision extended it to 12 and 36 months.

[36] These are related to storage and to the request to deal with the requests for access to data. These costs vary depending on the kind of data to be stored, the length of the retention period and on whether these period are harmonised throughout the Union. *Supra* n. 30, p. 7.

[37] COM (2005) 438, p. 7.

In the final text of the Directive, which was adopted with the full involvement of consultative bodies such as the 'Article 29 data protection working party' and the European data protection supervisor (EDPS),[38] the provision establishing the principle of cost reimbursement was deleted[39] and the data retention period was extended to cover a range between six months and two years from the date of the communication.[40] Finally, it is worth mentioning that the Directive resuscitates a provision of the draft framework decision (Article 5) obliging member states to adopt measures granting access to data retained to the 'competent national authorities'.[41] However, the draft framework provision was not entirely reproduced: the adjective 'national' proves that cross-border access to the data is not possible on the basis of the Directive.

In March 2006, the Council approved the draft Directive by qualified majority. Ireland, which had enacted legislation on data retention with a retention period (up to three years) longer than that provided for by the Directive (up to two years), was one of the countries to be outvoted and as announced during the voting procedure of the concerned measure, on 6 July 2006, challenged the newly adopted instrument before the Court of Justice, supported by the Slovak Republic (which also voted against).

The grounds of the challenge

Ireland claimed that the Directive's legal basis was inappropriate. The institutions, it said, should have adopted a framework decision. It reasoned that, as the Court stated in the PNR ruling, the centre of gravity of measures based on Article 95 EC is the harmonisation of national measures for the purpose of ensuring the functioning of the internal market. By contrast, according to Ireland, the contested directive primarily concerns the fight against crime.[42] Therefore, in light of

[38] The opinion of 'the Art. 29 working party' is mandatory under the general data protection regime, set out in Directive 95/46. The EDPS's advice was sought by the Commission while drafting the draft directive.

[39] However, as a *quid pro quo* to meet the electronic communication undertakings' concerns on the high costs associated by Directive 2006/24, the Commission committed itself to take due account of the benefits in terms of public security impact on society of data retention obligation and of the necessity to reimburse service providers for the additional costs incurred in complying with the Directive, when assessing the compatibility of national reimbursement schemes with the state aids provisions of the TEC. *See* 'Statement of the Commission', Council document 5777/06 ADD 1 REV of 17 Feb. 2006, available on the Council's register.

[40] Art. 6.

[41] This is Art. 4, *infra* n. 92.

[42] Par. 30-31.

the PNR judgment, the contested act could not be based on Article 95 EC.[43] At most, the internal market objective was ancillary to the latter.[44]

A further argument was related to the Community's incompetence to amend the 2002 first-pillar directive so as to regulate an activity falling under Title VI EU and, as such, is outside the scope of application of that directive.[45] The Irish put forward that the adoption of an instrument regulating data retention does not 'affect' the provisions of Directive 2002/58, within the meaning of Article 47 TEU. This provision was said to tolerate 'a random or incidental overlap of unimportant and secondary subject matter between instruments of the Community and of the Union.'[46]

The front of supporters of Article 95 as the appropriate legal basis was heterogeneous. In addition to the Parliament, the Council and the Commission, it included two member states (Spain and the Netherlands) and the European Data Protection Supervisor (EDPS). The reasons behind the Parliament's stance are fairly obvious: its powers within the first pillar are the fullest. The data protection supervisor's position is also understandable: data protection standards guaranteed by Directive 95/46 were higher than those in the proposed Framework Decision.[47]

In favour of Article 95 as the correct legal basis, it was put forward that the impugned act intends to harmonise different national measures for the operation of service providers.[48] This could not be done by a third-pillar measure without breaching Article 47 EU.[49] According to the latter: '[…] Nothing in this Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them.' The fact that the fight against crime and terrorism was a determining factor in adopting the Directive did not render Article 95 inappropriate.[50] The reference to the investigation, detection and prosecution of serious crime in Article 1(1) of Directive 2006/24 only served to indicate the legitimate objective of the restrictions imposed on the rights of individuals.[51] The 'defendants' also reasoned that Directive 2002/58 could

[43] Par. 86.

[44] Par. 31.

[45] *See* Art. 1(3) of Directive 2002/58.

[46] Par. 32.

[47] A general third pillar instrument on data protection was adopted with the Framework Decision 2008/977/JHA of 27 Nov. 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ* [2008] L 350/60.

[48] *See* par. 42 (Council), 50 (Commission), 47 (Spain and the Netherlands), 53 (European Data Protection Supervisor).

[49] Par. 45 (Council).

[50] Par. 43 (Council).

[51] Par. 52 (Commission).

only be amended properly by means of a Community instrument.[52] Finally, the Parliament contended that the contested directive respects the separation between the areas of competence of the first and third pillars. Indeed, it leaves to member states the setting out of the conditions for access to and processing of retained data and does not provide an obligation to deliver data to law enforcement authorities of a non-member state, as in the case of the EC-USA PNR agreement.[53]

The opinion of Avocate General Bot

The AG suggested rejecting Ireland's action.[54] He reached this conclusion through a line of arguments switching from positive reasons, proving that Article 95 was the required legal basis, to negative ones, showing that the provisions of Title VI of the TEU could not support the adoption of Directive 2006/24. In substance, he showed that the impugned measure has only the appearance of a third-pillar measure and displayed several arguments to justify his conclusion that the absence of harmonisation measures would affect the functioning of the internal market in electronic communications.[55]

He acknowledged that the rationale of the obligation to retain data, imposed on providers of electronic communications services, lies in the fact that it facilitates the investigation, detection and prosecution of serious crimes by providing an effective investigative tool. However, this circumstance is not sufficient to make it a third-pillar matter. Moreover, he reasoned that the fact that the legislator's recital on the need for data retention in the fight against crime is motivated by the need to justify the EC's interference with the right of individuals to privacy. It has nothing to do with the choice of the legal basis. He argued that Article 95(3) empowers the Community to ensure the functioning of the internal market and to pursue a public-interest objective such as guaranteeing a high level of security within the Community. The AG's point is not very convincing since Article 95(3) does not mention 'security' at all.

Another of the AG's arguments was that the provisions of Title VI do not cover the subject-matter of the contested Directive. The objective of investigating, detecting and prosecuting serious crime has a criminal aspect; however, this does not mean that all measures pursuing that objective should be brought under the third pillar. This would amount to unduly extending its scope.[56] Looking at

[52] Par. 49 (Spain and the Netherlands), 54 (Commission). Along these lines, *see* par. 51 (Commission), par. 54 (EDPS).

[53] Par. 38.

[54] *See* Opinion of AG Bot of 14/10/2008, in case C-301/06 *Ireland* v. *Parliament/Council*, nyr.

[55] Par. 85.

[56] Par. 101.

https://doi.org/10.1017/S157401961010008X Published online by Cambridge University Press

the content of the Directive, Bot noted that the Directive contains 'measures which relate to a stage prior to the implementation of police and judicial cooperation in criminal matters' and does not involve any *direct* intervention by the law enforcement authorities of the member states.

Drawing on the Commission's position during the procedure leading to the adoption of the Data Retention Directive, the AG also suggested how to define the boundary between the first- and third-pillar measures on access to traffic data. The former empowers the Community to harmonise the conditions under which providers of communications services must retain users' data. The latter enables the Union to lay down the conditions under which the competent national law enforcement authorities may access, use and exchange retained data in the carrying out of their duties. He acknowledged that such a division is not ideal and that a single measure, encompassing both aspects of data retention, would be preferable. However, the constraints of the constitutional architecture of the Treaty in its current form cannot be ignored. A clarification on the boundaries between the spheres of action covered by the different pillars is required by the principle of legal certainty.

In the last part of the opinion, Bot carefully examined the consistency of the PNR ruling with his finding that Article 95 is the correct legal basis for the data retention directive. In that ruling, the Court found that the proper legal basis for the EC/USA agreement was in the third pillar. That agreement is a form of international co-operation with the public authorities of a non-member state and concerns a stage subsequent to the initial collection of data by airline companies; moreover, the compulsory disclosure of data to a national body for security and law-enforcement purposes, is not fundamentally different from a *direct* exchange of data between public authorities, for example in criminal investigations. These characteristics make the PNR case fundamentally different from the case at hand.

Turning to the provisions of Directives 95/46 and 2002/58, the AG made a distinction between those excluding certain activities from the scope of the Directives and those merely authorising restrictions to data protection. He notes that both types of clauses mention similar public interest objectives. However, this is not sufficient 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. The relevant factor is whether the processing of data concerns an activity that is excluded from the scope of application of relevant Community law. If the operation of Community law is merely restricted, then the processing for public interest objectives remain within the realm of Community law. In the PNR ruling the contested decision concerned the processing of data for specific state activities, a subject-matter which was *excluded* from the scope of application of Directive 95/46. The contested Directive, however, does not harmonise conditions for

access to data and their use for specific state activities. It simply restricts the Community system of data protection.

Finally, AG Bot holds that accepting third-pillar provisions as the legal bases of the data retention directive would be contrary to Article 47 EU. Quoting the *Ecowas* case, he affirms 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.[57]

The judgment of the Court

The Court confirms the legality of the contested directive. However, the arguments raised in support of Article 95 TEC only partially overlap with those of the AG.

The Court does not start with an analysis of the objective and content of the contested measure, as one might have expected. It refers to the 'tobacco advertising II case'[58] judgment and holds that Article 95 enables the Community to act either to strike down *existing* and *future* obstacles to the functioning of the internal market, on the condition that the latter are likely to arise.[59] The Court emphasizes that the existing conditions for data retention vary depending on the nature of the data retained and the periods of retention. The latter jeopardises the creation of a 'level playing field' of service providers since they have significant economic implications.[60] Moreover, the regulatory differences are likely to increase since 'it is entirely foreseeable'[61] that the member states, which did not yet act in this field, will introduce new rules. As a result, it is also predictable that the passage of time will make the impact on the internal market more serious.[62]

The Court's second argument concerns the relationship between Directive 2002/58 and the contested Directive. The Court claims that the latter amends the former.[63] Since Directive 2002/58 is based on Article 95, Directive 2006/24 cannot be founded on a provision of the Union Treaty without infringing Article 47

[57] Par. 132.
[58] Case C-380/03 *Germany* v. *Parliament/Council* [2006] *ECR* I-11573.
[59] Par. 64.
[60] Par. 68.
[61] Par. 70.
[62] Par. 71.
[63] Par. 73.

thereof, at least 'in so far as the amendment of Directive 2002/58 effected by Directive 2006/24 comes within the scope of Community powers.'[64]

Thirdly, the Court analyses the legal basis by briefly looking at the *substantive* provisions of the contested act.[65] It observes that the Directive essentially regulates the activities of service providers and concerns only data that is generated or processed in the course of the provision of the relevant communication services and is closely linked to the exercise of commercial activity of the service providers. Thus, the contested Directive does not govern access to data or the use thereof by the police or judicial authorities of the member states:

> These matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the provisions of that directive, as is stated, in particular, in recital 25 in the preamble to, and Article 4 of, Directive 2006/24.[66]

The Court, without even looking at the objectives of the Directive, finds that the content of this measure essentially concerns activities of service providers in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty and, concludes that

> In light of that substantive content, Directive 2006/24 relates predominantly to the functioning of the internal market.[67]

The final part of the ruling refers to the PNR judgment. The Court is remarkably brief in ruling out its relevance for the present action:

> Unlike [the adequacy decision], which concerned a transfer of personal data within a framework instituted by the public authorities in order to ensure public security, Directive 2006/24 covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law enforcement purposes.[68]

Comment

The legal basis of internal market measures with a security dimension

The case is not the first in which the Court has to decide the legal bases of 'inter-pillar' measures and hence the problem of Community *versus* Union competence.

[64] Par. 78.
[65] Par. 79-84.
[66] Par. 83.
[67] Par. 85.
[68] Par. 91.

https://doi.org/10.1017/S157401961010008X Published online by Cambridge University Press

Notorious predecessors are on the one hand *Ecowas*[69] (first pillar v. second pillar),[70] and on the other PNR,[71] 'ship-source pollution',[72] 'environmental crime'[73] and 'airport transit visa'[74] (first-pillar v. third-pillar). The Irish challenge can be added to the latter line of cases.

In most cross-pillar litigation, except for PNR and partially 'ship source pollution',[75] the Court has opted in favour of the Community's competence, thus confirming its wide breadth.[76] Ever since the 'environmental crime' case the Court has resorted to the theory of the 'centre of gravity'[77] to allocate the legal basis of secondary legislation. In particular, the *Ecowas* case stands out for the Court's detailed analysis of the 'objectives and the content' of the contested decision. These were scrutinised at length in order to verify the possible infringement of Article 47 EU. By contrast, in the present case the Court is remarkably brief and it seems to apply the 'centre of gravity' test in a selective manner. The Court only focuses on the content of the challenged measure,[78] despite the applicant's insistence that the triggering factor of the impugned directive was the fight against crime and terrorism.[79] The Court does not pay attention to the fact that the contested Directive serves law enforcement objectives insofar as the data collected from electronic communication providers is used by national authorities to combat crime. By looking only at the content of the contested directive and underplaying its third-pillar objective, the Court confirms its role as protector of the Community

[69] *See supra* n. 10.

[70] A further case in which the Court examines the border between the first pillar and second pillar, is C-403/05 *European Parliament* v. *Commission* [2007] *ECR* I-9045. For a comment *see* M. Cremona, 45 *CMLRev.* (2008), p. 1727.

[71] *See supra* n. 6.

[72] Case C-440/05, *Commission* v. *Council* [2007] *ECR* I-9097.

[73] *See supra* n. 9.

[74] Case C-170/96, *Commission* v. *Council* [1998] *ECR* I-02763.

[75] In this case the Court found that the content of the contested framework decision fell only in part within the Community's sphere of competence (par. 69-74): the provisions on the type and level of the criminal sanctions fell outside it. However, since the provisions of the framework decision, outside the first pillar, were inextricably linked to the others, the impugned act was to be annulled in its entirety.

[76] A. Dawes, O. Lynskey, 'The ever-longer arm of EC law: the extension of community competence into the field of criminal law', 45 *CMLRev.* (2008), p. 131.

[77] Case C-176/03 (environmental crime) *supra* n. 9; C-300/89 *Commission* v. *Council* (*Titanium dioxide*) [1991] *ECR* I-2867. This is the devise used to allocate the legal basis of first pillar measures in order to decide upon the legal foundations of cross pillar acts. For an in depth analysis of litigation on cross pillar acts *see* R. Van Ooik, 'Cross pillar litigation before the ECJ: demarcation of Community and Union competences', *EuConst* 4 (2008), p. 408.

[78] In par. 85 the Court states: 'In light of that substantive content, Directive 2006/24 relates predominantly to the functioning of the internal market'.

[79] Par. 58.

competence against the 'incursions' of the Union. This case consolidates the judicial trend of policing the border between the first and third pillar in favour of the former. In that respect, this case is in line with the earlier case-law on Article 47 EU.[80]

In the present case, the Court clarifies that measures designed to harmonise national measures in order to ensure the functioning of the internal market can be founded on the first pillar even if they have a security dimension or objective.[81] It is unclear, though, whether the security objective should be ancillary or could also be predominant. In *Ecowas*, which may be taken as the paradigm of an accurate analysis of the centre of gravity of a measure, the Court held that if the challenged decision *predominantly* had aimed at a CFSP objective the Union would have been competent.[82] The application of *Ecowas* to the present case could have led the Court to exclude the first-pillar legal basis in case the *main* objective of the Directive was found to be the fight against crime. Regrettably, the Court did not have the chance to elaborate on this issue since it did not examine the objective of the measure. This may have been done on purpose to defend the Community's

[80] *See* P. Koutrakos, Editorial, 'Development and foreign policy: where to draw the line between pillars?', 33 *ELRev* (2008), p. 289. In *Ecowas* the Court preserved the *acquis communautaire* against any form of encroachment from the Union acting in the second pillar. However, *see* the point made by R.A. Wessel, C. Hillion, 'Competence distribution in EU external relations after *Ecowas*; clarification or continued fuzziness?', 46 *CMLRev.* (2009), p. 565, 567 on the Court's interpretation of Art. 47 TEU. They note that in para. 33 the Community judges seem to restrict the scope of application of this provision. Here, the Court holds that its task under this provision is to ensure that acts falling under Title V, and which by their very nature are capable of having legal effects, do not encroach upon the powers conferred by the EC Treaty on the Community. By limiting its assessment to acts of the second and third pillar that are endowed with legal effects, the Court seems to refuse to police the Community sphere of competence against the incursions of inter-governmental acts of political nature, such as the European Council conclusions. Perhaps, the risks, highlighted by the authors, that this kind of acts could actually affect the Community powers are more apparent than real. For a different view on the judgment, *see* another author who criticizes the broad interpretation of Art. 47 TEU. Van Vooren, *supra* n. 11, p. 19. *See also* J. Heliskoski, 'Small Arms and Light Weapons within the Union's Pillar Structure: An Analysis of Article 47 of the EU Treaty', 33 *ELRev*. (2008), p. 898.

[81] A parallel may be established between the position of the Court in the present case and that in the Tobacco advertising case I. Here, the Court had found that the contested directive (Directive 2001/37) could be validly adopted under Art. 95 since its object was the improvement of the conditions for the functioning of the internal market. The fact that public health was a decisive factor in the choice of adopting the contested harmonising measure did not prevent reliance on Art. 95. *See* case C-491/01 *British American Tobacco (Investments) and Imperial Tobacco* [2002] *ECR* I-11453, par. 77.

[82] *See* paras. 71-72 of the *Ecowas* case: 'Nevertheless, a concrete measure aiming to combat the proliferation of small arms and light weapons may be adopted by the Community under its development cooperation policy only if that measure, by virtue both of its aim and its content, falls within the scope of the competences conferred by the EC Treaty on the Community in that field. That is not the case if such a measure, even if it contributes to the economic and social development of the developing country, has as its main purpose the implementation of the CFSP.'

competence at all costs. The alternative explanation is that the Court has changed the legal basis test.

Be as it may, it is submitted that had the Court examined the objectives, there would have been in this case room for upholding the Directive along the lines of the AG's opinion. The Court could have stated that the objective of fighting crime overlaps with that of protecting the internal market. The content of the measure points to Article 95 as it concerns harmonising the conditions for data retention obligations. As a result, a first-pillar measure is required by Article 47 EU, as interpreted in *Ecowas*. In that decision, the Court confirms that when a measure on account of its aim and objective could have been adopted on the basis of both the EC Treaty and the EU Treaty, the former should be given precedence.[83]

The use of plural legal bases, corresponding to the different objectives pursued by the measure, could have been the alternative solution. However, while this is admissible exceptionally, in the case-law on single-pillar measures with a plurality of objectives without one being incidental to the other,[84] it is precluded in the context of cross-pillar measures.[85] This preclusion no longer operates after the entry into force of the Lisbon Treaty.

In my opinion, the contested Directive could indeed be validly enacted under Article 95, although it is acknowledged that the internal market rationale does not come out clearly in the text of this act. Indeed, as the Directive contains scant provisions proving that the variety of national legislation on data retention is liable to affect the internal market, the Court was forced to use the '*evidence submitted to the Court*'[86] in addition to a textual analysis. For example, one of the reasons which is crucial to understand the need for EC legislation in this area is the 'cost' issue. As is emphasised by Bot, service providers face significant costs in retaining data and this burden is proportional to the retention period and the amount of data to be retained.[87] This crucial aspect is not mentioned in the (final) text of the Directive. Bot is forced into interpretative acrobatics, i.e., to integrate the few words of recital 4 to 6 of the Directive with information found in the Commission's internal documents or in order to prove that the Directive facilitates the development of the internal market for electronic communications by providing common requirements for service providers.[88]

[83] Par. 60.

[84] Case C-178/03 *Commission* v. *Parliament and Council* [2006] *ECR* I-107, paras. 42 and 43; Case C-336/00 *Huber* [2002] *ECR* I-7699, par. 31; Case C-281/01 *Commission* v. *Council* [2002] *ECR* I-12049, par. 35; and Case C-211/01 *Commission* v. *Council* [2003] *ECR* I-8913, par. 40.

[85] *See* par. 75-76. As it has been noted, in *Ecowas*, no much explanation is provided for the presumed impossibility to use legal bases in different pillars. *See* Van Ooik, *supra* n. 77, p. 409.

[86] Par. 67, 69, 71.

[87] Par. 86.

[88] *See* his point on Art. 12(2) of Directive 2006/24 in par. 88.

Despite the defective statement of reasons for the contested Directive, it is credible that it improves the functioning of the internal market.[89] Given that the storage of data is costly, disparity of national measures on traffic data to be retained by electronic communication providers, and in particular the different length of time of the data retention obligation, could jeopardise the achievement of a level playing field for undertakings operating in the business of electronic communications. Service providers subject to very stringent data retention requirements would be at a disadvantage compared to competitors operating in countries where data retention standards are looser.[90] This is not to say that the fight against crime or terrorism has nothing to do with data retention obligations. National authorities enacted measures in this area with the *main* purpose of fighting against organised crime. However, one should distinguish between the objective of the *national measures* and that of the *Directive*, which is to safeguard the functioning of the internal market by removing obstacles created by national measures inspired by 'security preoccupations'.

A further point of interest is whether 'twin acts' could have been adopted, i.e., one within the first pillar and the other within the third one[91] in lieu of a single directive. Would this be a viable alternative legislative path, given the content and the aim of the Directive? It is submitted that this would be possible. Indeed, it is not entirely true that the Directive does not concern access to retained data by competent authorities. Let us consider Article 4.[92] Neither the AG nor the Court examines this provision in an appropriate manner.[93] This provision obliges mem-

[89] *Contra*, *see* Van Ooik, *supra* n. 77, p. 403; V. Mitsilegas, 'The external dimension of EU action in criminal matters', 12 *Eur. Foreign Aff. Rev.* (2007), note 123, p. 483; N. Lavranos, 'Data retention: first or third pillar instrument for fighting terrorism?,' *European Law Reporter* (2009) 4, p. 162. These authors argue that the main purpose of the challenged Directive was the fight against crime or terrorism and that the internal market is only a smokescreen.

[90] Does the Directive actually create a level playing field between service providers? This is an issue subject to discussion. It may be argued that an act setting out a retention period ranging between 6 and 24 months can hardly be defined as an instrument creating a level playing field.

[91] For examples of 'twin acts' adopted in the field of the area of freedom security and justice, *see* V. Hatzopoulos, 'With or without you ... judging politically in the field of Area of Freedom, Security and Justice, 22 *ELRev.* (2008), p. 52. The adoption of twin acts is no longer needed with the entry into force of the Lisbon Treaty. Indeed, the disappearance of the pillars implies that an EU act may now have simultaneous legal bases concerning matters that in the pre-Lisbon age would have fallen under the former first and third pillars.

[92] Art. 4 reads as follows: 'Member States shall adopt measures to ensure that data retained in accordance with this Directive *are provided only to the competent national authorities* (emphasis added) in specific cases and in accordance with national law'.

[93] Bot does not ignore Art. 4. However, his opinion touches on it very quickly and does not really explain how this provision was inserted into a first-pillar act. The Court does not even take this provision into consideration and bluntly denies that the Directive deals with access to data of public authorities.

ber states to adopt measures granting access to data to competent (national) authorities and as such, should have been inserted in a third-pillar instrument. Although Article 4 was intended to limit the conditions under which competent authorities are granted access, it cannot be denied that it at the same time enables law enforcement authorities to get hold of retained data. However, this does not mean that the Directive should have been anchored in the third pillar. The Court could have surgically extracted[94] this third-pillar provision to locate its legal basis in the third pillar. Article 4 is an isolated provision and is not 'inextricably linked' to the other provisions of the Directive within the meaning of the 'ship source pollution case'.[95] Hence, the Court could have declared that Article 4 has no basis in the first pillar and therefore it should have been inserted into a third-pillar instrument. Consequently, a third-pillar act, holding the text of Article 4, could have been adopted in order to make the fight against crime and terrorism more effective.

The inevitable consequence of this twin-track approach would have been a patchwork-like legislative framework. This was an inherent feature of the architecture of the Treaty prior to the Lisbon Treaty. The simplification brought about by the new Treaty in this respect is certainly salutary. It could also be argued that the Court did not opt for the artificial solution of 'twin acts' in anticipation of the entry into force of the Lisbon Treaty, under which the two pillars involved are merged. However, as has been noted, this would have been inappropriate as it amounts to adjudicating on the choice of legal foundations of Community measures on the basis of non-objective factors.[96] This is contrary to the principle of legal certainty.

Why is the present case different from the PNR ruling?

The Irish challenge has special links with the PNR case since they both question the legality of measures aimed at promoting the security[97] of EU citizens in the face of crime and terrorism through means that restrict their right to data protec-

[94] I borrow this terminology from Wessel and Hillion, *supra* n. 80, p. 575. These authors point out that a clarification is needed on the detailed application of the centre of gravity test doctrine in cross pillar cases. For example, it is not clear whether the Court should look at the content or objective of each and every provision or at the overall content of the measure to determine its main thrust (p. 576-577).

[95] In this case (C-440/05, *supra* n. 72) the fact that the first pillar provisions of the framework decision were 'inextricably linked' to the third pillar provisions (*see supra* n. 75) had led the Court to annul the contested act.

[96] *See* Lavranos, *supra* n. 89, p. 162.

[97] On the ambiguity of the notion of 'security' as protection against criminality and terrorist attacks or protection against (over)intrusive measures by law enforcement authorities, *see* 'Editorial', 45 *CMLRev.* (2008), p. 5.

tion. However, their outcome is opposite: whereas in the latter case, the challenged measures should have found their locus outside the first pillar, in the former one, Article 95 EC is confirmed to be the correct foundation of the 'data retention' Directive. A possible explanation for this contrast is that the Court carries out a legal basis test that is different depending on the nature of the contested act (i.e., an EC act concluding an international agreement or an EC measure). This issue is subject to debate[98] but looking at the case-law there is no concluding evidence that there is such a differentiation.

In my opinion, the divergent results of the two cases are amenable to the different *content* of the challenged acts. The AG's distinction between the contested Directive and the PNR agreement is more convincing than that of the Court. In particular, the line he draws between exclusionary and restricting clauses of Directives 2002/58 and 95/46 is persuasive. The former did not exclude data retention from its scope; on the contrary, it authorised restrictions on data protection for the purpose of retaining data and therefore the Community institutions were empowered to enact Directive 2006/24. By contrast, the latter did not apply to the activities of public authorities; the PNR agreement was all about access of border authorities to registration data of passengers; hence it came out of the scope of Directive 95/46.

Alternative grounds to challenge Directive 2006/24

Neither in the PNR case, nor in the present action, did the Court have the chance to consider (many would say 'avoided considering') the sensitive issue of human rights standard assured by the impugned EC legislation. However, to be fair, it should be mentioned that, in contrast to the PNR case,[99] the applicant in the present action did not question the Directive's compliance with the right to privacy,[100] although the Council did raise the issue.[101] Therefore, it was not strictly

[98] For a critical discussion of the case-law on the legal basis test for international agreements *see* M. Cremona, 'Defining competence in EU external relations: lessons from the Treaty reform,' in A. Dashwood and M. Maresceau (eds.), *Law and Practice of EU External Relations* (Cambridge, Cambridge University Press 2008), p. 39-42; P. Koutrakos, 'Legal basis and the delimitation of competence in EU external relations', in M. Cremona and B. De Witte, *EU foreign relations law: constitutional fundamentals* (Oxford, Oxford University Press 2008), p. 183.

[99] In the PNR ruling, the Parliament's challenge of the adequacy decision and of the PNR agreement was centered around infringement of the right to data protection. However, only the Advocate-General had considered possible violation of this right. He eventually concluded that the interference with this right was necessary and justified. *See* opinion of AG Léger, of 22/11/2005 in C-317/04 and C-318/04 *supra* n. 6.

[100] Par. 57. However, the Slovak Republic raised the issue of the privacy standards of the contested measure.

[101] According to the Council, supported, in this respect by the Parliament, the contested act does not breach Art. 8 of the ECHR since it serves a legitimate interest and complies with the proportionality principle (par. 46).

necessary to examine this ground. Nonetheless, this time the Court left the possibility of future challenges to the Data Retention Directive open.[102] A direct challenge to the Directive is clearly not possible since it is time-limited. However, these issues could be raised by private parties in the context of the plea of illegality against the contested measure, or national implementing acts.

NGOs and professional associations claim that the 2006 Directive violates the right to respect of private life and correspondence, freedom of expression and the right of providers to their property.[103] The opinion of the 'Article 29 data protection working party' was also very critical, to the extent that it questioned the necessity of general data retention measures and was convinced of the existence of less privacy intrusive approaches.[104]

By contrast, one author argues that overall, Directive 2006/24 adequately protects privacy. Indeed, data retention is regulated through a democratically enacted law, which overall respects the principle of proportionality. In particular, the scope of the data to be retained is narrow in that law enforcement authorities have access to data but not to the content of the communication, and the duration of the retention period is reasonable. Moreover, provisions on recordkeeping contribute to the proportionality of the measure and the provision making possible to retain data on 'unsuccessful calls' are supported by plausible arguments.[105]

In the author's opinion, the compatibility of the contested Directive with Article 8 of the ECHR or with the right to property[106] under Article 1 of the first Protocol of the ECHR is questionable. This is because, on the one hand, the violation of the right to privacy associated with the data retention obligation fails to comply with the proportionality principle. Indeed, the obligation imposed on service providers to retain traffic data of all users is very blunt since it caches all people without distinguishing different categories of users depending on them being a threat for the public order or not. On the other hand, it may be claimed that the costs for telecommunication undertakings associated with a fairly long retention period (up to two years) could be considered an impairment of the right to property and in particular of the proportionality principle, in case companies are not compensated for the costs incurred in complying with the obligation im-

[102] The Community judge emphasizes that Ireland challenged the legal basis of the contested Directive and not its compatibility with fundamental rights, arising from interference with the exercise of the right to privacy. *See* par. 57.

[103] F. Boehm, 'Confusing fundamental rights protection in Europe: Loopholes in Europe's fundamental rights protection exemplified on European data protection rules', *Law Working paper series*- Luxembourg (2009) 1, p. 11.

[104] *See* opinion 4/2005 of 21/10/2005.

[105] F. Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive,' 8 *Chi. J. Int'l L.* (2007), p. 249-252.

[106] For a suggestion that the right to property may be breached by data retention obligations, *see also* Breyer, *supra* n. 2, p. 374-375.

posed by member states to retain data. Indeed, as shown earlier, in the impact assessment carried out by the Commission to support its proposal for a Directive on data retention, two key aspects of the envisaged measure signalled that the proportionality principle was respected: these were the proposed retention period and the principle of cost reimbursement.[107] As already mentioned, in the final text of the Directive, the maximum retention period was stretched from one to two years; moreover, the principle of cost reimbursement went lost in the co-decision procedure and was replaced by a very 'imperfect substitute': a lenient Commission assessment of *possible* national reimbursement schemes in light of the state aid provisions of the TEC.[108] Both aspects lead us to question whether Directive 2006/24 still complies with the proportionality principle or whether it imposes on individuals excessive sacrifices.

A further ground of challenge of the Directive could be the infringement of the principle of subsidiarity.[109] This issue was raised in other cases in which the legal basis of a Community measure was attacked.[110] It may be argued that the Community legislator infringed that principle in enacting the Data Retention Directive, since cooperation between private undertakings and law enforcement authorities at national level was sufficient to make the fight against serious crime and terrorism effective and there was therefore no need for a Community initiative. Yet it is doubtful that this reading would withstand the Court's scrutiny. This is not only due to the fact that a challenge on subsidiarity grounds has never been successful. More specific factors are the following: the fight against crime/terrorism is only one of the reasons that led to the adoption of the Directive; the other has to do with the negative impact on the functioning of the internal market due to the existence of different national measures and to the likely adoption of new ones, increasing the existing regulatory disparity. Hence, a directive had to be adopted to ensure a level playing field for the operators affected by the data retention obligations. In conclusion, the described legislative measure was necessary to ensure that *both* its objectives, the fight against crime/terrorism and the safeguard-

[107] The other factors assuring respect of the proportionality principle were: the distinction between telephone and internet data and the limitation in the categories of data to be retained. COM (2005) 438, p. 7-8.

[108] This is because the Commission's decision to grant state aids is discretionary whereas under the Commission's proposal member states were obliged to reimburse for the costs associated with data retention obligations.

[109] For recent cases in which the breach of the principles of subsidiarity was invoked in support of the invalidity of Community acts, *see* Case C-110/03 *Kingdom of Belgium* v. *Commission* [2005] *ECR* I-02801 and Joined Cases C-154/04 and C-155/04 *The Queen, on the application of Alliance for Natural Health and Others* [2005] *ECR* I-06451. *See also* Case C-491/01 *supra* n. 81; Case C-377/98 *Kingdom of the Netherlands* v. *European Parliament and Council* [2001] *ECR* I-07079; Case C-233/94 *Federal Republic of Germany* v. *European Parliament and Council* [1997] *ECR* I-02405.

[110] *See* Case C-154/04 and C-155/04 and C-377/98, *supra* n. 109.

ing of the internal market, were achieved. National measures were clearly insufficient to attain the latter ones. The very fact that, as a matter of EC law, member states are now obliged to regulate this area, whereas before the adoption of the 2006 Directive most of them had not enacted national legislation on it[111] does not imply that the subsidiarity principle has been breached. Indeed, the adoption of new EC measures is the price to pay for improving the functioning of the internal market. When the latter objective is at stake, the threshold, triggering the adoption of EC legislation, was set at a very low level, as we know from the most recent 'tobacco products' case-law,[112] and in particular from the *Tobacco Advertising II* case (C-380/03), especially when the Court examines the likelihood of future obstacles to trade emerging.[113] In the present case, given that only a few member states had legislated on data retention, it is especially in the light of the latter category of obstacles that Article 95 appears to be justified for the concerned directive. However, it is regrettable that the text of the Directive does not provide sufficient explanations for its rationale. More emphasis should have been placed on how the future adoption of national legislation could create real obstacles to the functioning of the internal market.

[111] According to the Commission, the data retention regimes introduced or *planned* by the member states vary significantly. Not all of them have enacted legislation in this area: on the contrary, the majority of member states (about 15 on the basis of data of 2004) did *not* have mandatory data retention obligations; in half of the remaining countries, these obligations were *not* operational since implementing legislation was missing. However, in the few cases in which legislation was in place, the conditions for data retention widely differed. *See* SEC (2005) 1131, *supra* n. 30, p. 6.

[112] *See* Case C-491/01, *supra* n. 81; Case C-380/03, *supra* n. 58. For a more details on this low threshold, *see* the comment to the latter case written by M. Ludwigs, 44 *CMLRev.* (2007), p. 1167-1169.

[113] *See* par. 61 of C-380/03, commented by Ludwig *supra* n. 112, p. 1168-1169.

https://doi.org/10.1017/S157401961010008X Published online by Cambridge University Press