Public hearing in Case C-301/06 (1 July 2008)

Pleading of the EDPS

Mr. President, Members of the Court, Mr. Advocate General

It is an honour to plead in this important case before the Court of Justice. This case will allow the Court to specify the borderline between the different pillars in the EU-Treaty.

I will not elaborate on the main principles of the division in pillars. As agent of an authority in charge of supervising the processing of personal data and ensuring the rights of the data subjects, I will speak on the practical impact of this division on the Community-system for data protection.

It is of the utmost importance that the effectiveness (the 'effet utile') of this system be ensured. And this is only possible if all the obligations for operators to handle traffic data of their customers within their databases fall within the same legal framework.

Mr. President,

in the reasoning of the applicant the PNR-cases play a central role. The Irish government asks the Court to follow the approach adopted in the PNR-cases. I will also address the PNR-cases, but with the purpose of demonstrating that the facts of the present case are different to the facts of PNR.

More importantly however, the present case should be analysed in a much wider perspective than that of PNR. This case is about the scope of the system of data protection under Community law. This system is laid down in various legal instruments such as the general Directive 95/46 and Directive 2002/58, for the sector of electronic communications. I consider the Data Retention Directive, now contested before the Court, to be one of these instruments.

I would like to draw the attention of the Court to three aspects:

1. The nature of the data protection system,
2. The main differences with the PNR case, and
3. What if the present case were not covered by the first pillar.

The nature of the system of data protection

In *Österreichischer Rundfunk* the Court defined the scope of the Community system of data protection. The Court recognised that the system :

- has a wide scope,
- is defined in very broad terms
- and does not depend on the question whether in every specific case the processing of personal data has a connection to the free movement between the Member States.

The Court has said in this case: "*A contrary interpretation could make the limits of the field of application of the Directive unsure and uncertain*". I underline that Rundfunk was about the processing for purposes of public policy and even about the processing by government authorities.

Rundfunk also explains the main substance of the data protection system: This system does not prohibit data processing but requires that this processing complies with principles of data protection such as the principle of data quality. The system permits derogations, for instance for purposes of public policy. It also ensures that the data subject can exercise his or her subjective rights.

In short, it is a system with a broad scope, consisting of checks and balances in which the processing of personal data is subject to a number of conditions and limitations.

Article 13 of Directive 95/46 and Article 15 of Directive 2002/58 reflect this balanced nature. The directives do not exclude all processing activities for law enforcement purposes from their scope. But, they recognise the need for special, tailor made derogations for law enforcement in the Member States. The Data Retention Directive specifies the use of such derogation. It aims at harmonising the way in which the operators are obliged to retain data, under Article 15 of Directive 2002/58.

Of course, there is a limitation of scope, due to the scope of Community law, as further defined in Article 3 (2) of Directive 95/46 and in Article 1 (3) of 2002/58, and confirmed in the PNR-Judgement of the Court. But this limitation of scope should not harm the effectiveness of the system. This is all the more important, since under the third pillar of the EU-Treaty an equivalent system of data protection does not yet exist. Data protection in this area is currently fully a matter of national law.

This illustrates clearly what is at stake in the present case: the effectiveness of this system of data protection under EU-law. Effectiveness requires that the system can be applied in a consistent and coherent way, that the data subject can exercise his rights and that the enforcement is guaranteed.

Mr. President, this brings me to point 2.

The difference with the PNR-case

The PNR-judgment defines a borderline between the first and the third pillar in cases where personal data collected by private companies for commercial purposes are used for law enforcement purposes.

The Court distinguishes data processing in the course of commercial activities of the airlines and activities fully in the context of law enforcement, namely the transfer of data to the US-authorities.

Also in the present case, such a distinction can be made, yet with a different outcome. In the data retention directive, the regulated activities take place in the course of commercial activities. The directive does not regulate access by the police, nor transfer nor further use.

Instead, it stipulates that data processed by operators will not immediately be deleted when they are no longer needed for commercial purposes. They will be deleted later, after a fixed period.

Now, I will briefly describe the main differences with the PNR-case.

Firstly, the Data Retention Directive excludes the transfer from its scope. Secondly, it foresees no systematic transfer of data. Thirdly, it imposes data protection obligations on private companies, not on law enforcement authorities. Fourthly, it creates an overlapping of processing activities.

The first difference: The exclusion of data transfer.

The PNR-system was adopted to regulate the transfer to law enforcement authorities, in that case of the United States.

The data retention Directive does not regulate the transfer to law enforcement authorities. On the contrary, as clearly stated in Article 4 and Recital 25 of the data retention Directive, regulations on the transfer or access are left to national law.

Yet, on the contrary, the US-PNR system did not leave those aspects to national law. It regulated which competent authorities had access to the data and what mechanisms were used for access. It also regulated the further use, for instance, by determining when PNR data could be transferred by the US to other third countries.

The second difference: in the US-PNR system there was a systematic transfer of a given amount of data to the law enforcement authorities.

In the data retention case, there is no systematic transfer of data to the law enforcement authorities. On the contrary, each transfer has to be decided, at national level, on a case-by-case basis.

Only a very small number of all the data retained will necessarily be transferred. The decision to transfer will be made, under national law, by the police, the public prosecutor or the judge who requests the data for a specific case.

The third difference: in the US-PNR case, the relevant data protection obligations were imposed on the public authority receiving the data, not on the private company transferring them.

In the data retention case however, all these obligations remain the responsibility of the private company. The companies have to notify the data protection authority, they have to inform the data subject, they have to adopt security measures and they have to delete the data when the retention period has expired!

Back to US-PNR: When a data subject would like to exercise his right of access to the transferred PNR data, he has to make a request to the receiving authority. In the data retention case, he has to address the private company, that is, the electronic communications operator.

In a nutshell, electronic communications' operators will have to deal with the consequences and the obligations arising from the data retention directive on a daily basis, while law enforcement authorities will profit from its provisions only occasionally and in no case would have obligations imposed on them by the directive itself.

The fourth difference, the overlapping of processing activities: PNR data were only transferred for law enforcement purposes.

On the contrary, in the reality of the Data Retention Directive the same personal data will at the same time and for quite a while be retained for law enforcement purposes and for commercial purposes. These commercial purposes are foreseen in Article 6 of Directive 2002/58/EC. The operator needs to retain data for billing or for interconnection payments, or for marketing purposes and the provision of added value services. In these last situations, consent of the data subject is needed.

One could imagine the case where a data subject has given such consent. If he would like to sue the electronic communications operator because of a security breach that would have caused damage, he would base himself on the directives.

But, imagine if the Irish thesis were to be accepted, under which legal regime would the data subject seek remedy, under the first or the third pillar?

In this context, it is also good to mention that also the Community legislator did not want such uncertainty. The 13th Recital of the Data Retention Directive states that data should be retained in such a way as to avoid their being retained more than once. In other words: no distinction between the retention for commercial purposes and for law enforcement purposes.

To sum up, in the PNR case, the Court was confronted with a system where the main processing activity was the transfer of personal data to law enforcement authorities. But in the present case, the main focus is on the private operators. The obligations on the operators can not be detached from the first pillar without putting at risk the coherence and the effectiveness of the data protection system.

This brings me to the third and final part of my pleading.

What if this situation were to fall outside the first pillar?

I will sum up 6 undesirable consequences

1. Different data protection regimes

If the Court were to come to the conclusion that the subject matter of the data retention directive fell outside of the scope of Community law, the first consequence would be as follows.

In practice, data stored in a database of an operator would sometimes be covered by Community law and sometimes not.

For instance, the data protection directives would protect a customer of a Telephone Company as long as the data were retained for billing, or for the other purposes of Article 6 of Directive 2002/58. But, after payment of the bill or the end of the other commercial purpose this protection would no longer be guaranteed under Community-law.

2. No EU data protection when data are retained for law enforcement purposes

If the subject matter were to fall outside the first pillar, the protection of personal data would - within the present state of EU-law- be fully a matter of national law. Equally, there would be no uniform interpretation by the Court.

3. No respect of the data protection-system

The system includes tailor made derogations with specific conditions and safeguards for processing for law enforcement purposes. These specific conditions and safeguards under EU-law would no longer apply.

4. Not clear whether the 3rd pillar will give legal basis.

The fact that the subject matter is not covered by Community law, does not mean that the third pillar of the EU-Treaty will give an adequate legal basis. It is not obvious that the retention of data by private operators can be covered by 'Common Action in the field of Police Cooperation.'

Annulment would at least lead to legal uncertainty, until that question has been solved by the Court.

5. Annulment of the Data Retention Directive 2006/24 would also mean that Article 15 of 2002/58 is void.

If there is no legal basis for the Data Retention Directive 2006/24, there is no legal basis either for the exceptions under Article 15 of 2002/58 since it deals with the same

subject matter. In that case the conditions and limitations of Article 15 would not apply.

6. No guarantees that data subject can exercise his or her rights, such as the right of access and the right of correction.

The legal protection of the data subject, an essential element of the system of data protection would no longer be safeguarded, under EU-law.

Conclusion

Mr. President, Members of the Court, Mr. Advocate General,

with these pleading I have tried to demonstrate that an annulment of the directive as requested by Ireland would seriously affect the system of data protection under Community law. Moreover, such annulment would be contrary to the pillar structure of the EC-Treaty itself which does not exclude all activities relating to law enforcement from the first pillar of the Treaty. I fully support in this respect the submissions of the defendants in the present case.

Thank you.

Hielke HIJMANS

Agent of the European Data Protection Supervisor