SPEECH/04/549

Franco FRATTINI

Vice-President responsible for Justice, Freedom and Security

Data protection in the area of Justice, Freedom and Security

Meeting with the Joint Supervisory Authorities under the Third Pillar

Brussels, 21 December 2004

This is probably the first time such a meeting has ever been called.

For this reason, I must first of all thank you for inviting me to attend this meeting that brings you all together.

Many of you will have followed my hearing at the European Parliament.

You will have noted that on behalf of the Commission I pointed up the unanswered questions regarding data protection and stressed the need to set out a more coherent European strategy to guarantee an area of freedom, security and justice, while safeguarding the fundamental right of data protection which is now enshrined in two Articles in the Treaty.

The commitments we have given will shape the Commission's work: respect for the Charter and the Treaty, greater dialogue with the European Parliament and closer cooperation with the agencies safeguarding these rights.

Institutional relations between you and the Commission departments were already good. Commissioners Vitorino and Bolkestein worked very hard.

At times there may have been a time lag between communication of the work done by the various groups and a few problems in understanding the reasons underlying the various positions.

I am here today to say that we could do more, together, to perform our respective tasks more effectively.

The Commission has much hard work before it if it is to achieve one of the Union's three priorities: to step up police and judicial cooperation.

The agreements or decisions that set up your Joint Supervisory Authorities have assigned you sensitive tasks in specific areas supervising the complex case by case handling of personal data using the sensitive computer systems that have been developed.

This is still an important task, but one that may no longer meet today's demands.

So what are the challenges for the immediate future?

What new balances will it be necessary to find between privacy and security?

What will be the institutional framework for supervising data protection at European level in the medium and long term?

What will be your role? Will it be purely supervisory, or will you also have a major consultative role at the early stages of policy making?

How many data protection bodies will there be at European level, and which?

In the short term, what tasks can we accomplish together?

To answer these questions I believe it is important to start from the Resolution you adopted in Wroclaw on 14 September.

I am thinking in particular of your request that these problems should not be treated separately, agreement by agreement, but should be treated holistically, with the creation of an innovative institutional forum that will, at last, make it possible to take more strategic decisions.

We also know that while the SIS has had most success achieving the ambitious objectives set by the original Schengen Agreement, other common information systems have proved to be slow and flawed, and Europol, for example, is discussing the reasons for Member States' delays in transmitting data that do not stem from the need to safeguard privacy.

Lastly, we know that all these European databases pose legal and operative problems when we need to verify if and how the information can be collated at European or national level. We also know the risks of systems partially overlapping.

At national level, you do not always have the same powers.

At the same time, the Europol negotiations on the supply of data to third countries have shown that it is not easy to limit the number or type of authorities interested in data for the purposes of investigations.

In all these cases, we have run and still run the risk of letting down the police and judicial authorities (which are rightly keen to have new and more efficient instruments in the fight against crime and still find themselves forced to work with systems that need constant technological updating and are not always compatible, notwithstanding the considerable financial outlay). But we can also let down the agencies responsible for data protection (which are worried that access and the purposes for which the systems can be used will be increased without a clear legal basis, without sufficiently clear aims or without complying with important rules on data protection).

All this tells us that we have to identify new ways of increasing police and judicial cooperation and sharing data.

We may also need to identify together a new system of data protection.

We are not starting from scratch here; we must abide by the principles set out in the Charter of Fundamental Rights that have been enshrined in the Constitution for Europe, by rulings by the European Court of Human Rights, by the 1981 Strasbourg Convention No 108 and the European Council's Recommendations. There is also the collective experience of the Member States that, when transposing Directive 95/46/EC, almost always applied these different principles to the various ways of treating data gathered for security, justice and even intelligence purposes.

All this experience now needs to be built on and enhanced to take account of the times in which we are living.

This may require fresh general legal provisions at European level, but, there again, it might be enough to come up with a few general principles to be applied to the nature and drafting of future agreements.

The important thing is that we must complete the harmonisation of the data protection framework under the Third Pillar.

The safeguards for the people need to be maintained, respected and reviewed in the light of the development of networks, technologies and the types of data used, for example, in relation to the possibility of the extensive use of biometrics.

In the field of data protection, we may need to pay attention to the basic safeguards rather than to formal requirements, though these too are important.

Privacy and security are not diametrically opposed, nor is it a question of performing a balancing act, making sacrifices at the expense of the one or the other. In truth, one is the precondition for the other and vice versa. An essential condition for the right of security is the right to have human freedoms respected, as guarantees of the effectiveness of the actions of the public authorities.

I agree with you when you stress the need to pay attention to the principle of proportionality and to assess in advance decisions taken under the Third Pillar in terms of their impact on citizens' rights to avoid loopholes, fragmentations and overlaps between European measures and national solutions.

The Commission is prepared to do even more in this area and to be painstaking in the performance of the role assigned to it by the Treaties.

For some years now, the objective set by the Tampere European Council to make the European Union an area of freedom, justice and security has revealed the need for a coherent action plan to promote access to available databases and information sharing between the authorities concerned.

We must realise that some of the supposed obstacles thrown up by the notion of privacy are in fact the fruit of not entirely coherent policies, too much diversity between countries in some areas and, above all, of the fact that the detail of and speed with which rules have been adopted has prevented the development of an overall plan to interrelate systems centrally and at national level without giving rise to duplication or evading the principle of the objectives now enshrined at the highest level in Article II—68 of the Constitution for Europe. These difficulties are increased when ad hoc action is taken at European level, for example, regarding the sharing of information between police forces in connection with international summits or violence at football grounds.

This has given rise to recent proposals, aimed primarily at combating terrorism, that are intended to link up European systems and national archives as far as possible, notwithstanding the differences in current laws.

The Hague programme, which will take up the baton from Tampere for the next five years, introduces the principle of availability: police forces and judicial bodies will be able to access Member States' archives and obtain the information they need to perform the tasks they have been assigned.

I am aware of the concerns you have expressed regarding the proposals to increase the sharing of information: you have said you are aware of the need but are perplexed by the wording of the proposals and concerned that the principle of proportionality must be respected.

In this respect, the case of SIS II is definitely extremely important.

The European Parliament has received many of your suggestions regarding the Spanish proposals to amend the Schengen Agreement and I believe that the Italian and, subsequently, the Dutch presidency of the Schengen Joint Supervisory Authority worked particularly well, identifying the problems involved in creating new intelligent functions, access for Europol and Eurojust, and new objectives without changing the overall "static" structure of Schengen, which is based solely on a yes or no answer to the question whether there is any information on a given person.

The time has come for us to give a balanced response to the questions raised by the European regulators not only for the Joint Supervisory Authorities but also for the Article 29 Group, starting with the questions regarding the incorporation of biometric data in visas and passports, particularly in the light of the establishment of VIS and SIS II.

The problems stem in part from the fact that the First Pillar already contains harmonised rules with significant safeguards, while the Third Pillar has seen interruptions to the process to produce a handbook of guidelines and principles on data protection that began with the Italian initiative in 1999 and was continued under the Portuguese Union Presidency and by contributions from the Council's Legal Service.

The Hague programme, which has now provided for the "principle of availability" of data, completes the Tampere objectives and opens up some new opportunities, notably calling for the Commission to present proposals by 2005 that take account of the need to meet certain fundamental conditions regarding data protection (the lawfulness of the treatment, the integrity of the data, confidentiality guarantees, rules on access, the rights of the persons concerned and the need for supervision).

DG JLS is working on this and the time seems right to update the general principles in this field, starting with common standards for the supply of data to third countries and Interpol.

My Directorate-General as initiate a consultation involving the Ministries responsible for law enforcement cooperation as well as the Date Protection Authorities. The European Data Protection Supervisor was present in a meeting on 22 November. Data Protection Authorities are invited to a meeting on 11 January 2005. All these initiatives demonstrate the profound interests of the Commission in a continuous dialogue with the Data Protection Authorities.

I also know that you will be discussing these subjects at a meeting in The Hague on 28 January and you could subsequently take some important decisions at the European Conference in Poland in April.

This is all very useful because your role will be re evaluated. It is a positive sign that the Joint Supervisory Authorities have anticipated future developments by obtaining a joint secretariat, that the same delegates have been sent to the various meetings here in Brussels and that they have been meeting jointly for some months now.

In view of the provisions brought in by the Treaty, your advisory role could be extended beyond the specific remit of each Joint Supervisory Authority to developing a coherent reference framework in the same way as the Article 29 Group has done under the First Pillar.

The transfer of data to the USA concerning air passengers clearly shows that the distinction between the First and Third Pillars is becoming ever finer and that a horizontal approach needs to be adopted to examine rights and freedoms.

There are many points still to be hammered out. For example, the feasibility of:

- developing a core of guiding principles for the treatment of personal data under the Third Pillar, which might involve adapting the principles to the objectives pursued: for example, in the case of information sharing the principles set out in the Hague programme (p.22) could provide a suitable basis, while further principles could be developed to cover the creation of European databases;
- an a priori assessment of proportionality of any measures to be introduced in future, examining the impact of the proposal on fundamental rights, including the question of personal data protection, and going beyond the formal declarations contained in preambles to proposals;
- linking the adoption of new forms of police and judicial cooperation and the adoption of data protection guidelines: the deadline for the adoption of the latter is not laid down in the Hague programme and we have to assess the problem, taking account of legislative work already in progress;
- involving protection agencies more closely in drawing up guidelines in ways to be examined, and clarifying the role the Commission can play to make the best use of these contributions;
- paying special attention to the possibilities of applying the availability principle introduced in the Hague programme;
- developing special rules governing the transfer of data to third countries and other bodies, incorporating the principle that information received may be passed on with the prior consent of the party forwarding it;
- examining the current and future range of authorities conducting independent checks.

The involvement of data protection agencies from the outset can provide the added value needed and I must once again thank you for this opportunity, convinced as I am that we will all do our utmost to make the best practical use of the collaboration we all want to increase.