26TH INTERNATIONAL CONFERENCE ON PRIVACY AND PERSONAL DATA PROTECTION

Wroclaw, 14-16 septembre 2004

M. Alex TURK,
President, Commission nationale de l'informatique et des libertés (CNIL), Paris

Session : « Transborder data flows and the challenges of world economy »

Presentation of the session

I – Emergence of transborder data flow issues and answers found by international data protection tools and data protection authorities

The issue of transborder data flows was simultaneous to the emergence of national concerns in the area of personal data protection during the seventies.

Thus, Convention 108 and the OECD's guidelines were prepared exactly when the first national laws were adopted in the early eighties to respond to that concern : the protection provided in countries members to such tools helps ensure the free flow of data. As a result, those tools only regulate data transfers between countries that are parties to the Convention or adhere to its guidelines.

Independent data protection authorities elaborated solutions pragmatically, on a case by case basis, when proposed transfers took place to third countries : thus they elaborated a first contractual solution (FIAT case in 1986), and then binding corporate rules for multinational companies (IBM case in 1990).

The European directive was the first international legal tool containing clear rules on the issues of data transfers to third countries. Its philosophy, reproduced by lawmakers in non-European countries (Hong Kong, Canada, etc.), and by the European Council (additional Protocol), is as follows :

- Personal data can freely circulate only between countries ensuring adequate protection to people whose data are transferred, whether under general or sector based laws ;

- Exceptions to this principle can be implemented, allowing that the data be transferred to a country that does not ensure such protection, when the transfer takes place in conditions ensuring its safety, including under a contract.
  Mr. Ulrich Dammann, from the German federal data protection authority will discuss this historic prospect, and provide parts of answers to the following questions : how does the system work ? Where do we stand ?

  Mr. Ken Anderson, deputy privacy commissioner of the Canadian Province of Ontario, will tell us that personal data transfers cannot be considered other than in a « security chain » logic, and that a transfer cannot be separated from its original processing ; he will describe the educational work of the Ontario authority in this area.

II – Complexity and simplification of transborder data flows control tools

In our discussions, we cannot avoid to discuss the issue of the complexity of legal tools developed to control transborder data flows to third countries, and the resulting need for simplification.

The complexity results not only from personal data protection rules, but also from the complexity of transborder flows reality and from the legal reality in countries located in various continents. Indeed, in order to give each organisation the possibility to transfer data following methods suitable for it, the implementation model of rules relating to data transfers had to be made more complex (the specific regime of adequate protection provided in the USA by the « Safe Harbour », contracts, binding corporate rules for multinational companies, etc.). **Thus the paradox is that it is mainly to simplify companies' procedures, in a globalised world, that the model has become complex.**

At any case, it is important to remind that no simplification project in this area can be considered other than to the extend it protects the rights of people whose data are transferred.

Thus, it is the responsibility of data protection bodies to ensure that those various tools are properly and consistently implemented and to make sure, in doing so, that those rights and their effectiveness are always protected.

It is also the responsibility of lawmakers to pass data protection laws that ensure adequate protection and are recognised as such by the European commission. It is finally the companies' responsibility, including in their policies, to agree to comply with the highest level of protection, rather than looking for global solutions around the smallest common denominator, which requires that they then manage the complexity of higher specific requirements.

Other areas or other simplification methods may be explored, including in the area of electronic trading. **Mrs. Lilian Edwards**, the winner of the Barbara Wellbery Memorial Award, will explain her proposals in this area, which one has to agree are rather controversial …

III – Other modern challenges posed by transborder data flows to data protection authorities

Other challenges than those consisting in developing transborder data flows control methods or tools are facing data protection authorities, resulting from the well know phenomenon of globalisation.

> **Mr. Alfred Büllesbach, Data Protection Officer of the Daimler Chrysler Group**, has focused his contribution on the impact of globalisation on personal data protection.

In that context, two specific challenges face data protection authorities :

1. Boost co-operation actions in order to take into account the unprecedented development of transborder data flows towards new destinations

Our current world is marked in developed countries and in the North, by a strong outsourcing trend, and in developing countries, by a new capacity to better integrated in the global market through the world-wide communication system, including the internet. As a result, transborder data flows do not only take place like before between Northern countries but also recently between developed countries (Europe, OECD) and Southern countries, and more generally with developing countries whose labour is highly qualified (remote computer maintenance ; call centres relocations in India, Morocco, Tunisia, Senegal, etc.).

This trend results in a major priority for data protection bodies : taking, with the support of their governments and regional instructions, measures to encourage those countries to pass personal data protection laws, like 25 years ago between northern countries, by promoting co-operation and providing them with the experience and expertise they need.

Such co-operation actions have been initiated at the highest level by our Spanish colleagues in various Latin America countries ; similar projects are in progress in French-speaking countries and in Asia-Pacific countries. Such co-operation programmes are essential as they are the only way to allow to develop personal data protection simultaneously with the increase in economic and trade exchanges.

2. Taking into account the risks associated with public security and terrorism prevention laws in the recipient country

After a long and highly positive period during which various adequate protection tools were sought and successfully implemented to facilitate exchanges while ensuring protection, a new and more difficult period seems to begin. In the current insecurity context, authorities also face a very disturbing trend consisting in public authorities in some countries « raiding » private sector files.

Of course, the « Patriot Act » voted in the USA in October 2001 springs to the mind. In pursuance of Section 215 of that law, the FBI can require that data be produced by American companies and their subsidiaries, even though such data may come from countries other than the United States, and without the data subjects being informed.[1] This situation concerns, and

[1] Section 215 provides that a court may issue a secret injunction to produce any tangible thing to the FBI, including personal data, provided the FBI specifies that it is for the purpose of an investigation in connection

rightly so, our Canadian counterparts, since various government departments outsource their work to American service companies.

Based on safety clauses provided by all protection tools with a view to facing exceptional situations, shouldn't we react if it was found that data of non-US resident individuals were likely to be disclosed to the FBI under that law? Shouldn't we engage in negotiation with respective countries to make sure that those individuals are not subjected to that legislation and that the country of residence be informed ? Shouldn't we go up to forbidding some previously authorised data flows ?

In addition, what can companies consider in such situations ? Should we give up relocating some files in the United States ? How can subsidiaries react facing the US headquarter's will to centralise all its personnel-related data in the USA ?

I give you these various questions at the beginning of this session and hope that some solutions will emerge from our debate, from the speakers and then from the audience.

---

with terrorism or clandestine intelligence. Any person injuncted to produce such data is forbidden to inform third parties, including any data subject.