EUROPOL JSB TEN-YEAR ANNIVERSARY CONFERENCE
Brussels, 9 October 2008

Striking the Balance between the Fight against Crime and Fundamental Rights, New Developments and New Challenges

Francesco Pizzetti
President, Italian Data Protection Authority

On the occasion of celebrating ten years of activity of the Europol JSB, I think it appropriate to focus my presentation on the future challenges for data protection in the light of the developments in the law enforcement sector.

"Security" has become a key objective of political and governmental action both at world level and – above all – at European level.

Several initiatives have been implemented by the EU to foster the exchange of information and the fight against terrorism and so-called "serious" crime. Additionally, new proposals are put forward basically by the day, and some of them also entail the use of increasingly invasive, pervasive and – at times – intrusive monitoring techniques.

I am thinking, for instance, of the draft Framework Decision of the Council on the exchange of information under the availability principle; the Council Decision that incorporated the Prüm Treaty into the Community acquis; the expanded scope of use and access applying to the SIS II; the implementation of the Visa Information System, and the decision on fostering information exchanges in the EU.

Further light on the stance taken by the EU in this sector can be shed by two recent, significant documents. I am referring now to the Report of the Informal High-Level Advisory Group on the "Future of the European Home Affairs Policy" and the Public Consultation launched by the

European Commission on the "future" of the activities in the justice, freedom and security sector.

This is why I think it is necessary to briefly take stock of the rationale underlying these recent initiatives prior to addressing the role of Europol and data protection authorities (DPAs) in this new scenario.

If one considers the document of the Informal Group and the questions asked in the Commission's public consultation, the future challenge would appear to consist in implementing a *convergence* strategy. There is a shift from the mere "availability" of information to the veritable convergence of tools, facilities and staff with a view to streamlining the European policies in the fight against crime. Co-ordination, convergence, and co-operation: these are the words to be found most frequently not only in the documents I quoted, but also in all those that have been published so far in connection with the so-called Third Pillar.

Basically, the availability principle laid down in the Hague Programme, which is set to expire by end 2009, is being replaced by the convergence principle – this is the first major challenge we are facing.

The second major challenge to be addressed might be termed the "technological drift". A precondition for the convergence of information systems and tools is actually interoperability – i.e. facilitating the interaction between different systems, up to the veritable establishment of *shared information platforms*. Indeed, the Informal Group goes so far as to envisage a list of data categories that should be the subject of enhanced information exchanges pursuant to this all-pervasive EU strategy.

I believe that, given this scenario, we should first and foremost foster an in-depth analysis on the current, irresistible propensity by law enforcement bodies to collect and store – with the help of increasingly sophisticated tools – personal data that have been provided by citizens

exclusively for travel and/or business purposes. Let me only recall the PNR and SWIFT cases in this connection. We should establish to what extent this "*distorted*" use of the data in question – from commercial to security purposes – is appropriate. In other words, we should determine whether it is worth risking the malfunctioning of the economic system by committing public tasks to private entities – such as airline companies or banks.

However, this is just an example. One might also refer to the trend that is rife in many countries including Italy – whereby private entities installing video cameras for purposes related to their business are urged to connect with police and law enforcement authorities. This means that the video cameras, once installed, will also meet *ordre public* requirements. One might also quote the attention paid at European level to techniques such as body scanning, whereupon individuals can be seen naked during security controls. This is a terrifying, dismaying scenario in which citizens are at risk of being left powerless and defenceless vis-à-vis their controllers.

This is why it is appropriate to reflect on how to devise solutions to a situation in which European peoples are clamouring for increased security whilst the danger that personal data are used unlawfully is becoming increasingly real. It is an urgent requirement, partly because we are faced with a trend that might seriously jeopardize not only citizens' fundamental rights, but also the security and reliability of trade and economic, political and social relationships – which in turn might compound the risks brought about by globalization in a world that is increasingly lacking rules.

In the light of this new scenario, implementing the Lisbon Treaty is a major opportunity to upgrade and improve data protection legislation – partly because of the impact the Treaty is bound to produce on the operation of European institutions in view of the veritable communitarization of all the principles regulating societal relationships, including those related to the so-called Third Pillar.

It is actually unquestionable that further significant steps forward were made thanks to the Treaty along the lengthy road leading to the expansion of data protection principles. On the one hand it is established that data protection must be adequately taken into account in connection with internal and external security, whilst on the other hand it is envisaged that ad-hoc rules and legislation should be laid down in the said sectors with a view to enhancing respect for the principles that have long been affirmed and acknowledged within the framework of the First Pillar.

This is tantamount to stating that it is necessary to go beyond the current scenario, in which the protection of the data processed for law enforcement purposes is regulated by specific sector-related legislation and committed – if that legislation provides for setting up joint information systems – to dedicated groups of DPAs that work within the context of the individual organisations (Schengen, Europol, Eurodac). Conversely, a unified, general protection system should be implemented for all the data that are processed for the purposes that currently fall within the scope of Third Pillar issues.

Indeed, it is no chance that the rationale of the decisions and declarations adopted over the past few years by the European DPAs during their annual "Spring Conferences" has to do exactly with the points made above – i.e. the need to safeguard European citizens' fundamental rights within the framework of judicial and police co-operation, and to devise quicker, more effective responses to the risks arising out of the increasingly widespread collection of personal data for security purposes. Let me recall, in this connection, the Krakow Declaration (2005); the Budapest Declaration (2006); the Cyprus Declaration (2007) and the Position Paper on the Availability Principle; and the Rome Declaration (2008). The import of the principles laid down in those declarations is all the greater in the light of the new rules set out in the Treaty.

Taking account of this context and by having regard to the implementation of the Lisbon Treaty, I believe the decision taken by the European authorities in Cyprus to be especially important. On that occasion, a broader mandate was committed to the working party that had been addressing Third Pillar issues for some years – the so-called Police Working Party, which was aptly renamed Working Party on Police and Justice (WPPJ). Based on that decision, the

WPPJ started working under Italian chairmanship in order to discharge the mandate entrusted by the Conference – namely, to monitor data protection developments in the Third Pillar sector according to a co-ordinated, proactive approach.

Still, it is already the case that European data protection authorities and Third Pillar joint supervisory authorities such as the Europol JSB have no option other than taking up the challenges of convergence and technological acceleration by enhancing the convergence of their actions and plans and developing adequate technological skills.

Europol activities make up an excellent testing field in this regard. One of the objectives mentioned in the 2009 Europol Work Plan consists in enhancing Europol's role in connection with information exchanges at EU level. In practice, Europol is expected to turn into an information platform to make its analysis tools and information available to an ever widening number of authorities and organisations that deal with law enforcement in the individual Member States.

I think the Europol JSB is already fully aware of and ready to take up the challenges I mentioned shortly beforehand. However, there is little doubt that effective responses can only result from the convergence and consistency of the approaches adopted at EU level – indeed, at European level.

Therefore, it is necessary to establish links between the in-depth, albeit sector-related, activities performed by those supervisory authorities and the initiatives implemented in the Third Pillar sector by European DPAs – which I am representing here in my capacity as Chair of the WPPJ. We should clarify how to jointly improve co-operation between Member States in ensuring respect for fundamental rights and fostering, at the same time, the prevention of and fight against serious international organised crime.

This is one of the reasons why the WPPJ has been working for some time on drafting a sort of Joint Manual for the performance of inspections and/or audits in the law enforcement sector. I

believe this is a tangible example of the attempt to develop a shared, co-ordinated approach that can profit from the experience and skills available in the individual countries.

The wide-ranging experience gathered by the Europol JSB is especially helpful with a view to this common effort; however, it is actually more important to work in order to develop the co-operation between WPPJ and Europol JSB to the widest possible extent in accordance with convergence and mutual enhancement criteria.

We should join our voices in calling for real, effective empowerment of European supervisory authorities in order to adequately cope with the ongoing developments. The Framework Decision on data protection in the Third Pillar should be adopted as expeditiously as possible to clarify the general principles that are applicable in this sector. Technological convergence must not come along whilst the DPAs, including the JSBs/JSAs, are as yet unprepared to take up the new challenges. DPAs should be able to rely on technologically skilled staff and, where necessary, real enforcement powers. Controls must be effective and take place in accordance with co-ordinated policies – which are being worked out by the WPPJ as well.

Needless to say, this is not enough. European institutions should provide adequate responses, and such responses should not be limited to taking note of statements of principle. The many letters and communications sent by the WPPJ to institutional stakeholders over the past few months – to request clarification and draw attention to the views of European data protection authorities – have found little echo so far.

We should join our forces and increase our commitment towards ensuring that our shared efforts are acknowledged and taken into due account.

The WPPJ should enhance its role in close co-operation with all supervisory authorities and bodies.

European institutions should be aware of the importance of data protection and afford adequate recognition not only to the significant work carried out by the DPAs over the past years, but also to their commitment in developing new mechanisms to jointly organize and handle their

activities. Only in this manner can we rest assured that the area of freedom, security and justice will afford citizens not only increased security, but also justice and freedom to a greater extent.