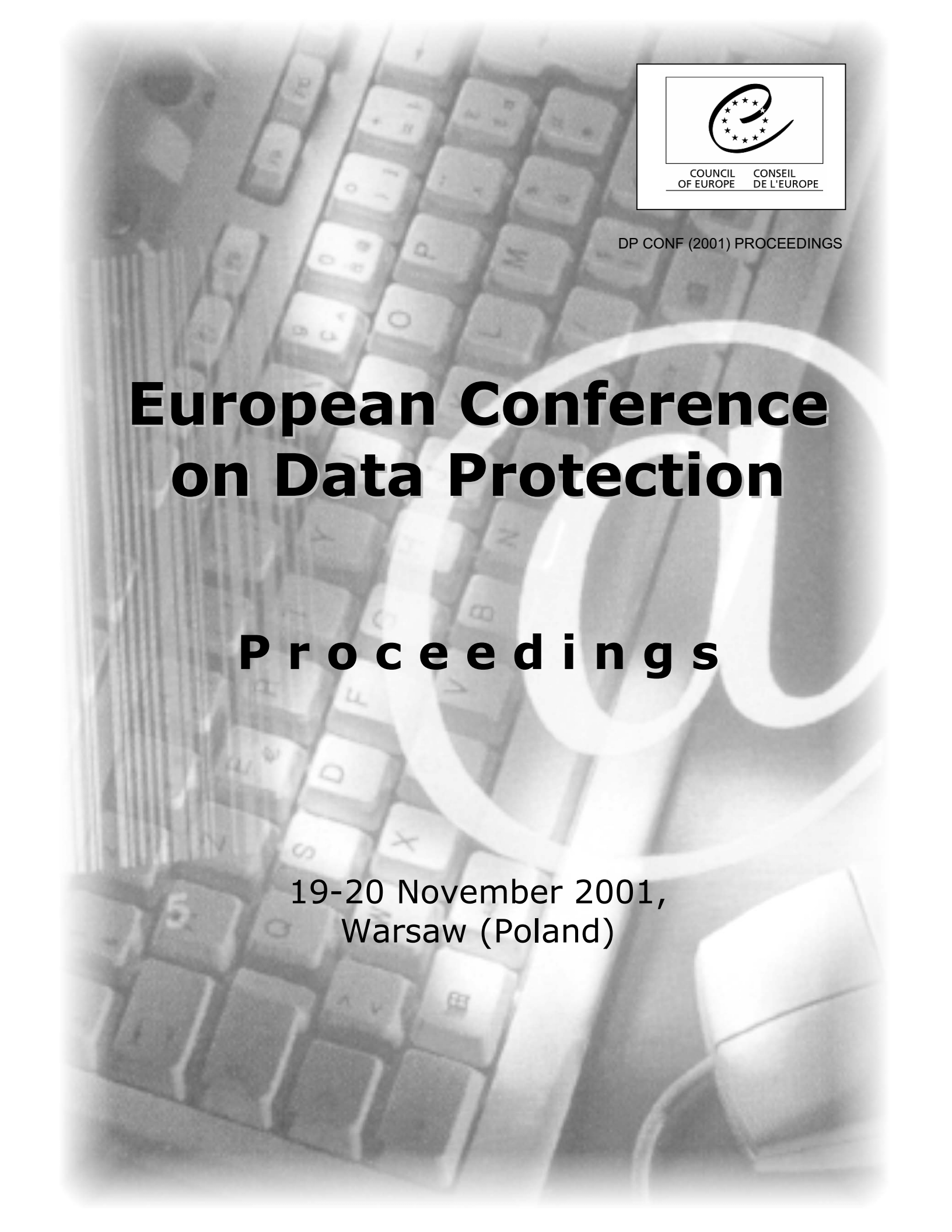

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

DP CONF (2001) PROCEEDINGS

European Conference on Data Protection

Proceedings

19-20 November 2001,
Warsaw (Poland)

European Conference on Data Protection

on

Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future

organised by

the Council of Europe and
the Inspector General of Poland
for Personal Data Protection

under the patronage of the
President of the Republic of Poland

Warsaw (Poland), 19-20 November 2001

P R O C E E D I N G S

CONTENTS

Page

FOREWORD

The theme of the European Conference on Data Protection, organised by the Council of Europe and the Inspector General of Poland for Personal Data Protection under the patronage of the President of the Republic of Poland, was "Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future". The Conference marked the 20th anniversary of the Convention.

The Convention lays down principles for ensuring respect for the fundamental human rights of all individuals with regard to processing of personal data and it was the first legally binding international instrument in the field of data protection; and since it is open to signature by member States of the Council of Europe and to non-member States, it still remains the only binding instrument with a worldwide scope of application.

Ms Ewa KULESZA, Inspector General on Data Protection of Poland and Chair of the Conference, opened the Conference. After the opening of the Conference Minister Jolanta SZYMANEK-DERESZ, Head of the Chancellery of the President of the Republic of Poland, read a welcoming address on behalf of Mr Aleksander KWASNIEWSKI, President of the Republic of Poland who was unable to attend the Conference due to urgent official duties. Mr Hans Christian KRUGER, Deputy Secretary General of the Council of Europe, pronounced an inaugural speech on behalf of the Council of Europe. Following the opening speeches, debates took place over two days on the following subjects:

- **Data protection law: present and future responses to the challenges of the information society**
  Chair: Mrs Ewa KULESZA, Inspector General on Personal Data Protection (Poland)
  Rapporteur: Mr Marek SAFJAN, President of the Constitutional Court (Poland)

- **The relevance of the data protection principles set out in Convention 108 and its Additional Protocol**
  Chair: Mr Jean-Philippe WALTER, Chair of the Council of Europe Consultative Committee of Convention 108 (T-PD) and Deputy Federal Commissioner, Swiss Federal Data Protection Commissioner (Switzerland)
  Rapporteurs: Mr Paul DE HERT, Researcher at the Centre for Law, Public Administration and Computerization, University of Tilburg, (Netherlands) and
  Ms Olga ESTADELLA, Associate Professor, Faculty of Law, Autonomous University of Barcelona (Spain)

- **Mechanisms for implementation and international co-operation in the context of data protection: existing mechanisms and mechanisms to be established**
  Chair: Mrs Eva SOUHRADA-KIRCHMAYER, Chair of the Council of Europe Project Group on Data Protection (CJ-PD) and Deputy Executive member of the Austrian Data Protection Commission and Deputy Head of the Data Protection Section in the Austrian Prime Minister's Office (Austria)
  Rapporteur: Ms Diana ALONSO BLAS, Senior International Officer, Data Protection Authority (The Netherlands)

- **The individual's position in a globalised information world: rights and obligations**
  Chair: Ms Charlotte M. PITRAT, Government Commissioner at the National Commission for Informatics and Liberties (CNIL), Prime Minister's Department (France)
  Rapporteur: Ms Nathalie MALLET-POUJOL, Head of Research at the "*Centre National de la Recherche Scientifique*" (CNRS), University of Montpellier (France)

Presentation of these reports was followed by round table discussions by panellists on related subjects: Present and future prospects for legislation on personal data protection in particular in the countries of Central and Eastern Europe; The fundamental principles of Convention 108 and their relevance now, in particular the role of information technologies in implementing data protection principles; The regulation of transborder data flows - an appropriate guarantee?; Mechanisms for implementing principles relating to data protection, in particular the position of supervisory authorities; International co-operation mechanisms for protecting personal data in a globalised information world; The individual's means for protecting his/her personal data and asserting his/her rights in the context of globalisation.

The General Rapporteur of the Conference, Mrs Waltraut KOTSCHY, Data Protection Commissioner of the Council of Europe, Executive Member of the Austrian Data Protection Commission and Head of the Data Protection Section in the Austrian Prime Minister's Office, presented the summary and conclusions of the debates. Mr Alexey KOJEMIAKOV, Head of the Department of Public Law in the Directorate General of Legal Affairs of the Council of Europe then presented proposals for follow-up action by the Council of Europe.

This volume contains the texts of the opening and closing speeches, the reports and papers presented by the participants at the Conference, the proposals for follow-up action by the Council of Europe and the main conclusions of the Conference presented by the General Rapporteur.

PROGRAMME

Monday, 19 November 2001

9.00 Registration of participants

10.00 **OPENING OF THE CONFERENCE**

Chair of the Conference:

Mrs Ewa KULESZA, Inspector General on Personal Data Protection (Poland)

Welcoming addresses by:

Minister Jolanta SZYMANEK-DERESZ, Head of the Chancellery of the President of the Republic of Poland on behalf of Mr Aleksander KWASNIEWSKI, President of the Republic of Poland*

Mr Hans Christian KRÜGER, Deputy Secretary General of the Council of Europe

10.30 **DATA PROTECTION LAW: PRESENT AND FUTURE RESPONSES TO THE CHALLENGES OF THE INFORMATION SOCIETY**

Chair of the sitting:

Ms Ewa KULESZA, Inspector General on Personal Data Protection (Poland)

Rapporteur:

Mr Marek SAFJAN, President of the Constitutional Court (Poland)

11.00 **Round table: Present and future prospects for legislation on personal data protection in particular in the countries of Central and Eastern Europe**

Panellists:

Mr Peter LIESKOVSKÝ, IT Specialist, Inspection Unit for the Protection of Personal Data (Slovak Republic)

Ms Vaida LINARTAITĖ, Chief Inspector of the State Data Protection Inspectorate (Lithuania)

Mr Karel NEUWIRT, President of the Office for Personal Data Protection (Czech Republic)

Mr Mirosław WYRZYKOWSKI, Dean of the Faculty of Law and Administration, Warsaw University (Poland)

Ms Anna WYROZUMSKA, Acting Director, Department of Legal and Consular Affairs, Ministry of Foreign Affairs (Poland)

12.00 Lunch

* The President of the Republic of Poland, Mr Aleksander KWASNIEWSKI was unable to present the speech due to urgent official duties.

14.00 **THE RELEVANCE OF THE DATA PROTECTION PRINCIPLES SET OUT IN CONVENTION 108 AND ITS ADDITIONAL PROTOCOL**

Chair of the sitting:

Mr Jean-Philippe WALTER, Chair of the Council of Europe Consultative Committee of Convention 108 (T-PD) and Deputy Federal Commissioner, Swiss Federal Data Protection Commissioner (Switzerland)

Rapporteurs:

Mr Paul DE HERT, Researcher at the Centre for Law, Public Administration and Computerization, University of Tilburg, (Netherlands)

Ms Olga ESTADELLA, Associate Professor, Faculty of Law, Autonomous University of Barcelona (Spain)

15.00 **Round Table: The fundamental principles of Convention 108 and their relevance now, in particular the role of information technologies in implementing data protection principles**

Panellists:

Mr Graham SUTTON, Head of the Data Protection Section, Lord Chancellor's Department (United Kingdom)

Mr Sören ÖMAN, Senior Legal Advisor, Ministry of Justice (Sweden)

Mr Hansjürgen GARSTKA, Data protection and Information Access Commissioner of the State of Berlin (Germany)

16.00 Break

16.30 **Round Table: The regulation of transborder data flows - an appropriate guarantee?**

Panellists:

Mr Ulf BRÜHANN, Internal Market, Directorate-General, Commission of the European Communities

Mr Christopher KUNER, ICC Special Adviser on Data Protection, Privacy and E-Business Issues, International Chamber of Commerce (ICC)

Ms Anne CARBLANC, Chief Administrator, OECD, Division of Information, IT and Communications

Mr Rafael LEON CAVERO, State Attorney, Ministry of Justice (Spain)

17.30 End of the first day

Tuesday, 20 November 2001

9.30 **MECHANISMS FOR IMPLEMENTATION AND INTERNATIONAL CO-OPERATION IN THE CONTEXT OF DATA PROTECTION: EXISTING MECHANISMS AND MECHANISMS TO BE ESTABLISHED**

Chair of the sitting:

Mrs Eva SOUHRADA-KIRCHMAYER, Chair of the Council of Europe Project Group on Data Protection (CJ-PD) and Deputy Executive member of the Austrian Data Protection Commission and Deputy Head of the Data Protection Section in the Austrian Prime Minister's Office (Austria)

Rapporteur:

Ms Diana ALONSO BLAS, Senior International Officer, Data Protection Authority (Netherlands)

10.00 **Round Table: Mechanisms for implementing principles relating to data protection, in particular the position of supervisory authorities**

Panellists:

Mr David SMITH, Assistant Commissioner, Office of the Information Commissioner (United Kingdom)

Mr Ulrich DAMMANN, Head of European and International Affairs, Federal Data Protection Authority (Germany)

Mr Bart DE SCHUTTER, Chairman of the Schengen Common Supervisory Authority and member of the Belgian Commission for the Protection of Privacy (Belgium)

11.00 Break

11.30 **Round Table: International co-operation mechanisms for protecting personal data in a globalised information world**

Panellists:

Mr Juan Manuel FERNANDEZ LOPEZ, Director, Data Protection Authority (Spain)

Ms Marie GEORGES, Head of the Division of European and International Affairs and Prospectives, National Commission for Informatics and Liberties (CNIL) (France)

Mr Joe MEADE, Data Protection Commissioner (Ireland)

Mr Giovanni BUTTARELLI, Secretary General of *Garante per la Protezione dei Dati Personali* and Vice-Chairman of the Schengen Common Supervisory Authority (Italy)

12.30 Lunch

14.00 **THE INDIVIDUAL'S POSITION IN A GLOBALISED INFORMATION WORLD: RIGHTS AND OBLIGATIONS**

Chair of the sitting:

Ms Charlotte M. PITRAT, Government Commissioner at the National Commission for Informatics and Liberties (CNIL), Prime Minister's Department (France)

Rapporteur:

Ms Nathalie MALLET-POUJOL, Head of Research at the "*Centre National de la Recherche Scientifique*" (CNRS), University of Montpellier (France)

14.30 **Round table: The individual's means for protecting his/her personal data and asserting his/her rights in the context of globalisation**

Panellists:

Ms Françoise TULKENS, Judge at the European Court of Human Rights, Council of Europe

Mr Andrzej MALANOWSKI, Director of Unit I for Fundamental Rights and Citizens' Freedoms, Bureau of the Ombudsman for Human Rights (Poland)

Ms Sarah ANDREWS, Research Director at the Electronic Privacy Information Center (EPIC) (United States of America)

16.00 Break

16.30 **SUMMARY AND CONCLUSIONS BY THE GENERAL RAPPORTEUR OF THE CONFERENCE**

Mrs Waltraut KOTSCHY, Data Protection Commissioner of the Council of Europe, Executive Member of the Austrian Data Protection Commission and Head of the Data Protection Section in the Austrian Prime Minister's Office

17.00 **PROPOSALS FOR FOLLOW-UP ACTION BY THE COUNCIL OF EUROPE**

Mr Alexey KOJEMIAKOV, Head of the Department of Public Law, Directorate General of Legal Affairs, Council of Europe

17.30 **CLOSING OF THE CONFERENCE**

Closing speeches by:

Mr Alexey KOJEMIAKOV, Head of the Department of Public Law, Directorate General of Legal Affairs, Council of Europe

Mrs Ewa KULESZA, Inspector General on Personal Data Protection (Poland)

OPENING SPEECHES

Opening speech by Ms Jolanta SZYMANEK-DERESZ, Minister, Head of the Chancellery of the President of the Republic of Poland, on behalf of Mr Aleksander KWASNIEWSKI, President of the Republic of Poland

---

OPENING SPEECH∗

by

Ms Jolanta SZYMANEK-DERESZ, Minister
Head of the Chancellery of the President of the Republic of Poland
on behalf of
Mr Aleksander KWASNIEWSKI
President of the Republic of Poland

Ladies and Gentlemen,

I consider it a great honour to assume the honorary patronage of the Conference in which so many guests are taking part and which is dedicated to such vital issues. The Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data refers to problems of supreme importance as they concern the rights of individuals - rights which, in a democratic society, comprise a broad spectrum of activities and limits which even public authorities are not allowed to exceed. The rights which have been guarded by the Council of Europe for more than half a century. The Convention was adopted twenty years ago as a result of concern with an individual's right to privacy. I am glad that the most outstanding experts from Europe and from across the Atlantic have gathered today in Warsaw in order to discuss this subject. Your opinion is especially important and valuable in the period of final preparations for ratification of the Convention by Poland and at the same time in the final phase of negotiations for our country's membership of the European Union.

The present year is, in Poland, the time for recapitulation of our presence in the Council of Europe. It has been ten years since our country was accepted as a member of the organization whose role in defining legal standards and promoting international co-operation is difficult to overestimate. As we look back as a country of firm democracy, we are proud of our achievements up to the present. However, at the same time we are aware of the responsibility that was rested upon us in order Polish law might still be improved and comply with high European standards. In order that it should be generally accepted and respected by citizens.

The development of information technology together with other processes which in their global aspect facilitate the access to numerous data files pose new challenges. The right of individuals to define which information about themselves they would like to share with others, had to be placed under protection against any violations which might appear together with automated data processing. Poland performs this task with great responsibility, raising it to constitutional standing. It has been four years since we adopted the Act on the Protection of Personal Data. At the end of September I also signed the Act on the Protection of Data Files adjusting Polish law to present-day requirements.

Ladies and Gentlemen,

∗The President of the Republic of Poland, Mr Aleksander KWASNIEWSKI was unable to present the speech due to urgent official duties.

The protection of individuals with regard to automatic processing of personal data belongs to a very delicate matter of modern, legal issues. It needs reasonable treatment of all its requirements and interests but also, it makes the fight against degeneration in protection of information necessary. Many doubts arise on the threshold between protection of privacy and access to information – which as a general rule is open to the public. The questions of protection of private data referring to public persons are also very complicated. Such problems occur in all democratic countries in which advanced technology has developed. Hence, achievement of uniformity in terms of European standards of data protection – the purpose of the Council of Europe Conference - is of great importance.

I am convinced that this group of distinguished experts and professionals in this field who are taking part in the Conference in the Royal Castle in Warsaw will successfully wrestle with the problems which derive from the protection of individuals with regard to automatic processing of personal data and will find solutions that will make the future – the future of the citizens and their privacy – safer. Let me wish you fruitful debates.

Aleksander Kwaśniewski

OPENING SPEECH

by

Mr Hans-Christian KRÜGER
Deputy Secretary General of the
Council of Europe

Minister,
Inspector General for personal data protection,
Ladies and Gentlemen,

It is a great honour and a pleasure for me to participate in the opening of the European Conference on Data Protection on the occasion of the 20th anniversary of our Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

I would like to thank the authorities of the Republic of Poland for hosting this Conference and, in particular, the President of the Republic for his patronage. I would also like to thank the Inspector General for the Protection of Personal Data, and her staff, for all their hard work in preparing the conference. The Council of Europe would, furthermore, like to congratulate your country for having set up this supervisory authority and we look forward to your ratification of the data protection Convention.

It is particularly significant that we are holding the Conference this year as it provides us with an opportunity to assess the achievements of this Convention over the past twenty years and to look towards its future.

The Convention was adopted in 1981 in response to concerns about the rising trend towards massive electronic storage of data concerning the private sphere of individuals. The rapid progress made in the field of information technology and, in particular, the developments in electronic data processing and the setting up of extensive data banks have increasingly facilitated not only the collection and storage of these data, but also the processing and interlinking of personal data.

Whilst these developments offer considerable advantages in terms of efficiency and productivity, they also contain potential risks. Modern technology provides access in seconds to limitless quantities of personal data and the possibility of creating “personality profiles” through the combination of different data files. In our information society, the existence and application of well-established data protection principles is essential to safeguard the individual against unlawful abuses of his or her personal data.

When it was opened for signature, the Council of Europe’s data protection Convention was the first binding international legal instrument in this field. Since it is open to member and non member States of the Council of Europe, it still remains the only binding instrument with a worldwide scope of application.

Its principles continue to be the hard core of personal data protection. They provide the main point of reference for those States which are currently drafting or reforming national legislation in the field of personal data protection.

Four states have ratified the Council of Europe's data protection Convention this year, bringing the total number of ratifications to 25; some of the seven signatory states, including our host state, have announced its imminent ratification. These facts serve as evidence of its continuing importance.

In the twenty years since the Convention was opened for signature, data protection has increasingly become a subject of topical interest to professionals, the public and the media. It has become evident that specific rules are necessary to deal with the different requirements of the various sectors such as health, social security, insurance, banking, employment, the police, telecommunications, direct marketing. The Council of Europe has adopted twelve Recommendations in relation to the protection of personal data in the above-mentioned fields.

Furthermore, in May of this year the Committee of Ministers of the Council of Europe adopted an Additional Protocol to the data protection Convention regarding supervisory authorities and transborder data flows. This legal instrument was opened for signature by member states two weeks ago and so far has already been ratified by one state and signed by a further fifteen states.

The Additional Protocol takes into account that, with the increase in transborder data flows, it is necessary to ensure an effective protection in relation to exchanges of personal data across national borders. It requires Parties to set up supervisory authorities with effective powers and complete independence in the exercise of their functions.

The Council of Europe Convention on data protection was a source of inspiration in the elaboration of the Directive of the European Communities. The close co-operation between these two organisations in the field of data protection has continued with the application of the European Communities to become a Party to the Convention and the subsequent adoption in 1999 of the Amendments allowing the European Communities to accede to this Convention.

These international legal instruments of the Council of Europe, together with those of the European Union and other international organisations, and the case law of the European Court of Human Rights concerning data protection as part of the individual's enjoyment of his or her right to respect for private life as guaranteed by Article 8 of the European Convention on Human Rights, constitute the European acquis in the field of data protection.

This European acquis contributes to the consolidation and expansion of the European standards on data protection. It is enriched by the work carried out by the Council of Europe's data protection committees, which provide an essential forum for the updating of the data protection principles and for giving rapid responses to the challenges of the information society. Their work sometimes goes beyond the greater Europe with the participation of Canada, Japan, the United States of America and others.

At present our committees are working on new issues directly linked with the latest technological developments such as video surveillance and smart cards. They are also continuing to examine ways of updating contractual solutions with regard to transborder data flows and the impact of data protection principles on police and judicial co-operation in criminal matters. In the light of recent events, this last issue has become even more important.

The heinous terrorist attacks in the United States of America on 11 September 2001, as well as the attacks which have occurred in Europe and throughout the world, have brought the fight against terrorism to the forefront of world politics. This will undoubtedly lead to a significant increase in the circulation of personal data between the different security services.

In spite of these challenges to democracy, the fight against terrorism should not tempt us to unlawfully infringe on human rights and individual privacy. The European Court of Human Rights already made this point in 1978, in the case of *Klass v. Germany*, when it stated that Contracting States to the European Convention on Human Rights do not enjoy an unlimited

discretion to subject persons within their jurisdiction to secret surveillance and, in particular (I quote):

> "The Court (…) affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

The Council of Europe has always sought to maintain the balance and to find solutions to possible conflicts between those international legal instruments aiming to protect personal data and those aiming to prevent and prosecute crime. This is also the case with the Council of Europe Convention on Cybercrime, which will be opened for signature on 23 November 2001 in Budapest. The Council of Europe's data protection Convention contains the necessary elements to permit any storage and exchange of personal data required by the fight against terrorism. This is made possible by the derogation of some provisions of the Convention where such derogations are provided for by law and constitute a necessary measure in a democratic society in the interests of protecting State security, public safety or the suppression of criminal offences. There is, therefore, no contradiction between the protection of personal data and the investigation and suppression of criminal offences and terrorism.

On its 20th anniversary, it is important that we ask ourselves: Are the Council of Europe data protection Convention and its principles still relevant today? Or have the technological and legal developments of the past 20 years made it necessary to update them? And if so, to what extent?

All these questions and many others will be examined during this European Conference on Data Protection and I am certain that, given the variety and the high professional qualifications of the eminent participants here today, you will succeed in finding the most appropriate solutions.

I wish you all success for your important conference and thank you for your attention.

REPORTS AND SUMMARIES

THE RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION IN THE INFORMATION SOCIETY

Report by

Mr Marek SAFJAN
President of the Constitutional Court
Professor at the University of Warsaw
(Poland)

The growth of modern civilisation is connected with the development of information. Modern information and data transmission methods constitute today the most characteristic feature of state of the art technology. The twentieth century has come to a close with a veritable explosion of capabilities of data collection, storage and processing by electronic means, deemed incredible until recently. In the contemporary world the individual is a beneficiary, but at the same time a victim, of modern technology in data collection.

We perceive this phenomenon at every level of the functioning of the individual in society and at every stage of the individual's life.

It is worthwhile noting these acutely manifested conflicts and making a preliminary attempt to identify them. Therefore, let us enumerate the following:

- conflict between the public interest and private interest ("vertical" conflict);
- conflict of interests - among individuals ("horizontal" conflict);
- conflict of particular rights: the right to privacy *versus* the right to access information.

The right to protection of private life constitutes a relatively new concept in the development of contemporary law, if its beginnings are attributed to the famous publication by the American professors Warren and Brandeis in the Harvard Law Review at the end of the 19th century, and most concisely reflected in the expressions the "right to be alone" and "my home is my castle". The right to information autonomy made a stunning career in the 20th century and penetrated the traditional legislations (although not without difficulty) in the countries of continental Europe. The development of this concept leads to the quest for increasingly effective and more adequate instruments of protection. It is a veritable revolution in thought concerning the sphere of privacy – as it is determined not only by the limits of traditionally conceived secrecy or confidentiality, but also the limits of broadly conceived information autonomy of the human person.

It should be noted, however, that this dynamically developing concept of protection of the individual person has emerged almost concurrently with the development of the right to access information, to the transparency of public life, to liberty and freedom of expression of one's views, to conscious participation in public life and to the enjoyment of the benefits of democracy, etc. These two mutually contradictory trends express, at the same time, the Janus-faced nature of modern civilisation.

The choice between them does not appear to be simple or obvious, as it depends on the concept of the development of civilisation. The conflicts that appear here are very real in nature, and not just theoretical, therefore one should not seek to obscure them.

The basic problem, related to the concept of personal data protection, is thus derived from the question concerning the place of the individual in contemporary civilisation and his relationships to the state, to society, and to other individuals. The globalization of information, the speed of the flow of data, the universal accessibility of information, the multiple facets of information gathering (health care, insurance, education, administration of justice, taxes, registration of the population, scientific and statistical research, marketing etc.) constitute extraordinary threats, and yet they simultaneously serve the individual and increase his/her effectiveness. Without switching on a computer and access to a database one can hardly imagine today the functioning of public and private bodies, the state and its agencies. Without much exaggeration one can say that the handling of information gathered in electronic data banks is a *conditio sine qua non* for the functioning of the modern state. But also never before has the concept of the protection of privacy been subjected to an equally difficult test.

Modern man, when facing such a test, escapes into privacy. Undoubtedly, a psychological mechanism intervenes here: the more limited, the more endangered privacy is, and the greater the pressure from the outside world to know everything about a person – the greater value it gains and the more we begin to value it. The profound paradox of the situation of contemporary time consists indeed exactly in the fact that we are unable to free ourselves by any means whatsoever from the "globalisation" of information and from the issue of access to it. On the contrary – it is extremely important for us to be able to make extensive use of such information; we demand from the surrounding environment and from the media satisfaction of the growing appetite for information concerning other people and other matters. We would still like to consume such information in the cosy environment of our homes, exposed to neither criticism nor witnesses, and above all, without ourselves being included directly in the database. The vision of man hidden behind the high wall of his privacy, contacting the world by means of the computer and wishing to know everything – again by using the computer – about his neighbour also hidden behind the impermeable wall of the privacy of his home – indicates in brief the tensions that exist between contradictory expectations of modern man.

Contemporary man has a growing interest in the world and, while becoming to an increasing degree a consumer of information, he wishes at the same time to be better protected in the domain of his own privacy. *My home is my castle* – this statement has not lost any of its validity over almost 100 years since the American lawyers Brandeis and Warren formulated the legal concept of privacy. The above-mentioned paradox of the "Janus face" of contemporary civilisation unfolds with increasing strength in the sphere of legal regulations, which seem to be moving in parallel in opposite directions, reflecting fairly closely, however, the expectations of modern societies.

For on the one hand one can notice the set of instruments serving to protect the right to privacy expanding to the furthest limits, as a result of which in some countries it gains the rank of the right to privacy directly guaranteed by constitutional norms (the fundamental premises related to the protection of personal data are at the same time contained within its limits); yet, on the other hand, one can observe the emergence, also on the level of constitutional norms, of the very strongly apparent trend toward the development of the right of access to information that would provide guarantees for access to the information gathered and maintained in public data banks. This tension also appears in the framework of the Polish Constitution, which grants their proper place to both of these values. Which current will take the upper hand and win?

The history of development of personal data protection may lead to the conclusion that we are dealing here with the creation of a peculiar appearance of information autonomy, since the individual, while remaining under the strong pressure of the demands of contemporary civilisation, has an ever diminishing influence over the scope of the information disclosed concerning himself. It is not feasible to avoid these requirements, therefore, in consequence, also the scope of true liberty of decision making is becoming narrower. The burden of protection of the individual and his privacy is more visibly shifting toward the institutional, and thus public-legal institutions and means. In consequence, the scope of autonomy of the individual is narrowing (in some fields completely). It is no longer the individual alone that decides on the scope of his own information-related autonomy. The decisions concerning the areas in which he

can still remain free from external interference are being taken on his behalf by the law and by the public institutions. The scope of privacy is therefore not such as it is delimited by the individual, but such as is determined by the sphere of the public interest and the interest of other individuals. Only in this shrinking space left at the disposal of the individual is there still room for his free, unconstrained decisions. It is worth realising this fact as we use the term "information autonomy".

It is trivial to state that in the contemporary world the individual is entangled in activities which per se create the necessity to collect personal data. Without the creation of information databases, the functioning of the individual as a being social by nature and benefiting from the advantages of civilisation is undermined – this concerns every sphere of activity: from birth to death, from kindergarten to the workplace. Without data concerning one's marital status, place of residence, education, bank account, blood type, and soon also identification by one's own DNA code, insurance policy, tax registration number and the number assigned in population records - the individual does not exist as a subject in these social relations, which are subject to legal regulation. The virtual reality in electronic space becomes much more real than the reality of objectively existing persons and objects. The individual who is not captured by the registers, not depicted in a database, not attached to a specific category of subjects – is almost non-existent (we shall just note the problem linked to constitutional jurisprudence concerning the status of homeless people, not included in population records, as in order to realise certain rights of such people it would be necessary to have respective judgements of the Constitutional Tribunal – see case K. 10/96).

Is there still any room left in that space for the autonomy of the individual? The individual may “freely” decide on the scope of information made accessible by himself, but only in the sense in which he can decide on the very fact of participation in social, professional or community relations and not as far as the consequences resulting from that fact are concerned. Is there any room here for an authentic choice and self-conscious adoption of independent decisions?

The issue of protection of the right to privacy, especially the protection of personal data and information-related autonomy arises, therefore, at the stage when the threat to privacy reaches a climax. Privacy, in the sense in which we speak of the information-related autonomy of the individual, is becoming subject to protection on the same principle as that applied to protected species of flora or fauna facing extinction. The concept of data protection is – as we have already mentioned – a notion derived from the protection of privacy. It constitutes a creation which was conceived from the broad notion of privacy and is, in a certain sense, its unwanted but very dynamically growing child. Unwanted, however paradoxically that might sound, because accepting a different perspective on protection, as the sphere of privacy of the individual is determined beyond the reach of the individual himself and no longer depends on him.

Regardless of the opinions expressed above, it ought to be noted that it is very fortunate that the problem as such has been noticed. The identification and definition of threats mean a lot in this area. For it should be firmly stressed that in the shaping of certain international legal standards in this domain, a leading role was played by the mechanisms of legal protection adopted within the framework of the Council of Europe. Let us recall, as a matter of regularity, the accomplishments existing hitherto in this area, starting with Resolution 509 (1968) of the Parliamentary Assembly of the Council of Europe concerning the protection of human rights in the light of contemporary scientific and technical projects, as well as Resolution No. 3 of 1971 concerning the issue of protection of privacy in relation to the development of computerized technologies of personal data collection. Undoubtedly of break-through significance was Convention No. 108 of the Council of Europe of 1981 on the protection of electronically processed personal data, which entered into force in 1985 and was ratified by the overwhelming majority of the member countries. The recommendations of the Council of Europe subsequently covered a broad range of sector specific problems (from banking data to statistical and medical data), related to the functioning of marketing, police services, and eventually even to the gathering of data on the genetic code of the individual). Many regulations of Community law

related to the protection of personal data drew their inspiration from the concepts and ideas developed in their initial stage in the framework of the Council of Europe.

There are two main reasons for the creation of mechanisms of personal data protection which seem to merit particular attention. *Firstly*, the ineffectiveness of traditional mechanisms for the protection of privacy which were available in the field of criminal law and civil law – the civil law sanctions as well as the penal sanctions had turned out to be absolutely ineffective from the point of view of the preventive function. Threats to the individual, as was rightly noticed, will not be eliminated until preventive instruments become mobilized. Hence the decisive break-through in the construction of personal data protection – with greater emphasis placed on the prevention of violation and less on the removal of its consequences (since traditional instruments of protection may prove to be sufficient here). Hence, undoubtedly, originated the idea of establishing a new public institution in the form of the Commissioner for the Protection of Personal Data.

Secondly, the recognition of mainly the instruments of a public law nature (administrative law) as the basic arm of protection – which thereby consists of institutional protection, and not protection having its source and legitimacy in the autonomous dispositions of the individual. Aware of a certain simplification involved, I wish to repeat with insistence: it is not the individual that decides on the scope of protection, but the drafters of the law who make the decisions in anticipation on his behalf. The appearances and the stress laid on the approval of the individual, as a premise still in most cases required for the creation of data banks, ought not to deceive us. The individual is only one of the actors in that show. He occupies the vertex of the triangle, along the sides of which are located the public interest and the interest of other individuals.

Interest in the problem area of personal data protection has surfaced in Poland relatively recently, at the same time as the debate on this issue began. That issue was hardly noticed earlier on, although – and it is worth underlining – the doctrine, and subsequently the jurisprudence, developed the concept of protection of privacy against the framework of general provisions concerning the protection of personal rights contained in the civil code (Article 23 and 24). The problem was therefore clearly of a particular nature, and it did not extend beyond the limits of one branch of the law.

It is interesting that the discussion on these issues could start only after the transformation of the political and economic system and it is related to the reconstruction of the standards of a democratic state. Only then could the conflicts between the sphere of the rights of the individual (the right to privacy) and the protection of personal data be noticed and identified. The links between democracy and the idea of personal data protection are more than obvious. In a totalitarian state, which was able to evaluate information concerning the citizen and in which information about the citizen was – more than anywhere else – a source and instrument of exercising power, where multiple secret personal data banks existed, gathered by the covert security services; by the very nature of such realities it seemed impossible to even operate with the notion of “information autonomy” alone. It assumes, after all, at least some restraint over the discretionary authority of public power and the subordination of its activities to transparent legal rules. Already since the early 1970s electronically processed data banks were being created (the systems: PESEL – personal data records, “*Magister*” – register of persons with university degrees, *“Rejestr skazanych*” – register of convicted persons). These systems, created pursuant to low ranking provisions, without sufficiently precise legal grounds in any act of parliament, did not introduce any, even minimal, standards of protection of personal rights. Until recently the disclosure of information on illness, contained in medical sick leave certificates, was taken for granted without giving rise to any questions (how strongly certain stereotypes were embedded in our thought is indicated by the fact that only the decision of the Constitutional Tribunal of 1998 removed this provision, which had been overtly in contradiction with the constitutional rights of the individual, from the legal system; see decision of the Constitutional Tribunal dated May 19, 1998, U. 5/97).

But perhaps the most disconcerting was not so much the indolence of the legislator himself, but rather the lack of understanding of that problem among the elites of the legal profession, not to

mention the sensitivity of the average citizen. We have come a long way from that “standard” precisely in the sphere of awareness, which is not to say that the problem is now at last sufficiently known and understood by society. The introduction of the concept of personal data protection to the area of our legal culture constitutes a real victory of the spirit over physical matter. But its resistance still remains perceptible[1].

The data protection concept is based on balancing different interests. The fears are real that the preservation of perfect balance in this domain is not possible. The trends finding expression, on the one hand, in the right to protection of information-related autonomy, constituting a component part of the right to privacy, but on the other hand in the right of access to information, which expresses both the public interest and the interest of other subjects, may be compared to two trains moving rapidly towards one another on the same track. Any time a collision might occur. The instruments of legal protection are built in each of these areas as if they were independent from each other. The mechanism of the conflict seems to be by its very assumptions built into the legal regulations adopted in this area. An illustration of this thesis might also be provided by the Constitution of the Republic of Poland adopted on 2 April 1997. On the one hand the Constitution, for the first time in the history of Polish law, has established a clear-cut constitutional basis for the protection of privacy, and thus one that is universal, extremely voluminous and pertaining to every domain of activity of the individual (which of course is not to say that privacy had not been perceived as a legally respected value prior to the entry into force of the constitution), providing in Article 47 that: “Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life”.

The constitutional norm does not create, at least *expressis verbis*, any breaches or exclusions in the contents of that right. At the same time, the constitution additionally guarantees (in Article 49) the freedom and protection of the privacy of communication, limited only in cases specified by the statute and in ways which are determined in the same act of law.

It is also an essential value of the Constitution that it introduces the constitutional guarantee of the protection of personal data and the autonomy of information in Article 51:

- by limiting the obligation for the individual to disclose information exclusively to the cases specified by the statute (Section 1 Article 51);
- by determining the limits of allowable collection of personal data by the public authorities (only "that which is necessary in a democratic state ruled by law") – Section 2 Article 51;
- by guaranteeing the individual the right of access to data collections concerning him and the right to demand the correction or deletion of information that is inaccurate, incomplete or acquired by means contrary to statue (Section 3 and 4 Article 51 of the Constitution).

The limits of information autonomy defined in Article 51 of the Constitution clearly indicate that this right is not absolute and remaining in the sphere of full discretion of the individual, as the Constitution provides for the obligation to disclose personal information in the cases specified by the statute.

The respective law consists, above all, of the Act on the protection of personal data of 29 August 1997, which allows, among other things, for the processing of data (without the consent

[1] This is also a matter of some sensitivity or perhaps legal intuition of the persons responsible for the provision of access to data (e.g. in the university community only recently has the thought managed to surface, and not without difficulty, that the provision of general availability of personal data concerning education is not the best idea, as not everybody needs to know that student X has failed to pass his exam, or that professor Y has received a catastrophic score in a feed-back survey among students to evaluate his lectures). Even more disconcerting might be the fact that progress in the sphere of popular awareness is very slow in the domain of such extremely sensitive data as medical information about the patient.

of the data subject), if it is “indispensable for the performance of tasks specified by the law that are realized for public benefit" (Article 23 section I item 4). It should be noted in passing that this formula is very general and that it might even be regarded as too ample.

At the same time, the Constitution protects (in the section on political rights and freedoms), and that is a strange paradox, a value which remains in contradiction to the right to private life, namely the right of the individual to be informed about the activities of the organs of public authority and of persons discharging public functions (Article 61 of the Constitution). This right is defined very broadly and covers also the "receipt of information on the activities of self-governing economic and professional organs and other persons or organisational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury” (Section 1 Article 61). This may be realised by means of access to documents and entry to the sittings of the collective organs of public authority (Section 2 Article 61). The limitation of this right may be imposed solely to protect the rights and freedoms of other persons and economic subjects, public order, security or important economic interests of the State (Article 61 Section 3). The paradox of this solution consists in the fact, among other things, that privacy and information autonomy may be restricted by the category of the public interest related to access to information, but at the same time privacy and autonomy constrain the limits of interference justified by the public interest oriented to the realisation of the right to information, since in accessing information due regard for the rights of other persons must be observed. Thus, real and not imaginary tension is present here, one which only in theory seems to express unequivocally the proportions and the balance between those values.

Which is to be granted priority in such cases of inevitable collision – privacy or the right to information? The evidence of how difficult it is to draw the demarcation line here can always be found in the disputes stirred by press publications in which information concerning public figures is revealed. Although one needs to be fully aware of the controversial and complicated nature of such a proposition, it seems that whenever information becomes a necessary component of the control exercised by democratic society over the public authorities, the values pertaining to the domain of protection of privacy, and therefore also the personal data of the persons involved in the sphere of public activity, must give way to the primary, overruling importance of the right to information. The antinomy of constitutional values (clearly present between the Articles 47, 51 and 61 of the Constitution) should also be resolved in this way – and therefore with the recognition of the priority of the entitlement to information, whenever interference with the privacy of other persons becomes an inevitable element of effective scrutiny exercised by a democratic society. Otherwise, the right to information would remain an empty cliché. The Act on the access to information adopted by Parliament a few weeks ago (on 6 September 2001, Official Journal – Dz. U. No 112, item 1198[2]) is also not free from such tensions and contradictions. This law, however, is being received by a large part of public opinion with the conviction that access to information is a prerequisite of democratic participation in public life. At the same time, however, I must express my concern that the general public has not been sufficiently informed about the consequences of the introduction of this type of solution, which may, after all, limit the scope of our privacy. In situations like this it is advisable to abstain from the use of euphemisms and, at the same time, not to avoid engaging in an open discussion on our choices concerning the values protected.

Where do the actual limits of information autonomy indeed lie? At this point it is not a question of formal analysis or criticism of the solution which has been integrated into modern constitutional regulations not only in Poland[3], but also, after all, in international regulations, considering, for instance Article 8 of the Convention on the protection of human rights and

[2] Act on the access to public information of 6 September 2001.

[3] Similar antinomies and paradoxes are found in the framework of the regulations contained in the new Act on the protection of personal data, which, on the one hand, justifies the collection of personal data in the public interest (Article 23 section I item 4), and on the other hand, justifies the prohibition of providing access to data by the need to protect privacy (Article 30 item 4). It should be acknowledged that this also concerns data which have been gathered in infringement of privacy or without the consent of the person in question.

fundamental freedoms, or Convention No 108 of the Council of Europe on the protection of personal data[4]. The point is merely to acknowledge the fact that the limits of information autonomy are to a large extent – though not exclusively – determined on the basis of particular general clauses, which are neither complete, nor defined with full precision.

These are some of the reasons for which, without underrating at this point the significance of the dynamically developing legal discipline called the "right to protection of personal data" – we cannot lose from sight the fact that it is above all the traditions, the legal culture of the citizens, but also certain restraint of the public authorities, that will determine the limits of truly protected information autonomy. It is the culture of the democratic society that will play the dominant role, that will permit the elimination of the specific abuse of the protection of personal data (which may sometimes severely hamper the functioning of the individual in a society, similarly to obtrusiveness in the collection of information). One cannot lose sight of the fact that the protection of data is devised for the benefit of the human person, and not against him. Even the most perfect legal instruments will remain futile in a society which is itself unable to appreciate and recognize the values of privacy. Using a certain metaphor, one could note that in the opposite situation, when modern information technologies make it possible to process information drawn directly from the consciousness of the citizens – an instrument of protection prohibiting such practices will be introduced, on the condition, however, that this will not be in contradiction with the public interest.

We are not too distant from the vision of information's dominance over privacy, and thereby over the human being as such. The computer-based and genetic image of the person has become absolutely realistic. The discovery of the genetic code and the processing of data gathered in that manner is no longer just a theoretical threat, but is a true reality. There is a dramatic struggle in progress for genetic information concerning employees or the clients of insurance companies, for example. The outcome of this struggle has not yet been resolved, evidence of which is provided by the results of the proceedings of the Council of Europe's Committee for Bio-Ethics (CDBI), which has prepared a draft convention on the protection of human rights with respect to the applications of modern biology and medicine[5]. The Committee has failed to arrive at agreement on its position concerning the issue of processing and providing access to genetic data. The final version of Article 12 of the Convention – contrary to earlier expectations – does not introduce any absolute prohibition of the disclosure of genetic information to insurers and employers. It is fortunate that the respective provision concerning the genetic code has been included in the Polish law on the protection of personal data (in Article 27). Despite the efforts made in this direction, we are still very distant from the establishment of a uniform standard of protection throughout the European countries.

In conclusion, I should like to attempt to make a few observations of a more general nature. The creation of new regulations concerning the protection of personal data should, according to my belief, be devoid of an excessively technical, too narrow or purely sector-focused approach. In the framework of such often extremely detailed and technical rules developed in certain fora, including the Council of Europe, at times the essence of the matter is lost, and therewith the protection of the ordinary interests of the individual related to his functioning in social life. The balancing of the existing conflicts between different values, such as the one that I have mentioned in this presentation (privacy versus the right to information) always requires a broader, multi-disciplinary approach. Data protection specialists cannot work in isolation from those who deal with the media and access to information. The issues concerning data banks in contemporary medicine, especially in genetics, are also an excellent example which confirms that the coherent activities of representatives of many different disciplines are highly purposeful. But most importantly - let us always maintain the desirable moderation in the area of legal

[4] E.g. compare the exceptions to the principle of personal data protection specified in Article 9 of Convention No. 108 of the Council of Europe of 28 January 1981, namely if the statute provides for this as a necessary instrument in a democratic society: a) for the protection of the state, public security, currency related interest of the state or combating crime; b) for the protection of the person concerned and of the rights and freedoms of other persons.

[5] The Convention was signed on 4 April 1997 in Oviedo (Spain). Poland has also signed this Convention.

regulation, and let us not lose sight of those goals and values which data protection is intended to serve.

REPORT

THE RELEVANCE OF CONVENTION 108

Report by

Mr Paul DE HERT and Mr Eric SCHREUDERS
Researchers at the Centre for Law,
Public Administration and Informatisation of
Tilburg University
(The Netherlands)

TABLE OF CONTENTS

In this report we compare Convention 108 rather extensively to the European Convention for the Protection of Human Rights and we compare the Convention with the European Union (EU) data protection rules. We conclude that Convention 108 is still of importance. We raise the question whether the original and Guideline oriented approach of the Convention might not be more favourable than the more recent approach to data protection regulations set out in the EU data protection rules and in the Additional Protocol to Convention 108 opened for signature on 8 November 2001. Another question raised is that adding a (new) right to data protection into the Convention for the Protection of Human Rights might be an option to consider.

I. INTRODUCTION

The Council of Europe

The Council of Europe, based in Strasbourg, is an intergovernmental organisation established after the second world war for the purpose of achieving greater unity between European

democratic countries[1]. The main organisations the Council is required to work with are the European Union and the Organisation for Security and Co-operation in Europe.

The Council of Europe is much more inclusive than the European Union. In practice, the Council of Europe and the European Community, known since the Treaty of Maastricht as the European Union in order to emphasise its political as well as economic role, are profoundly different institutions, even though the Union's fifteen members are also part of the Council of Europe. The Council of Europe now has well over 40 members.

The Council of Europe's approach is legal, social and educational. The Council of Europe has amongst other achievements established a range of authorities and institutional machinery, arising from its international treaties. The European Court of Human Rights, established within the framework of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereafter referred to as the ECHR), is the most noteworthy example.

The ECHR, concluded in 1950, was the first international treaty to be concluded within the Council of Europe. The treaty is an instrument which not only assures real protection of fundamental rights and freedoms but also sets up a jurisdictional mechanism capable of guaranteeing their respect (*see below*). Our focus here is on the Convention for the protection of individuals with regard to automatic processing of personal data, concluded on January 28, 1981 (hereafter the Convention).

The Convention for the protection of individuals with regard to automatic processing of personal data

It is no exaggeration to state that, preceded by data protection bills in some Member States[2], European data protection saw the light with this Convention[3]. The purpose of this Convention, as expressed in Article 1, is to secure in the territory of each party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him[4]. The Convention has a wide scope and includes processing done in both the public *and* private sectors[5]. The central notion in the Convention is *personal data*, meaning any information relating to identified or identifiable individuals. We will come back to this below, but it should be underlined here that the Convention (and data protection in general) does not protect privacy data or data concerning the intimate sphere of human life, but *personal data*, a term with a broader meaning.

The Convention defines a number of principles for the fair and lawful collection and use of such data[6]. Notably, data can only be collected for a specific purpose and should not be used for any

---

[1] On the Council: TOMKINS, A., 'Civil Liberties in the Council of Europe: a Critical Survey' in GEARTY, C. (ed.), *European Civil Liberties and the European Convention on Human Rights. A Comparative Study*, The Hague, Martinus Nijhoff Publishers, 1997, 2-4.

[2] It is said that the adventure of data protection started with the *Datenschutzgesetz* of one of the German *Länder*. Cf. Hessischer Datenschutzgesetz, 7 oktober 1970, *GVBl.* I, S 625. This bill has provided for the main elements of data protection as we know it today: duties for data users, rights for data subjects and a specific watchdog mechanism. See: HONDIUS, F., 'Een grondrecht op databescherming?', in DE WILD, A. & EILDERS, B. (eds.), *Jurist en computer*, Kluwer, Deventer, 1985, 171.

[3] Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, 28 January 1981, *European Treaty Series*, No.108; *International Legal Materials*, 1981, I, 422. The convention came into force on 1 October 1985 after ratification by five countries: Sweden, Norway, France, Germany and Spain. Since then, almost all member countries of the Council of Europe have signed the convention, and it specifically provides for the possibility of accession by non-member states.

[4] In the convention this also serves as a definition of data protection.

[5] See: HONDIUS, F., *l.c.*, 172-173. The Common Law option to make a sectoral convention has been rejected.

[6] For a discussion: GUTWIRTH, S., *Waarheidsaanspraken in recht en wetenschap. Een onderzoek naar de verhouding tussen recht en wetenschap met bijzondere illustraties uit het informaticarecht*, Antwerp-

other reason. Data must be accurate, adequate for this purpose and stored only for as long as is necessary. The convention also establishes the right of access to and rectification of data for the person concerned (data subject) [7], and requires special protection for data of a sensitive nature, for example on religion, political beliefs, genetics or medical information. In order to become party to the convention, states must ensure that their national legislation contains these basic principles with respect to the personal data of every individual in their territory.

In order to adapt the general principles set out in the 1981 Convention to the specific requirements of various sectors of activity in society, a number of recommendations dealing with the following subjects have been adopted by the Council of Europe: medical databanks (1981); scientific and other statistical research (1983); direct marketing (1985); social security (1986); police records (1987); employment data (1989); financial payments and related transactions (1990); communication of data to third persons by public institutions (1991); protection of personal data in the field of telecommunications, in particular telephone services (1995), the protection of medical and genetic data (1997); the protection of personal data collected and processed for statistical purposes (1997); Recommendation R (99) 5 containing Guidelines for the protection of privacy on the Internet (1999); and a recommendation dealing with the protection of data collected and processed for insurance purposes (2000). These recommendations have the advantage of being easier to draw up, to adopt and to implement: instead of signature and ratification by each of the member States, they only require unanimous adoption by the Committee of Ministers. It is therefore simpler to adapt them to changing circumstances than to amend conventions; and, above all, although they are not legally binding, they contain real standards of reference for all member States, whether they are Parties to the Convention or not. A recommendation constitutes therefore a request to consider in good faith the possibility of elaborating and implementing domestic law in conformity with internationally agreed interpretation of the principles laid down in the Convention[8].

Where does the Convention fit into the International context?

These basic principles of European data protection are also spelled out in the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data and the European Data Protection Directive[9]. The general ideas behind the three legal instruments are very similar. More or less, they all try to reconcile fundamental but competing values such as privacy, free flow of information, governmental need for surveillance and taxation, etc. The three texts and their principles apply to personal data, whether in the public or private sector. This is crucial, because, as will be seen below, traditional human rights instruments only provide for protection against governmental actions.

However, there are important differences between these three international data protection texts. *Firstly,* the two European instruments widen the scope of the OECD Guidelines in many

---

Apeldoorn, MAKLU, 1993, 687 et seq.; DE HERT, P., 'European Data Protection As A Framework For The Use Of Camera's And Video's For Police Forces' in NIJBOER, J. & REIJNTJES, J. (eds.), *Proceedings of the First World Conference on New Trends in Criminal Investigation and Evidence*, 1997, The Hague, Koninklijke Vermande, 556-560.

[7] Moreover, ratifying countries should offer each other mutual assistance. A data subject in one ratifying country wishing to gain access to a file in another ratifying country may obtain the assistance of that country's data protection authority. The same principle applies to administrative investigations.

[8] See on the motives behind the sectorial approach: WALDEN, I., 'Data Protection', in REED, Ch. (ed.), *Computer Law*, London, Blackstone Press Limited, 1993, (second edition), 300.

[9] OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980 in *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, OECD, 1980, 9-12; *International Legal Materials*, 1981, I, 317.; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities*, L 281, 1995, November 23, 31-50. On the background of the Directive and on the motive to add this Directive to the existing texts: GUTWIRTH, S., *o.c.*, 697-705; PEARCE, G. & PLATTEN, N., 'Achieving Personal Data Protection in the European Union', *Journal of Common Market Studies*, 1998, Vol. 36, No. 4, 529-539.

respects. For instance, the latter only takes into account automatic processing of personal data. The Council of Europe Convention creates the possibility for the member states to apply the Convention to personal data files that are not processed automatically. What is still optional in the Convention becomes binding in the European Directive. This instrument defines in general terms 'processing' as *any set of operations which is performed upon personal data, whether or not by automatic means*.

Secondly, there is the place reserved in the 1995 Directive for the use of voluntary codes of practice drawn up by professional or trade associations in addition to traditional regulatory and technological solutions.[10] Reference to these codes is absent from the other two texts.

Thirdly, in the European texts, but absent from the OECD Guidelines, are the independent supervisory data protection committees responsible for monitoring the application of the data protection rules.[11] These supervisory authorities are intended to be watchdogs endowed with investigative powers, such as powers of access to data, and effective powers of intervention, such as the crucial power of *a priori consent.*[12] Without this consent, processing of personal data by governmental bodies or by individuals is not allowed and the European supervisory bodies must check processing proposals before they consent. Following this prior check, the body may give an opinion or (depending on national law) an authorisation regarding the processing. The controlling body is also endowed with the power to engage in legal proceedings where the provisions of the directive are violated.[13] Few cases of criminal prosecutions under data protection legislation have occurred in Western Europe, and it would seem that data protection authorities tend to rely on informal and civil sanctions against offending data users. Informal sanctions generally involve an investigation by the authority, with the threat of publicity as the incentive for data users to remedy the identified problem areas.[14]

---

[10] PEARCE, G. & PLATTEN, N., *l.c.*, 543. These arrangements are already common in the US and in some European Member States, notably the Netherlands. The directive envisages that the preparation of codes by those directly involved in implementing data protection legislation would improve acceptability and avoid over-detailed regulation. While industry codes are not a substitute for legislation, since such arrangements are not obligatory, they can perform a valuable role in supplementing legislation in fields subject to rapid technological change. For instance, there are already signs that the absence of global regulation of the Internet is encouraging some companies to develop their own codes that will facilitate Internet commerce and protect net users. See also: WALDEN, I., 'Data Protection', *l.c.*, 300.

[11] The OECD Guidelines do not refer to the idea of supervisory data protection committees, but it is picked up and introduced in the Council of Europe Convention as a way of permitting international data protection co-operation (Article 13: "The Parties agree to render each other mutual assistance in order to implement this convention. For that purpose each Party shall designate one or more authorities (...)"), and generalised for all purposes in the directive: "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them" (Art. 28.1 of the Directive). In practice this has resulted in the creation of a specialised agency in each country, headed by a data protection commissioner or registrar who also supervises compliance with domestic law and considers complaints and requests for help from individuals. There is no international body to oversee the Council of Europe Convention or the Directive, apart from a Consultative Committee to advise on interpretation and consider possible amendments to the Convention. See on the role and functioning of the data protection authorities: RAAB, Ch., 'The Governance of Data Protection', in KOOIMAN, J. (ed.), *Modern Governance. New Government-Society Interactions*, London, Sage Publications, 1993, 90-91.

[12] Art. 28.3 of the Directive.

[13] Art. 28.3 of the Directive. The Directive does not impose on member states the use of criminal sanctions for violations of the principles, but most data protection bills do contain criminal sanctions. See for an overview of the data protection regulatory systems in fifteen European countries, Hong Kong, New Zealand, Canada and the United States: CAMPBELL, D. & FISHER, J. (eds.), *Data Transmission and Privacy*, Dordrecht, Martinus Nijhoff Publishers, 1994, 509p.

[14] WALDEN, I., l.c., 300.

Fourthly, the history of data protection can be understood in terms of a growing arsenal of specific subjective rights.[15] Compared to older texts the 1995 Directive is a dazzling display of generosity towards the data subject. Next to the wide scope of the Directive, there are the many new subjective rights absent from the other two texts. Very novel is the right to object to processing: Article 14 of the Directive gives the data subject a right to object to processing and disclosure of data in certain cases, particularly where direct marketing is concerned. Also, there is the new right to protection against certain profiles: with some exceptions, Article 15 declares that no one is to be subject to 'a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.'

Also, the Directive obliges Member States to control and limit the processing of data relating to offences, criminal convictions or security measures.[16] Although discretion is left to Member States to organise this category of data, the general message is one of refusal of the contemporary American trend towards open criminal records and the processing of personal data for security reasons.

II. THE RELEVANCE OF THE CONVENTION IN THE LIGHT OF THE ECHR

The European Convention for the Protection of Human Rights (ECHR)

The European Convention for the Protection of Human Rights and Fundamental Freedoms (hereafter referred to as the ECHR), concluded in 1950, is designed to protect individuals' fundamental rights and freedoms. The Council of Europe has instituted a judicial procedure which is unique in the world and which allows individuals to bring actions against governments, if they consider that they are the victims of a violation of the Convention.

The original two-level system, in which complaints were dealt with first by the European Commission and then by the European Court of Human Rights, has now been replaced by a single and permanent Court. This was judged to be more rapid and effective. Moreover complainants now have direct access to the Court.[17]

Unlike the Universal Declaration of Human Rights (1948), the ECHR contains only civil and political rights much like those contained in the US Bill of Rights. Since the Convention was drawn up, new rights and obligations have been added in what are known as the Protocols. States can choose which of these Protocols to accept but many have been widely adopted. The main rights in the ECHR are: the right to life; the right to liberty and security of person; the right to fair administration of justice; the right to respect for private and family life, home and correspondence; freedom of thought, conscience and religion; freedom of expression and to hold opinions; freedom of peaceful assembly and association, including the right to join a trade union; the right to marry and found a family. Further protection in the Protocols covers: the right to peaceful enjoyment of possessions; certain rights to education; liberty of movement and freedom to choose where to live; the right to leave a country including one's own. Prohibited under the ECHR and its Protocols are: torture and inhuman or degrading treatment and punishment: slavery, servitude and forced labour; criminal laws that are retroactive;

---

[15] See more generally about the development of data protection in Europe: MAYER-SCHÖNBERGER, V., 'Generational development of data protection in Europe', in AGRE, Ph. & ROTENBERG, M. (eds.), *Technology and Privacy: the new landscape*, Cambridge, the MIT Press, 1997, 219-238.

[16] Article 8(5) of the Directive.

[17] See on Protocol No. 11: ROWE, N. & SCHLETTE, V., 'The Protection of Human Rights in Europe after the Eleventh Protocol to the ECHR', *E.L.Rev. HR*, 1998, vol. 23, 3-16; DRZEMCZEWSKI, A. and MEYER-LADEWIG, J., 'Principal Characteristics of the New ECHR Control Mechanism as Established by Protocol No. 11, Signed on 11 May 1994', *Human Rights Law Journal*, vol. 15, no. 3, 81-86. See also: LAWSON, R. & SCHERMERS, H., *Leading Cases of the European Court of Human Rights*, Maklu, Antwerp, 1997, xxxix-xl. The text of the Protocol is included on pages 692-698.

discrimination in the enjoyment of rights and freedoms guaranteed by the ECHR; expulsion of a state's own nationals or denying them entry; the collective expulsion of aliens.

Of great importance for us here is Article 8 of the ECHR stating that: "(1.) Everyone has the right to respect for his private and family life, his home and his correspondence. (2.) There shall be no interference by a public authority with the exercise of this right except *such as is in accordance with the law* and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

The right to privacy contained in Article 8 of the ECHR is of obvious importance for the field of data protection. To give only one example: data protection merely covers the automatic processing of personal information, and excludes most non-digital processing of information, for instance handwritten files. It is evident, however, that those files can also create risk of abuse of personal data. In those cases the right to privacy *may* offer protection for the persons concerned.

Let us return to the ECHR. What is not in this text? The ECHR only covers civil and political rights. For the so-called social rights one has to turn to the European Social Charter, the counterpart of the ECHR in the sphere of economic and social rights, which lays down twenty-three fundamental rights.

There are also a number of civil and political liberties which are not included in the Convention, but can be found in other international human rights treaties such as the United Nations International Covenant on Civil and Political Rights[18] and the recent UN Convention on the Rights of the Child (1989).[19]

---

[18] For instance: the right of accused persons to be kept separately from convicted persons (ICCPR Article 10); the prohibition of war propaganda (ICCPR Article 20); certain children's rights (ICCPR Article 24); rights as to political participation (ICCPR Article 25); protection of minorities (ICCPR Article 26-27).

[19] This convention includes amongst others the following mixture of social and civil rights: the right to protection against all forms of discrimination (Article 2), the right to protection in procedures, undertaken by institutions, courts of law or administrative authorities (Article 3), the inherent right to life (Article 6), the right of the child to a name and nationality (Article 7), to preserve its identity (Article 8), to family life (Article 9), to leave or enter a State Party (Article 10), the right to protection from illicit transfer (Article 11), to express its opinion freely (Article 12), to freedom of thought, conscience and religion (Article 14), to benefit from social security (Article 16), accessibility of the media (Article 17), primary responsibilities of parents (Article 18) protection from abuse, injury, neglect (Article 19), protection of the child temporarily deprived of its family environment (Article 20), protection of adoption and the adopted child (Article 21), protection of the child who is seeking refugee status (Article 22), the right of the disabled child to enjoy a full and decent life (Article 23), the right of the child to enjoy the best possible health (Article 24), to a periodic review of all the circumstances relating to its treatment (Article 25), the right of all children to an adequate standard of living (Article 27), the right of the child to education (Article 28), basic goals of education (Article 29), the right of the child belonging to a minority to enjoy its own culture, to practise its own religion or to use its own language (Article 30), the right of the child to rest and leisure (Article 31), protection from economic exploitation (Article 32), protection against the use of narcotic and psychotropic substances (Article 33), against sexual exploitation (Article 34), against abduction (Article 35), against all other forms of exploitation (Article 36), protection of children in armed conflicts (Article 38) and finally some rights for the child who has infringed the penal law (Article 40). See on this Convention: FORDER, C., 'Het gezin in internationale verdragen', *RM Themis*, 1997, No. 4, 137-142; Centrum voor de Rechten van het Kind, 'Het V.N.-verdrag inzake de rechten van het Kind en zijn directe werking in het Belgische (interne) recht', *Rechtskundig Weekblad*., 1992-1993, Vol. 56; 230; CLOSSET, G., 'La Convention des droits de l'enfant et la Belgique', *Révue Générale de Droit Civile Belge*, 1991, Vol. 5, 583 and foll.; VERHELLEN, E., 'Kinderrechten en onderwijs. Een driedubbele taak', *Tijdschrift voor Onderwijsrecht en Onderwijsbeleid*, 1997-1998, No.. 2, 74-77; SMITH, J., 'The Rights of the Child', in CASTERMANS-HOLLEMAN, M., VAN HOOF, Fr. & SMITH, J. (eds.), *The Role of the Nation-State in the 21st Century. Human Rights, International Organisations and Foreign Policy. Essays in Honour of Peter Baehr*, The Hague, Kluwer Law International, 1998, 163-173.

In the same way one could make a comparison between the ECHR and the recent Charter of Fundamental Rights of the European Union of 7 December 2000. This Charter not only proclaims a right to privacy similar to Article 8 of the ECHR, but also, and very important for us here, contains in Article 8 a fundamental right to data protection absent from the ECHR:

> *Article 8. Protection of personal data*
>
> 1. *Everyone has the right to the protection of personal data concerning him or her.*
>
> 2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> 3. *Compliance with these rules shall be subject to control by an independent authority.*

We will see below that the relationship privacy - data protection is not wholly without problems. These problems explain and justify the enactment in the Charter of the European Union of a separate right to data protection. To explain this we wish to go back to the origins of the Convention on data protection. Why is there such a Convention and why was Article 8 of the ECHR simply not enough?

The historical need for a Convention beside the ECHR

The advent of the Convention and of *data protection* in general as a distinct set of rules to govern the processing of personal data can only be understood in the light of the flaws in traditional western human rights protection.[20]

At the end of the 1960s the Parliamentary Assembly of the Council of Europe asked the Committee of Ministers whether the ECHR and national law gave sufficient protection to the right of privacy in view of developments in information processing. The committee concluded that there were several problems to be resolved: 1) The European Convention on Human Rights covers, in general terms, in Article 8, the right to a private life, but does not apply to the private sector. 2) The right to a private life would not necessarily include all personal data, and so there was a question whether a large proportion of data would be sufficiently safeguarded. 3) The right of access to data on oneself was not covered by the concept of the right to privacy as expressed in Article 8. In short, the European convention had a defensive approach to privacy and more positive action was necessary. As a result, in 1971 a Committee of Experts was established which prepared two recommendations with basic principles for the protection of privacy regarding electronic databanks. These recommendations were agreed in 1973 and 1974, one covering the private sector and the other the public sector (Resolutions (73) 22 and (74) 29). Without excluding the possibility of further action, it was felt that a common approach was necessary in both sectors. Meanwhile, the German *Land* of Hesse had passed the world's first data protection law in 1970, followed by Sweden in 1973 and several others in the next few years.

These laws led in the second half of the 1970s to the preparation of the Council of Europe Convention on data protection for three major reasons: 1) Several national data protection laws included provisions on transborder data flows restricting the export of data so that privacy would be protected. This permission or licensing system threatened international co-operation and communication. 2) Although national laws were inspired by the same basic principles, there were several differences in substance and procedure. Consequently, in the case of international data processing there could be serious problems of conflicts of law. 3) The human rights

[20] See: DE HERT, P., 'Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955-1997', in *Jaarboek ICM 1997*, Antwerp, Maklu, 1998, 40-45; HUSTINX, P., 'COE and Data Protection: What has been Achieved', *Transnational Data and Communications Report*, 1989, November, 21-22.

concept behind Article 8 of the European Convention on Human Rights needed to be expanded to more fully cover the processing of personal data. The drafting of the convention started in 1976 and it was opened for signature on 28 January 1981.

The reasons for adopting a separate convention are still valid

Let us return to the three initial problems with Article 8 of the ECHR as identified by the Committee of Ministers. (1) Article 8 of the ECHR does not apply to the private sector. (2) The right to a private life would not necessarily include all personal data, and so there was the question of whether a large proportion of data would be sufficiently safeguarded. (3) The right of access to data on oneself was not covered by the concept of the right to privacy as expressed in Article 8. It is our belief that today, many years later, this analysis, and hence the reasons for having a separate convention on data protection, still holds.

1) The problem of 'third party applicability' of *'Drittwirkung'* of contemporary human rights remains. Unlike the French 1789 *Déclaration*[21], most nineteenth and twentieth century constitutional and human rights documents are conceived from the view-point that that human rights are primarily recognised to strike a 'fair balance' between individual liberty and the interest of society. Therefore an individual cannot legally invoke human rights against another citizen supposedly threatening the rights of the former.[22] This also holds for the ECHR. For example, on the European level, a complaint against another private person will be declared incompatible *ratione personae* by the Convention organs and for that reason will be inadmissible.[23] Partly, the doctrine of the positive obligations remedies this[24], but the Convention is far from having

[21] The *Déclaration* is addressed both to the political institutions and the citizens. Cf. BOESJES, J., 'De horizontale werking van grondrechten', *Nederlands Juristenblad*, 1973, 906.

[22] It is, for instance, well-established US constitutional law that searches by private citizens, as opposed to government agents, are not restricted by the Fourth Amendment. Cf. Supreme Court, *United States v. Jacobsen*, *United States Supreme Court Reports (US)*, 1984, Vol. 466, 109 (upholding warrantless examination by drug agents of package opened and closed by delivery service employees). Also: Supreme Court, *Walter v. United States*, *United States Supreme Court Reports (US)*, 1980, Vol. 447, 649. See: LATZER, B., *o.c.*, 43.

[23] On the basis of Article 25 of the Convention only States can be held responsible. Complaints against other individuals will be declared inadmissible *ratione personae* as being 'incompatible with the provisions of the Convention' (ECHR Article 35 new; ECHR Article 27 old).

[24] Third party applicability of the Convention only exists in an indirect way, via the responsibility of the State Party. Violations of the rights and freedoms of the Convention by other individuals should then be construed as a State action (a failure of the domestic legislature, of the courts or of the administrative authorities). This 'solution' sometimes works: it can be derived from some of the decisions of the Convention organs that a State has to guarantee 'Drittwirkung'. For instance, with regard to Article 2 ('Everyone's right to life shall be protected by law'), applicants try to make the State responsible for physical harm caused by third parties. In *Osman v. the United Kingdom* (ECHR, *Osman v. the United Kingdom*, 28 October 1998, *R.A.D.-R.J.D.*, 1998, VIII; *NJCM-Bulletin*, 1997, Vol. 24, 512-524, annotation E. MYJER). The applicants asserted that by failing to take adequate and appropriate steps to protect the lives of the second applicant and his father, Ali Osman, from the real and known danger which Paget-Lewis, a teacher at the school of the second applicant who killed the second applicant's father, posed, the authorities had failed to comply with their positive obligation under Article 2 of the Convention. The Court confirmed that this article may imply, inter alia, positive obligation for a State to take preventive operational measures to protect individuals whose lives are at risk from criminal acts of another individual: "The Court notes that the first sentence of Article 2 para. 1 enjoins the State not only to refrain from the intentional and unlawful taking of life, but also to take appropriate steps to safeguard the lives of those within its jurisdiction (...). It is common ground that the State's obligation in this respect extends beyond its primary duty to secure the right to life by putting in place effective criminal-law provisions to deter the commission of offences against the person backed up by law enforcement machinery for the prevention, suppression and sanctioning of breaches of such provisions. It is thus accepted by those appearing before the Court that Article 2 of the Convention may also imply in certain well-defined circumstances a positive obligation on the authorities to take preventive operational measures to protect an individual whose life is at risk from the criminal acts of another individual (ECHR, *Osman v. The United Kingdom*, *l.c.*, para. 115). See about the positive obligations in regard to Article 2 ECHR: HARRIS, D., 'The Right to Life under the European Convention on Human Rights', *Maastricht Journal of European and Comparative Law*, 1994, Vol. 1, 129. See also: SPIELMANN, D., *L'effet potentiel de la Convention européenne des droits de l'homme entre*

acquired *de facto* horizontal effect.[25] Hence, many problems regarding for example working circumstances can only be dealt with by the Convention organs if the employer is a state organ.[26] Some courts in national legal orders have accepted to a certain extent the third party applicability of the European Convention, for instance in Luxembourg[27] and in the Netherlands.[28] Even when one assumes that this trend will continue, which remains to be seen[29], several problems still need to be solved. Most courts refrain from explicitly referring to the human rights listed in the European convention or the national bill of rights and do not take into consideration the limitation grounds incorporated in these texts, thus giving themselves greater discretion. This can result in a double system of human rights protection: a severe regime of protection for governmental infringements and a less severe, more flexible system for non-governmental infringements.[30]

---

personnes privées, Brussels, Bruylant, 1995, 160p.; LAWSON, R., 'Positieve verplichtingen onder het EVRM: opkomst en ondergang van de faire balance-test' (deel 1), *NJCM-Bulletin*, 1995, Vol. 20, No. 5, 559-567; VAN DIJK, P., '*Positive Obligations* Implied in the European Convention on Human Rights: Are the States Still the *Masters* of the Convention?', in CASTERMANS-HOLLEMAN, M., VAN HOOF, Fr. & SMITH, J. (eds.), *The Role of the Nation-State in the 21st Century. Human Rights, International Organisations and Foreign Policy. Essays in Honour of Peter Baehr*, The Hague, Kluwer Law International, 1998, 17-33. On the negative impact of the lack of horizontal effect on the liberties of workers: COLLINS, H., *Justice in Dismissal. The Law of Termination of Employment*, Oxford, Clarendon Press, 1992, 187-188. See also for the US: FINKIN, M., *Privacy in Employment Law*, Washington D.C., BNA Books, 1995, with 1999 Cumulative supplement, 477p.

[25] Cf. "it could be argued that State responsibility is not incurred if the link between the infringement and the domestic law is less obvious" (LAWSON, R., 'Out of Control, State Responsibility and Human Rights: Will the ILC's Definition of the 'Act of State' Meet the Challenges of the 21st Century?', in CASTERMANS-HOLLEMAN, M., VAN HOOF, Fr. & SMITH, J. (eds.), *The Role of the Nation-State in the 21st Century. Human Rights, International Organisations and Foreign Policy. Essays in Honour of Peter Baehr*, The Hague, Kluwer Law International, 1998, 107).

[26] On the issue of wiretapping by an employer: ECHR, *Alison Halford v. United Kingdom*, June 25, 1997, *R.A.D.-R.J.D.*, 1997, III, 1004-1038; *NJCM-Bulletin*, 1997, Vol. 22, 765-767. See: MYER, E., 'De niet bevorderde, getapte agente', *NJCM-Bulletin*, 1997, Vol. 22, 1088-1092; DE HERT, P., *Artikel 8 EVRM en het Belgisch recht. De bescherming van privacy, gezin, woonst en communicatie*, Gent, Mys & Breesch Uitgeverij, 1998, 347-349. The applicant, Ms Alison Halford, was born in 1940 and lives in Wirral. From 1962 until her retirement in 1992 she worked in the police service. She alleged that calls made from her home and her office telephones were intercepted for the purposes of obtaining information to use against her in the discrimination proceedings. The Court found that no provision in domestic law regulated these kind of interceptions. The interference was not "in accordance with the law" for the purposes of Article 8 para. 2 of the Convention, since domestic law did not provide adequate protection to Ms Halford against interferences by the police with her right to respect for her private life and correspondence. Hence, there had been a violation of Article 8 in relation to the interception of calls made on Ms Halford's office telephones (ECHR, *Alison Halford v. United Kingdom*, para. 51)

[27] SPIELMANN, D., 'Le Juge luxembourgois et la Cour européenne des droits de l'Homme' in TAVERNIER, P. (ed.), *Quelle Europe pour les droits de l'Homme?*, Brussels, Bruylant, 1996, 311-312, with ref.; SPIELMANN, D., *L'effet potentiel de la Convention européenne des droits de l'homme entre personnes privées*, *o.c.*, 44-55. The latter work also contains chapters on the situation in France, Belgium, Austria, Germany and Malta. See for the situation in Canada, the US and the United Kingdom: CLAPHAM, A., *Human Rights in the Private Sphere*, Oxford, Clarendon Press, 1993, 150-342.

[28] KLERK, Y. & JANSE DE JONGE, E., 'The Netherlands', in GEARTY, C. (ed.), *o.c.*, 122-123, with ref.: VERHEY, L., *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy*, Zwolle, W.E.J. Tjeenk Willink, 1992, 487p.

[29] In the Belgian cases on 'cameras on the workplace', there are judges and courts that consider the right to privacy incorporated in Article 8, ECHR, to be established sufficiently strongly in Belgian law to take it into consideration when judging conflicts between private persons (Kort. Ged. Rb. Brussels, November 6, 1996, *Journ.Procès*, 1996, No. 316, 26, annotation F. JONGEN), but at the same time there are other judges and courts that deny the applicability of this right (Arbeidshof Brussels, May 18, 1992, *Pasic.*, 1992, May-June, 71-72). See: DE HERT, P., *Privacy en het gebruik van visuele technieken door burger en politie. Belgische regelgeving vandaag en morgen*, Brussels, Ed. Politeia, 1998, 115-117.

[30] See in more detail: HERT, P., *Artikel 8 EVRM en het Belgisch recht*, *o.c.*, 53-55. A similar danger for a double standard system exists in regard to the so-called positive obligations implied in the ECHR. Broad application of this doctrine, could erode the spirit of the Convention, since the Court assumes that positive obligations do not fall under the limitations that exist for negative obligations. See: VAN DIJK, P., '*Positive*

2) Although the organs of the ECHR have recalled on several occasions that data protection is an issue which falls within the scope of Article 8 of the Convention[31], they have also held that not all aspects of the processing of personal data fall within the scope of the ECHR.

3) In the Leander case the Court states that the refusal to give Leander access to his personal data falls within the scope of Article 8 of the ECHR.[32] A claim for access therefore can be based upon Article 8.[33] But the Court also stipulates rather 'bluntly' that this does not mean that Article 8 of the ECHR gives a general right to access to personal data.[34] In the case of McMichael the right to access is again recognised.[35] But, as in the Leander case, a general right of access to personal data is not granted. In this case the Court does not explicitly deny such a right, but it 'simply' does not mention the issue.[36]

Privacy and data protection: twins but not identical

In 1998 De Hert concluded a long study of forty years of jurisprudence on the relationship between data protection and the right to privacy contained in Article 8 of the ECHR. The results may be summarised as follows:

- It shows that neither the Court nor the Commission uses terminology as we know it from the data protection rules and regulations. Although Article 8 of the ECHR is important, data protection issues or aspects can also be found in the Articles 5, 6, 10 and 13 of the ECHR. A general and conclusive right to data protection is not formulated in the jurisprudence of the Court.

- In particular, the Court makes a distinction between personal data that fall within the scope of the ECHR and personal data that do not fall within its scope. One could say that in the eyes of the Court there is processing of personal data that affects private life and processing of personal data that does not affect the private life of individuals.

- Moreover, it is striking to note that the Court and the Commission have paid very little attention to 'their own' Convention 108. It might not be too difficult to link Convention 108 more or less directly to Article 8 of the ECHR. In this respect the Case of Z v. Finland is remarkable. In this case the Court for the first time referred to Convention 108.[37] After a rather long period, the Court again referred to Convention 108 in the recent cases of and Amann[38] and Rotaru.[39] This does however not change the rather unimportant and not very influential position of Convention 108 with regard to the right to private life of Article 8 of the ECHR.

Analysis of the Court's decisions shows that the ECHR does not include an 'overall' right to the protection of personal data and that the ECHR does not provide data protection in the way Convention 108 does. Therefore it may be claimed that the ECHR should include a right to data protection, just as the EU Charter does.

Obligations Implied in the European Convention on Human Rights: Are the States Still the *Masters* of the Convention?', *l.c.*, 17-33.

[31] For instance: ECRM, Tom Lundvall v.. Sweden, 11 December 1985, case 10473/83, *D.R.*, vol. 45, 130.

[32] ECHR, Torsten Leander v. Sweden, March 26, 1987, *Séries A*, vol. 116 para. 48.

[33] Cf. ECHR, Antony and Margaret McMichael v. United Kingdom, 24 February 1995, *Series A*, vol. 307-B, para. 91.

[34] ECHR, Graham Gaskin v. United Kingdom, *l.c.*, para. 37.

[35] Cf. ECHR, Antony and Margaret McMichael v. United Kingdom, *l.c.*, para. 9.

[36] Cf. ECHR, Antony and Margaret McMichael v. United Kingdom, *l.c.*, para. 9.

[37] ECHR, Z. v. Finland, *l.c.*, para. 95.

[38] ECHR. Amann v. Switzerland, 16 February 2000, Case 27798/95, para. 65.

[39] ECHR, Rotaru v. Romania, 4 May 2000, *R.T.D.H.*, 2001, § 57 and 60.

III. THE RELEVANCE OF THE CONVENTION IN THE LIGHT OF THE EU DATA PROTECTION RULES

Following the adoption of the EU data protection regulations, an important question is whether the Convention still has a role to play. We think it does. The Convention has a number of advantages over the EU data protection rules.

Firstly, almost all member countries of the Council of Europe have signed the Convention, and it specifically provides for the possibility of accession by non-member states. Therefore the Convention has a global scope which does not apply to the EU data protection rules.

Secondly, The 1995 EU Directive does not apply to processing done by the police and secret services, because of a lack of competence in this area of the European Community.[40]

Thirdly, Convention 108 will remain important because EU data protection regulations are in many ways more politically influenced than the Convention is.

Fourthly, the information age, with no territorial boundaries, is more in need of a set of general and technology-neutral rules with strong international potential, than of a large number of very specific rights and obligations strictly dividing the information society into the European Union on the one hand, and 'the others' on the other 'privacy and data protection barbaric' hand.

IV. CONCLUDING THOUGHTS AND SUGGESTIONS

The main issue might well be the question whether (a) the Convention will remain a remarkable document containing a set of Guidelines aimed at decent processing of personal data on an international and global scale or, (b) whether the Convention will slowly become of less and less importance as the European Union based rules with their rather formalistic and bureaucratic nature gain more and more ground. An example of the fact that the EU regulations have the upper hand can be found in the Additional Protocol to the Convention, adopted on 23 May 2001 (opened for signature as from 8 November 2001), incorporating into the Convention the EU data protection ideas on supervisory authorities and on the transfer to so-called third countries.

The first option seems preferable to us. It is therefore worthwhile considering whether a specific right to data protection in the ECHR would strengthen the position of the Convention and strengthen an approach to data protection by means of general guidelines with global potential. A more preferable option may be to interest, for example, the United States of America, Canada or New Zealand in joining Convention 108 than trying to export the typically continental European Union data protection regulations across oceans. Wide acceptance of the Additional Protocol will probably not be very helpful in persuading the United States to join the Convention, and could undermine the general and global potential of the Convention.

These questions will be all the more important when we try to tackle privacy and data protection issues in the 'virtual' world of the Internet: A world without boundaries, physical territory, or effective ways of supervising and controlling the processing of personal data by means of national and governmental supervisory bodies. A world where the idea of 'first' and 'third' countries is by nature very problematic since the Internet in itself is global and boundary-free. The Internet seems more of a world where self-regulation based upon general principles seems more feasible than a territorially restricted approach aimed at detailed provision backed and controlled by national and government-oriented supervisory authorities trying to stop the 'natural' international transfer of personal data on the Internet.

[40] See Art. 3, 1995 Directive.

THE RELEVANCE OF CONVENTION 108

SUMMARY

In the report we compare Convention 108 rather extensively to the European Convention for the Protection of Human Rights and we compare the Convention with the EU data protection rules. We conclude that Convention 108 is still of importance. We raise the question whether the original and Guideline oriented approach of the Convention might not be more favourable than the more recent approach to data protection regulations set out in the EU data protection rules and in the Additional Protocol to Convention 108 opened for signature 8 November 2001. Another question raised is that adding a (new) right to data protection into the Convention for the Protection of Human Rights might be an option to consider.

I INTRODUCTION

The report concentrates on Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, concluded in 1950 and on on the Convention for the protection of individuals with regard to automatic processing of personal data, concluded on January 28, 1981 (hereafter the Convention). The convention can be seen as a landmark since European data protection saw the light with the Convention for the protection of individuals in regard to automatic processing of personal data. The Convention defines a number of principles for the fair and lawful collection and use of such data. Notably, data can only be collected for a specific purpose and should not be used for any other reason. Data must be accurate, adequate for this purpose and stored only for as long as is necessary. The convention also establishes the right of access to and rectification of data for the person concerned (data subject), and requires special protection for data of a sensitive nature, for example on religion, political beliefs, genetics or medical information. In order to become party to the convention, states must ensure that their national legislation contains these basic principles in respect to the personal data of every individual in their territory.

These basic principles of European data protection are also spelled out in the OECD-Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data and the European Data Protection Directive. The general ideas behind the three legal instruments are very similar. More or less, they all try to reconcile fundamental but competing values such as privacy, free flow of information, governmental need for surveillance and taxing, etc. The three texts and their principles apply to personal data, whether in public or private sectors. This is very crucial, because traditional human rights instruments only provide for protection against governmental actions.

II THE RELEVANCE OF THE CONVENTION IN THE LIGHT OF THE ECHR

Of great importance is Article 8 of the ECHR stating that: “(1.) Everyone has the right to respect for his private and family life, his home and his correspondence. (2.) There shall be no interference by a public authority with the exercise of this right except *such as is in accordance with the law* and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

The relationship privacy - data protection is not wholly without problems. These problems explain and justify the enactment in the Charter of the European Union of a separate right to data protection.

Article 8 of the ECHR has three problems that lead to the conclusions that Convention 108 is still relevant. 1) Article 8 of the ECHR does not apply to the private sector. 2) The right to a private life would not necessarily include all personal data, and so there was a question whether a large proportion of data would be sufficiently safeguarded. 3) The right of access to data on oneself was not covered by the concept of the right to privacy as expressed in Article 8.

Privacy and data protection: twins but not the same

In 1998 De Hert concluded a long study of jurisprudence on the relationship between data protection and the right to privacy contained in Article 8 of the ECHR. The results may be summarised as follows
- It shows that neither the Court nor the Commission uses terminology as we know it from the data protection rules and regulations. Although Article 8 of the ECHR is important, data protection issues or aspects can also be found in the Articles 5, 6, 10 and 13 of the ECHR. A general and conclusive right to data protection is not formulated in the jurisprudence of the Court.
- Especially the Court makes a distinction between personal data that fall within the scope of the ECHR and personal data that do not fall within its scope. One could say that in the eyes of the Court there is the processing of personal data that affects the private life and that there is processing of personal that does not affect the private life of individuals.
- Moreover, it is striking to note that neither the Court nor the Commission has paid much attention to 'their own' Convention 108. It might not be to difficult to link Convention 108 more or less directly to Article 8 of the ECHR. In this respect the Case of Z v. Finland is remarkable. In this case the Court for the first time referred to Convention 108.[1] After a rather long period, the Court again referred to Convention 108 in the recent cases of and Amann[2] and Rotaru.[3] This however does not change the rather unimportant and not very influential position of Convention 108 with regard to the right to private life of Article 8 of the European Convention for the Protection of Human Rights.

III THE RELEVANCE OF THE CONVENTION IN THE LIGHT OF THE EU DATA-PROTECTION RULES

Succeeded by the EU-data protection regulations, an important question is whether there is still a role to play for the Convention. We think there is. The Convention has a number of advantages over the EU data protection rules.

Firstly, almost all member countries of the Council of Europe have signed the Convention, and it specifically provides for the possibility of accession by non-member states. Therefore the Convention has a global scope not preset in the EU data protection rules.

Secondly, The EU 1995 Directive does not apply to processing done by the police and secret services, because of a lack of competence in this area of the European Community.[4]

Thirdly, Convention 108 can remain important because of the fact that EU data protection regulations are in many ways more politically influenced than the Convention is.

---

[1] ECHR, Z. v. Finland, *l.c.*, par. 95.

[2] ECHR. Amann v. Switzerland, 16 February 2000, Case 27798/95, par. 65.

[3] ECHR, Rotaru v.. Romania, 4 May 2000, *R.T.D.H.*, 2001, § 57 and 60.

[4] See Art. 3, 1995 Directive.

Fourthly, the information age without territorial boundaries is more in need of a set of general and technology-neutral rules with strong international potential, then it is in need of a large number of very specified rights and obligations strictly dividing the information society into the European Union on the one hand and 'the others' on the other 'privacy and data-protection barbaric' hand.

IV CONCLUDING THOUGHTS AND SUGGESTIONS

The main issue might well be the question whether (a) the Convention will remain a remarkable document containing a set of Guidelines aimed at decent processing of personal data on an international and global scale or, (b) whether the Convention will slowly become of less and less importance as the European-Union based rules with their rather formalistic and bureaucratic nature will gain more and more ground. An example of the fact that the EU regulations have the upper hand, can be found in the Additional Protocol to the Convention adopted 23 May incorporating into the Convention the EU data protection ideas on supervising authorities and on the transfer to so called third countries.

The first option seems more favourable to us. It is therefor worthwhile to consider whether a specific right to data protection in the ECHR would strengthen the position of the Convention and strengthen an approach of data-protection by means of general guidelines with global potential.

These questions will be all the more important when we try to tackle privacy and data protection issues in the 'virtual' world of the Internet. A world without boundaries, physical territory or effective ways to supervise and control the processing of personal data by means of national and governmental supervising bodies. A world where the idea of 'first' and 'third' countries is by nature very problematic since the Internet in itself is global and boundary-free. The Internet seems more of a world where self-regulation based upon general principles seems more feasible than a territorially restricted approach aimed at detailed provision backed and controlled by national and governmental oriented supervising authorities trying to stop the 'natural' international transfer of personal data on the Internet.

REPORT

THE RELEVANCE OF THE DATA PROTECTION PRINCIPLES SET OUT IN CONVENTION 108 AND ITS ADDITIONAL PROTOCOL

Report by

Ms Olga ESTADELLA YUSTE
Associate Professor of International Law
Autonomous University of Barcelona (Spain)

TABLE OF CONTENTS

INTRODUCTION

The Council of Europe has conducted pioneering work in the area of protection of the individual's privacy in respect of electronic data processing. As far back as 1968 the Consultative Assembly of the Council of Europe called upon the Committee of Ministers to do a study to establish whether the member states had enacted national legislation that protected adequately the individual's right to his private life in view of the recent development of information technology. The study found that the national legislations were not fully adapted to the changes introduced by the new information technologies. Based on the findings of this

study an Inter-governmental Committee of Experts was formed. The Committee of Experts was asked to propose appropriate measures to be adopted at the European regional level. Based on the proposals made by the Inter-governmental Committee, in 1973 and 1974, the Committee of Ministers approved two resolutions concerning the protection of the individual's life with regard to automatic processing of data both in the private sector[1] and in the public sector. These resolutions specified a number of basic principles of personal data protection. They left each member state entirely free to incorporate (or not) these principles in its national law whether by statute or through other forms of regulations. These two resolutions are of historic importance because they are the first international documents which contained "guidelines" addressed to member states with regard to personal data protection.[2]

These resolutions seemed to have served as source of inspiration for the more elaborate Convention for the protection of individuals with regard to automatic processing of personal data – Convention 108 – which further developed and elaborated the principles adopted in the two resolutions referred to above. On 28 January 1981 the Convention was opened for signature by the member states of the Council of Europe. It entered into force on 1 October 1985, three months after the date on which five member states had ratified the Convention.[3] Today, 20 years later, the importance of the Convention is still growing, not only because more than twenty member states have ratified the Convention, but in particular because the Convention was supplemented with a Protocol.

In this paper I will present an analysis of the relevance of the various data protection principles as defined in the Convention and its Protocol. First I will discuss which principles can be found in Chapter II of the Convention. Secondly, I will discuss whether there are other principles of data protection that can be found elsewhere. And thirdly, I will provide my personal view on whether there are grounds to propose a revision of some or all of the data protection principles found in the Convention.

1. FUNDAMENTAL PRINCIPLES OF DATA PROTECTION

The fundamental data protection principles are some general standards that apply to different types of personal data that are the subject of electronic processing in different business sectors, such as the banking sector, the marketing sector or for statistical purposes. Furthermore, these principles are not exclusively found in Convention 108. They are part of a much wider international tradition. Similar principles can be found in other international legal instruments (such as the Guidelines governing the protection of privacy issued by the OECD and the United Nations, and the Directive adopted by the European Union) and in the majority of national statutes on personal data protection.

1.1 Collection limitation principle

Article 5 of Convention 108 states this principle in the following terms: "Personal data undergoing automatic processing shall be obtained and processed fairly and lawfully, stored for specified and legitimate purposes and not used in any way incompatible with those purposes". This principle means that any automatic processing involving personal data must be conducted for a purpose that is socially accepted/justified. This wording seems to be related more to moral aspects regarding the freedom of the individual and the behaviour of individuals in a social context, than to the data themselves. Therefore one may ask: What does it mean that personal data may only be used for a purpose that is socially accepted? What are the constraints on the use of personal data and in what context do these constraints arise?

---

[1] Res. (73) 22 and Res. (74) 29, on the protection of personal data in automated data banks in the private sector and the public sector, 26 September 1973 and 1974.

[2] GARZON, G., "La protección jurídica de los datos de carácter personal: consideraciones metodológicas", *Primera reunión Nacional sobre Informatica y Derecho*. Mexico, 1982 , p. 14.

[3] Article 22.2 Convention 108. The first five States were: Germany 19.6.1985; Spain 31.1.1984; France 24.3.1983; Norway 20.2.1984; and Sweden 29.9.1982.

In general, one might think that the activities of the file controller that have a lawful purpose must be socially acceptable. Furthermore, the constraints on the use of data largely arise in the context of special categories of data. The special categories of data are certain data that, if not properly used, may cause serious prejudice to a person's interests or rights. In general, these categories of data include those revealing racial origin, political opinion, association with labour unions, religious or other beliefs, health, sexual life, and criminal record. It is not easy to determine the test that permits one to classify data as a special category. On the one hand, one may argue that there are no data that are per se, by nature, sensitive, and that any set of data may become sensitive depending on the context in which and the purpose for which they are used.[4] On the other hand, one may observe in today's customary practice that certain data, merely because of their nature, entail a serious risk of damage to and invasion of privacy.

As far as I am concerned neither view is incorrect, as both views recognise that constraints apply to the use of these data. Whether it is the data per se, or the context in which the data are used, is ultimately an academic question. However, I would like to stress that either view has drawbacks. Firstly, it may be inappropriate to adopt fixed categories of sensitive data – as Convention 108 does – because a particular category of data may be more special in nature in one country than in another country, depending on its sociological and cultural context in the countries involved. For this reason it seems more appropriate not to include an exhaustive list of special personal data but rather to offer each member state the opportunity to adjust in its national law the collection limitation principle to the cultural particularities of the member state.

Secondly, if special personal data are included in international instruments this may create the need to impose and enforce special conditions. For example, the application to the national data protection agency for a special permit to process special data to transfer such data across borders, or the allocation of more responsibility to the file controller containing special data, etc. Their inclusion in international instruments results in such special data becoming a class of data that trigger additional obligations both for the owner of the file and for the national data protection agency.

1.2 Use limitation principle

In general, the use limitation principle is intimately connected with the collection limitation principle and it is virtually a logical consequence of it albeit in its negative aspect. The objective of this principle is to avoid the creation or existence of files containing personal data that have been collected for arbitrary reasons or for no specific reason at all. The use limitation principle does not prohibit the collection, storage or the processing of personal data. It merely establishes limitations both in time and in quantity.

The limitation in quantity affects both the collection of personal data and the use of these data. It is not permitted to collect more data than the minimum quantity of data that is strictly necessary in order to achieve the purpose of the creation of the file. Furthermore the data cannot be collected by use of methods that are questionable. For example, one cannot collect data with hidden equipment that would accurately record the opinions of the persons involved or their personal images.

Therefore, the person to whom the data relate must know and be aware of the fact that his/her data are being collected. The limitation in quantity affects the use and the automated processing of personal data as it seeks to avoid change in the purpose originally established when the file was created. However, there are a few exceptions to the rule that the data subject must know and be aware of the collection. In particular when the national authority considers it appropriate, for a limited number of very specific reasons, such as in the interest of a criminal investigation.

---

[4] See OECD, *Explanatory Memorandum on the Guidelines Governing the Protection of Privacy and the TDF of Personal Data*. OECD, Paris 1981; CONCIL OF EUROPE, "Explanatory Report on the Convention for the protection of Individuals with regard to Automatic processing of Personal Data", *ILM*, vol.19, 1980, p. 299.

The limitation in time seeks to specify a period of time during which personal data may be stored or automatically processed. In practice it proves extremely difficult to specify the limitation in time as data files are created for so many different purposes and sometimes seek to achieve more than one objective. For this reason, rather than specifying a limitation in time (such as 10 years from the time of collection or creation of the file), the majority of international instruments provide that the limitation is established when the purpose of the file is achieved, or when the activity of the file controller ceases for external reasons. The principle of a limitation in time seeks to enhance a person's control over the existence of data that relate to him/her and a person's control over the possible exercise of his/her individual rights in respect of his/her data.

Convention 108 contains the use limitation principle. It states that the amount of personal data undergoing automatic processing shall not be excessive in relation to the purposes for which they are stored, and that the data shall be preserved in a form which permits the identification of the data subjects for no longer than is required for the purpose for which those data are stored. This provision makes clear that the limitation in time does not require the controller of the file to delete the personal data or to reformat the automated file, but rather that he/she only needs to remove that part of the personal data identifying the data subject. Hence, in most cases where the size of the population of data subjects is sufficiently large, removal of name and birth date, would be sufficient to comply with this principle. This solution seems to support the view that data exist that per se, or by nature, cannot be abused. However, this view is not without danger, because the storage of personal data without any specific object may facilitate the establishment of a connection between the data and the data subject which would enable the use of personal data for purposes different from the ones for which the file was originally created.

1.3 Data quality principle

The principle of data quality seeks to guarantee that personal data stored in automated or manual files are accurate and complete. In order to satisfy this principle the information must be accurate and up to date. What does it mean that the information must be accurate and up to date? One cannot apply this standard without taking into account the purpose of the file. For example, once the purpose of the file has been achieved, the data quality principle need no longer be observed because the data will be deleted from the system in accordance with the principle of limitation in time.

Traditional systems for the collection and processing of personal data made it extremely difficult to require the file controllers to update their databases at regular intervals largely because the processes were slow and required a large number of people. Because of these drawbacks in the traditional systems there was no social expectation that data that were stored were accurate and would be updated. With the arrival of new information technologies the social expectation has changed, in particular when it comes to the quality of the data. It should come as no surprise that the international instruments reflect this new social expectation. The first problem that one has to address is to establish the frequency with which personal data that have been collected must be verified and updated.

Some social groups have suggested that personal data must be updated on an annual basis, unless the system used to collect or store the data is able to verify the accuracy of the data on a continuous basis during the use of the file.[5] Other groups have suggested that the frequency with which data must be updated and the conditions that apply to the updating process should be left to the national data protection authorities.

Whether personal data meet the standard imposed by the quality principle becomes evident when the data subject exercises his/her right of access or when the data subject is negatively affected by the electronic processing.

---

[5] This was the view of UNESCO during the drafting of the UN Guidelines, *Guidelines for the regulation of computerised personal data files. Report of the Secretary General*. Sess. 44. Doc. A/44/606/ 24 October 1989.

Convention 108 states that personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored; and shall be accurate and, where necessary, kept up to date (Art. 5 c and d). Thus there is no obligation on the part of the file controller to update the personal data per se, because the standard adopted by the Convention is very flexible. Updating is only required "where necessary". Hence one may ask: "How does one decide whether it is necessary or not to update personal data?" and "Who makes this decision?" One must assume that the decision is made by the file controller, and that it becomes necessary to update personal data when there is a real and imminent risk that the personal data held may cause prejudice to the data subject or his/her interests.

1.4 Purpose specification principle

This principle implies an obligation to specify the purpose for which a file is created. In other words, personal data must be used only in accordance with the purpose as initially specified. This principle is intimately linked with the data quality principle and with the limitation principle that have been discussed above.

The moment in which one must specify the purpose of the file cannot be after the data have been collected. Thus the purpose specification principle acts as a mechanism that makes it impossible to collect, store or use personal data in a form or manner that is not foreseen by the member states. It is only possible to collect data that are strictly necessary in order to achieve specific purposes established by the file controller (limitation in quantity). The specification of the purpose of the file is needed, in the first place, for the benefit of the data subject. It includes an obligation to inform the data subject as to why his/her personal data are being collected and that his/her personal data may be transferred across borders. In the second place, the file controller must inform the national data protection agency of the specified purpose of the file.

The methods that can be used to enforce the specification principle are numerous and can be chosen depending on whether the personal data are to be used in the public sector or in the private sector. In the public sector methods of communication may be used, such as publication of the purpose for which the automatic file is created in the official gazette. In the private sector general methods of communication may be used, for example a newspaper with local or national distribution, or a direct notification of the person involved, among others.

Convention 108 provides that personal data undergoing automatic processing shall be stored for specified purposes and not used in a way incompatible with those purposes. This provision is clear. Personal data cannot be used for purposes that are not compatible with those given originally.

1.5 Security Principle

The security principle imposes on the owner of a file the obligation to establish measures that protect personal data against the risks of partial loss, complete destruction, modification and inadequate access. The objective that is being pursued by this principle is to maintain the confidentiality and integrity of personal data despite external actions that may create a risk and consequently prejudice the interests and the rights of the individual. This is a very important principle, because ultimately the real protection of personal privacy depends, to a large extent, on the security measures that have been adopted by the administrative entity, i.e., the file controller.[6] The majority of the international instruments concerning personal data protection do not provide an exhaustive list of the security measures that the file controller must adopt, although they do provide general standards that can be implemented in each member state's national laws in the most appropriate form. In general, security measures must always seek to prevent: a) accidental destruction resulting from natural causes (fire, water, etc.), human causes

[6] According to a study on the categories related to the security measures for data processing, the causes are the following: 65% errors, 13% dishonest employers, 8% inappropriate infrastructure, 6% ex-employers, 5% others, 3% persons not related to the file activity. See COURTNEY, R.H., "Proper assignment of responsibility for data security", *Information Age*, vol.11, num.2, 1989, pp.84.

(error in data transmission, or in programming, etc.) or mechanical failures of either hardware or software; b) intentional destruction resulting from sabotage or vandalism; c) inadequate access to personal data resulting in the modification, inadequate transmission or inappropriate use of data.

The security principle raises a number of questions such as, for example, “What security measures are considered appropriate?” To define these standards it will be necessary to underline those that guarantee the security of the files according to the knowledge of an expert in the matter. Moreover, it goes without saying that the effectiveness of the security measures depends on their periodic updating and the adoption of new measures to incorporate advances in technology. This is particularly important since recent advances in technology have increased the opportunities to access computer servers that are stationed off-site, from a person’s home.[7]

The responsibility for enforcing compliance with the security principle, and deciding whether or not security measures that have been adopted are “reasonable” and “appropriate” lies with the national data protection authority.[8] Moreover, in the event of international data transmission, the data protection authority must assess whether the foreign controller of the file complies with identical or similar security standards.

Convention 108 provides that appropriate security measures shall be taken for the protection of personal data stored in automatic files against accidental or unauthorised destruction, accidental loss, and against unauthorised access, alteration or dissemination (Art.7). In the explanatory memorandum to the Convention it is stated that the security measures that must be adopted depend on the following factors: a) the sensitivity of the data (obviously sensitive data require tighter security measures); b) the need to restrict access to the data; c) the need to store the data for a long period; d) the risk that a specific file poses; and e) the role that the file plays, among others. This makes it evident that security measures are adopted for each concrete case. Therefore the national laws prescribe which security measures the file controller must adopt and whether they require approval from the national data protection authority. Similarly, the explanatory memorandum to the Convention stresses that security measures must be adopted in accordance with the methods and techniques developed by information technology.

1.6 Individual participation principle (the right to know, to access and to correct)

1.6.1 The right to know

The right to know[9] consists of knowing that a file exists that contains one’s personal data, the objective or purpose for which the file was created, the identity and the residence of the file controller, and knowing whether the file is intended to become part of the data that are circulated internationally.

When this right was created, it was understood that the file controller had an obligation to notify, individually, each of the persons whose personal data have been collected in the electronic files, including in those instances where the data subject affected had provided his personal data to the file controller. In practice what is used is a more limited method, and something more closely related to the right to access, notably that the file controller discloses the data prior to an application by the data subject affected. The disclosure of these data must be conducted in a manner that makes the data comprehensible for any person who does not have a thorough understanding of

---

[7] COUNCIL OF EUROPE, *New Technologies: a Challenge for the Protection of Privacy*. Study prepared by the Committee of Experts on Data Protection (1989).

[8] Kirby studied the possibility that file controllers should take out an insurance policy against loss or damage during the automatic processing of personal data. KIRBY, M.D., "Legal aspects of information technology", in: OECD (ed.), *An Exploration of Legal Issues in Information and Communications Technologies*, Series of Information Computer Communication Policy, vol 4, Paris, 1983.

[9] In general, on the right to know: SEIPEL, P., "The Right to know", p.7-45, in BLUME, P., (ed.), *Nordic Studies in Information Technology and Law*, Kluwer Computer and Law series, Deventer, The Netherlands, 1991.

advanced information technology. The time needed between the moment of application and the disclosure of the data must be reasonable. This formula guarantees to a person that his personal data are not diverted to purposes that are different from those specified.

As far as the guarantees of individual rights to data protection are concerned they can be extended to the right to access and the right to correct. In these cases a person may exercise his rights either by filing a complaint with the national data protection authority or by initiating legal or administrative proceedings. Both options are not available in all countries. In particular in countries that have adopted data protection laws only for particular sectors (the so-called sectorial approach) and consequently do not have a national data protection authority, a data subject has only one option, namely to initiate legal proceedings. On the other hand, in countries that have adopted data protection laws covering all activities affecting personal data (the so-called omnibus approach) a person is normally required to first file a complaint regarding a violation of his individual right to data protection, with the national data protection authority. The authority will review the merits of the complaint. The majority of the national laws allow a data subject to lodge an appeal against the decision of the national data protection authority with the civil or administrative courts. And in some specific cases the data subject may bring a claim in a civil or administrative court directly, without having to exhaust his remedy before the national data protection authority. However, having to enforce individual rights through the courts in order to resolve a dispute has drawbacks. It tends to be slow and costly, in particular when the case requires the court to hear experts in order to resolve the matter.

Convention 108 adopts a minimum standard in respect of individual rights thereby leaving discretion on the part of the member states to grant in their national laws a wider measure of protection than that stipulated in the Convention (Art. 11). The Convention recognises the right to know the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the file controller. The same provision provides that any person shall have a remedy if a request for confirmation or, as the case may be, communication, rectification or deletion is not complied with.

1.6.2 The right of access

The right to access is a personal right that cannot be exercised by anyone except the person affected by the data collected in the manual or automated files.[10] This does not imply that those who exercise this right are required to reveal the reasons why they wish to access the data. The mere existence of the data in an automated personal file is sufficient to create this individual right on the part of the data subject.

The right to access implies that the data subjects affected are entitled to know what information concerning them has been collected and stored in an automated or manual file. The file controller may comply with his obligation to grant access in various manners. The most common is by sending a copy of the personal data held in the file. This copy must contain information that can be understood without the need for advanced knowledge of information technology in order to understand it. It may consist of a photocopy, a printed copy, or a reproduction of the data after having undergone editorial changes – deletions – in order to prevent disclosure of data concerning third parties.

Another method of complying with the obligation to grant access is by providing the data orally in an interview with the data subject without providing physical access to the file containing the personal data, so that in effect the file controller provides the requested information. Moreover, the file controller does not have an obligation to disclose in detail the methods employed in order to achieve the purpose for which the personal data have been collected. Is a data subject entitled to exercise his right to access data which have been registered provisionally? Or is a data subject only entitled to exercise his right to access in respect of personal data that have already been the

[10] According to Rodotá the right of access is a fundamental right of the individual whose information is being processed. RODOTA, S., "Protecting Informational privacy: trends and problems", in: Korthals, W.F., et al.(ed.) *International Law towards the 21st Century*, Kluwer, 1992, p.261-273.

object of automatic processing? I take the view that a data subject is entitled to exercise his right to access even if his data have not yet been processed automatically.

One of the difficulties of exercising the right of access involves the ability to transfer this right to third parties so that they may exercise it in the name of the data subject. The international instruments do not take a position with respect to the question of whether this right may be assigned by the data subject to a third party in the same fashion as any other right that is alienable, or whether this right is a human right and as such is inseparable and not capable of being assigned. The majority view among scholars is that the right to access is not subject to being of legal age, or having full physical or mental capacities. In those instances where it is established that a data subject is not capable of exercising his right to access, access may be provided using a court order. A contrary view would result in the exclusion of these persons from this right. However, access provided using a court order must be executed in the interest and for the benefit of the data subject and not to satisfy the interests of third parties, such as the parents or the custodian, among others.

Convention 108 recognises that any data subject may obtain at reasonable intervals, and without delay or at no excessive cost, *confirmation* that an automated file containing personal data relating to him exists, and a *communication* of these personal data in a manner that can be understood (Art. 8 b). This provision distinguishes between "confirmation" and "communication". According to the explanatory memorandum of the Convention, "confirmation" means a simple notification which may be given either by the file controller or by the national data protection authority.[11] The data subject may exercise his right to access either directly by contacting the owner of the file, or indirectly in those instances where the national authorities maintain a register of the files that exist and of the data that they contain. With the "communication" the right to access reaches the ultimate limit of its scope. The data subject is informed in certain detail about the information that refers to him and that is collected and stored in automated or manual files. This communication must be made by a method that can be understood and at no excessive cost, and member states are free to decide as to whether the costs must be charged to the file controller or to the data subject.

1.6.3 The right to correct

As a result of the right to access files, whether domestic or foreign, the data subject may learn that the data collected are not correct, or are not in accordance with the substantive provisions concerning data protection. For this reason the possibility is provided that the data be corrected. The right to correct can only be exercised in respect of personal data of a factual nature and not in respect of opinions or views based on such data. This right is exercised by making a request to the file controller: a) that the data be completed; b) that incorrect data be deleted or erased; c) that the data be corrected when due to practical problems it is impossible to erase the data; d) that the incorrect data be corrected; e) that those data that have been collected or processed in a manner that is not in accordance with the substantive provisions on personal data protection be erased (e.g. sensitive data in an ordinary file). When the incorrect data have been corrected the file controller must notify the data subject.

The Convention recognises the right to correct personal data (Art. 8 c), when the data have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in the Convention. By reading the relevant provisions of the Convention it does not become clear whether a data subject may exercise his/her right to correct during collection of the data or when the automatic processing has begun.

1.7 Exceptions to the basic principles of personal data protection

The Convention states some exceptions in respect of all these principles, except the security principle in its Article 9. The exception must be provided for by the law of the member state and constitute a necessary measure in a democratic society in the interests of: a) protecting State

[11] Explanatory Report, Convention 108.

security, public safety, the monetary interests of the State or the prevention of criminal offences; b) protecting the data subject or the rights and freedoms of others.

Another restriction created in this article, but one which only affects the rights of the individual, is the restriction to files used for statistical purposes[12], and for scientific purposes, when there is no manifest risk that the privacy of the data subjects may be negatively affected.

2. OTHER PROVISIONS IN THE CONVENTION WHICH RECOGNISE PRINCIPLES ON PERSONAL DATA PROTECTION

Chapter II of the Convention refers to the basic principles of data protection, and this reference raises two questions. The first is whether these principles are indeed the only principles recognised by the Convention, or whether in other provisions the Convention contains more basic principles of data protection that are of general application. Personally I favour the second possibility. For example, the accountability principle may be deducted from Article 8 of the Convention, even though this principle does not appear in Chapter II. Moreover, there can be no doubt that the Convention and its Protocol recognise the principle of free movement of personal data among member states, although it does not appear in Chapter II. Finally, I consider the principle of cooperation and mutual assistance between member states a principle that has been sufficiently recognised to qualify as a basic principle. The Convention dedicates its entire Chapter IV to the cooperation and mutual assistance between member states, a fundamental topic in international conventions concerning data protection, where the continuous transborder transmission of personal data could easily create problems to the states. These three principles will be discussed in more detail subsequently.

I answered the first question positively. The second question is whether it would be appropriate to include all these three additional basic principles in the same chapter. In my view it would not only be appropriate, it would also be necessary to do so because Chapter II is increasingly becoming the hard core of data protection, the importance of which may in due course extend beyond the Convention when it becomes part of European customary law.

2.1 Accountability principle

The accountability principle is based on a clear international tradition in other international instruments concerning personal data protection, such as the Guidelines of the United Nations and the OECD, and the Directive of the European Union. Nevertheless, although Convention 108 does not include the accountability principle expressly as part of the other basic principles, it can be deducted from various provisions of the Convention. Therefore it is not meant to be excluded from the text.

The Convention confirms on the one hand that the file controller decides the purpose of the automated file, the categories of personal data that are registered and the operations that are conducted. On the other hand, the provisions of the Convention grant a set of remedies to the data subjects which permit the data subjects to enforce their rights when they are infringed and to denounce the infringement of the provisions of domestic law that give effect to the basic principles of data protection (Art. 8 d and Art. 10). Based on the above, one may conclude that these are remedies against the file controller, and hence it is his responsibility that the files meet the standards pursuant to the Convention.

What is the scope of the accountability principle? This principle implies the need to identify the file controller, whether national or foreign, who has collected the personal data, so that he may be assigned a set of responsibilities derived from carrying out automatic processing of personal data. An important question is whether the responsibility for any non-compliance with the legal

[12] In particular on the access to statistical information, HOESEL, "Access to statistical data for policy-oriented research in the Netherlands", p.34, in: *Seminar on openness and protection of privacy in the information society*, Voorburg, 1987; RAPAPORT, "Statistical information as a tool for authorities and citizens", p. 16 in: *Seminar on openness and protection of privacy in the information society*, Voorburg, 1987.

obligations must rest exclusively with the file controller or whether it must be shared among those involved in the operations of automatic processing of personal data. The majority views seem to be that liability lies exclusively with the person/entity that decided to create the file.[13] This implies the need to specify the purpose of the file, because from that moment on, the controller has to observe the legal provisions regarding the matter. Consequently the person who has decided to create the file need not be the same as the owner of the business where the file is located.

On the matter of shared responsibility, Turn[14] has distinguished three categories of responsibilities for persons who are involved in automatic processing. The first category are responsibilities that the data controller should be accountable for. This is the person, agency or institution (public or private) that has authority over the data file and over the automated processing that is being conducted. The second category are responsibilities that rest on the custodian of the file. This is the agency or entity whose employees are in physical possession of the file and who conduct automatic operations. These persons are responsible for compliance with the security measures determined by the file controller. The third and last category is the user. This is the person or agency authorised by the file controller to use certain data files in accordance with the framework specified by the controller. The user shall be liable for use of the personal data in accordance with the terms stipulated by the controller.

In general, the principle of responsibility is not invoked until the file controller has failed to perform the legal obligations. His obligations may be divided into two categories. The first is of a general nature. It provides that the automatic processing of personal data must comply with the basic principles and it must guarantee the basic rights of the data subject.

The second category of obligations has a more specific nature. This category is related to the provisions on data protection stated in the national laws. The file controller shall: a) comply with the requirements in respect of the inscription of files, notify the national data protection authority of a change in address or in ownership of the file, apply for a permit to transmit the personal data across borders (if required by domestic law); b) guarantee that the transmission of personal data across borders does not violate any basic principles of data protection; c) apply for a permit from the national data protection authority to change the purpose of the file; d) adopt internal codes of conduct that adequately reflect the data protection principles.

2.2 The principle of free movement of data among member states

Another principle that the Convention and its Protocol recognise, and that in my view should be included in the chapter of basic principles, is that related to transborder data flows. I refer to the principle of free movement of data among member states that guarantees the protection of the data. This notion is captured in Chapter III and in the preamble of the Convention. In particular, the idea that a balance must be struck between the principle of free movement of data, on the one hand, and that of respect for privacy in view of the progress of information technology, on the other hand, motivated the Council of Europe to adopt a convention that could reconcile these two fundamental values that are enshrined in the European Convention on Human Rights of 1950. I do not suggest that all the detailed provisions applying to transborder data flows should be incorporated in the basic principles. I just propose that this general principle should be mentioned together with the others.

Are there any precedents where this principle was incorporated in other international instruments or national legislation? Both the Guidelines governing the protection of privacy of the United Nations and the OECD incorporate this principle. The OECD Guidelines are particular in the sense that they make a distinction between basic principles of national application and those of international application. The principle of free movement of data among member states is included in the second

[13] In general, see HELLNER, J., "Liability in the computer context", p. 81, in: Seipel, (ed), *From data protection to knowledge machines*, Kluwer, 1990.

[14] TURN, *Privacy and security in personal information data-bank systems*, Rand Corporation, Santa Monica, 1974, pp. 40 ss.

group of principles. As far as national legislations are concerned, the majority contain provisions that recognise this principle, although they do not mention it together with the other basic principles.

Why is this principle important? It is commonly known that the new information technologies increase the speed and the frequency with which automated files containing personal data may be transmitted across borders. This fact has not passed unnoticed by either lawyers or legislators who have tried to prevent the level of privacy protection from being reduced as a result of automated processing of personal data in third countries.

Provisions setting standards for the protection of personal data need not only be adopted at the national level. It is important that such protection is supplemented by standards that apply to activities outside the national territory.

Choosing a solution at the national level that promotes strict privacy protection that restricts transborder data flows would not be adequate. Such strict protection would be counter to the principles of international law, such as the principle of freedom of communication and information. Moreover it could negatively affect international trade and commerce. For this reason Convention 108 and other international instruments on data protection have observed a need to adopt certain standards and restrictions that enable a balance to be struck between the international principles of data protection and domestic legal provisions. In summary, the provisions in international instruments on transborder data flows have as a primary objective privacy protection without posing an excessive burden on the free flow of information so as to avoid negative effects on trade and commerce, and international relations.

2.3 The principle of co-operation and mutual assistance

Another principle that would be appropriate to include in the hard core of the principles of this Convention is that of cooperation and mutual assistance between member states in matters relating to data protection. As mentioned before, it is not necessary that the entire Chapter IV about mutual assistance and Article 1 of the Protocol be incorporated in the basic principles. It would be sufficient to add a general provision that states the obligation of the member states to cooperate internationally in matters of data protection, in particular when transborder data flows are involved. Although in the national legislation one will not find such a provision among the basic principles, this provision is frequently included among the responsibilities of the national data protection authority.

3. PROPOSAL FOR A POSSIBLE REVISION OF CONVENTION 108

Anyone who assesses the 20 years during which Convention 108 has been in force will come to the conclusion that the Convention has been a great success. It has been ratified by a large number of member states which in turn means that these states have adopted national data protection laws. In other words, each member state has created its own national data protection authority which ensures that the principles set forth in the Convention are properly incorporated and enforced in its national legal system. Therefore one may say that today at the European regional level individual privacy is adequately protected against intrusion from information technology.

However, despite all the positive aspects of the Convention, one may ask whether there are any reasons to amend or revise the Convention. Without any doubt the extent to which society uses information technology has increased dramatically during the last twenty years, resulting in new problems that would have been inconceivable only a few years ago and that may pose a threat to privacy. To what extent is it appropriate to bring the Convention up to date so as to address the new challenges posed by our society that uses more information technology every day? In my opinion it is not necessary to conduct a major revision that would modify the Convention substantially. However, it may be appropriate to revise some aspects of the Convention, for the following reasons.

In the first place, one must not forget that Convention 108 is closely linked to the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950, in particular its Article 8. For this

reason Convention 108 has sought and must continue to seek to increase the scope of the protection of human rights, in particular the right to private life, although it must attempt to reconcile it with the freedom of movement of information among nation states.

In the second place, the Council of Europe has used recommendations as an alternative mechanism that may regulate new challenges posed by information technology, that affect personal data, and that supplements the basic principles for specific sectors. Among the recommendations adopted by the Committee of Ministers of the Council of Europe are: the medical sector, statistics and research and development, the marketing sector, the social security sector. Strictly speaking, these recommendations do not constitute more than sectorial instruments prescribing certain minimum standards. The majority of the recommendations are limited in scope and only seek to regulate those aspects of a sector that – one may argue – require legal regulation of personal data protection.

Those recommendations are directed to the Governments and they are not binding in nature. In other words, member states of the Council of Europe are not obliged to follow these recommendations and to implement them into their national laws.[15] As has been pointed out by many legal scholars, the fact that these so-called measures of "soft law" are uncertain, as far as their legal nature is concerned, does not mean that they do not have some legal effect. Carrillo Salcedo has held that provisions of "soft law" "express aspirations concerning legal policies adopted by the majority of the international community and they manifest, if nothing more, the need for new standards that reflect the generally shared beliefs".[16] Other legal scholars have argued that the acceptance of a principle of "soft law" may have the effect that the member state concerned cannot act in a manner that is contrary to the principle, except when there is a fundamental change in circumstances.

Regardless of the legal effect that standards of "soft law" may or may not have, one may argue that it is possible that with the progressive acceptance of these standards domestically a new customary practice is being developed, which in time may evolve into a standard of customary international or regional law. However, it remains to be seen in which direction state practice and international practice will develop so as to determine to what extent these standards are legally binding.

In summary, for the reasons expressed, I do not believe that it is necessary to substantially modify the Convention, though it would be appropriate to revise its hard core, in other words, its basic principles. In particular, the list of basic principles should include the accountability principle, that of cooperation and mutual assistance, and that of free movement of information among member states. Moreover, it would seem appropriate to move to another chapter the provisions that are not closely related to the basic principles, such as those that state exceptions and restrictions (Article 9), sanctions and remedies (Article 10) and the obligations of the parties (Article 4). Thus, a complete list of basic principles of personal data protection would permit their application to various sectors (from the marketing sector to the criminal law enforcement sector). Moreover it would leave sufficient latitude on the part of the member states that have ratified the Convention to develop and extend these principles in their respective national laws.

---

[15] However, according to Heredero´s study on Recommendation No. R (87) 15 regulating the use of personal data in the police sector, Spain not only accepted, but also stated that this recommendation "implies a compromise for Spain". HEREDERO HIGUERAS, M., "El uso con fines policiales de los datos personales registrados en soporte informatizado", *Anuario 1992 Computerworld*, 1992, pp.36.

[16] CARRILLO, *Curso de derecho internacional público*, Tecnos, Madrid, 1991, pp. 133.

THE RELEVANCE OF THE DATA PROTECTION PRINCIPLES SET OUT IN CONVENTION 108 AND ITS ADDITIONAL PROTOCOL

SUMMARY

The data protection principles are general standards that apply to different types of personal data that are the subject of electronic processing in different sectors, such as the banking sector, the marketing sector or for statistical purposes, the public sector. These principles are not exclusively found in Convention 108, but they are part of a much wider international tradition that can be found in other international legal instruments (such as the Guidelines governing the protection of privacy issued by the OECD and the United Nations, and the Directive adopted by the European Union) and in the majority of national statutes on personal data protection.

In this paper an analysis is presented of the relevance of the various data protection principles as defined in Convention 108 and its Additional Protocol. First the principles in Chapter II of the Convention will be discussed. This is the case for the collection limitation principle, the use limitation principle, data quality principle, purpose specification principle, security principle, individual participation principle: the right to know, the right of access and the right to correct.

Secondly, the question will be discussed of whether there are other principles of data protection that can be found elsewhere. Chapter II of the Convention refers to the basic principles of data protection, and this reference raises two questions. The first one is whether these principles are indeed the only principles recognised by the Convention, or whether in other provisions the Convention contains more basic principles of data protection that are of general application, such as the accountability principle, the principle of free movement of personal data among member states, or the principle of cooperation and mutual assistance between member states. Subsequently these three principles will be discussed in more detail together with the question of whether it would be appropriate to include these three additional basic principles all in the same Chapter II of the Convention.

And thirdly, a personal view will be provided on whether there are grounds to propose a revision of some or all of the data protection principles found in Convention 108.

REPORT

MECHANISMS FOR IMPLEMENTATION AND INTERNATIONAL CO-OPERATION IN THE CONTEXT OF DATA PROTECTION: EXISTING MECHANISMS AND MECHANISMS TO BE ESTABLISHED

Report by

Mrs Diana ALONSO BLAS
Senior International Officer
Dutch Data Protection Authority
(The Netherlands)

TABLE OF CONTENTS

INTRODUCTION

This report has been written for the European Conference on Data Protection that will take place in The Royal Castle, Warsaw (Poland) in November 2001.

As the title of this conference is *The Council of Europe Convention 108: present and future,* this document mainly concentrates on the text of the Convention and, where appropriate, other Council of Europe instruments. Convention 108 was the first international instrument in the field of the protection of personal data and has therefore played a fundamental role in this domain,

inspiring all national legislation which came into force from the moment of its adoption on. The importance and great value of the Convention is undeniable.

However, as one of the objectives of the conference is to examine the Convention in the light of the developments that have taken place during the last twenty years, this report will also refer to other relevant international texts in this field and, in particular, to the text of the European data protection directive[1].

Several reasons justify using the Directive as an element of reference in this report.

The Directive, as explained in Recital 11 of its preamble, gives substance to and amplifies the principles contained in the Council of Europe Convention. It is based on the same principles but it is more extensive and detailed. It contains therefore a number of new interesting elements and develops others that already existed in the Convention.

Furthermore, from the moment of its adoption, the Directive has had a substantial influence on the discussions within the Council of Europe, not only because of the obvious interest of its provisions for those working in the data protection field, but also due to the fact that all the Member States of the European Union have ratified Convention 108 and are therefore represented in the Consultative Committee of the Convention.

In practice, the majority of the members of the Consultative Committee are members of the European Union and are hence obliged to comply with the provisions of the Directive.

I. MECHANISMS FOR IMPLEMENTING DATA PROTECTION PRINCIPLES, IN PARTICULAR THE ROLE OF SUPERVISORY AUTHORITIES

This chapter will examine in the first place the rules of the Convention and the European Directive concerning this matter as well as the new provisions contained in the Additional Protocol to the Convention adopted on 23 May 2001.

Thereafter, attention will be paid in particular to the role played by the different data protection authorities in Europe and a general description of the differences and similarities between them will be given.

Against this background, the necessity or desirability of amending the provisions of the Convention concerning these issues will be examined.

The provisions of the Convention

Chapter II of Convention 108[2] deals with the basic principles for data protection[3]. The issue of the implementation mechanisms for these principles is only addressed in one article of the Convention, Article 10.

---

[1] The European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, Volume 38, 23 November 1995, page 31. From now on referred to as “the Directive”.

[2] Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981.

[3] See for a detailed explanation of the principles, the paper by Jean-Philippe WALTER, *La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et la coopération internationale à l'aube du XXIe siècle*, presented at the 20th Data Commissioners Conference in Santiago de Compostela, Spain, September 1998.

Article 10 reads as follows:

> Article 10: sanctions and remedies
>
> Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

The text of the explanatory memorandum to the Convention offers a quite short explanation concerning this issue in point 60. It mainly addresses two questions:

- The duties of the data users and the rights of the data subjects should be reflected in the national legislation of Member States by corresponding sanctions and remedies in order to guarantee effective data protection by the Convention.

- In accordance with the non-executive character of the Convention, each Member State should be free to determine the nature of these sanctions and remedies. The text mentions three possibilities: civil, administrative or criminal.

It is relevant to notice that the Convention did not at that point impose any obligations on the Parties concerning the creation of a data protection authority. However, most of the national rules giving effect to the Convention provided for such an authority.

The European Court of Human Rights has underlined in some cases the necessity of having an independent authority that could assess the conformity of data processing operations with Article 8 of the European Convention on Human Rights[4].

More recent instruments of the Council of Europe[5] have recommended setting up such an authority and the United Nations Guidelines of December 1990 also include this obligation[6]

Mechanisms of implementation in the European Directive

The provisions of the European Directive on mechanisms of implementation are much more detailed than Article 10 of the Convention. Chapter III of the Directive bears the title Judicial remedies, liability and sanctions. In addition to that, Article 28 imposes on the Member States of the European Union the obligation to have one or more supervisory authorities and defines in detail the tasks to be entrusted to these authorities.

Different reasons explain this difference in approach.

- In the first place, it should be recalled that the Directive came into place almost fifteen years after the Convention. During these years data protection doctrine had been developed in greater detail and almost all the countries of the European Union (with the exception of Italy and Greece) had legislation in place based on the Convention. The Directive benefited consequently from all the practical experience accumulated during those years.

---

[4] As underlined by Jean-Philippe WALTER in his paper *La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, published in A. Epiney/M. Freiermuth (edit.), *La protection des données en Suisse et en Europe*, Fribourg 1999, p.83ss. In particular J.P. Walter mentions the case *Gaskin v. United Kingdom* (7 July 1989) and *Kopp v. Switzerland* (25 March 1998).

[5] Such as the Recommendation No. R (97) 18 on the protection of personal data collected and processed for statistical purposes.

[6] Guidelines concerning computerized personal data files, adopted by the General Assembly on 14 December 1990, in particular § 8.

- In the second place, it should be underlined that the Convention and the Directive have a different nature and are part of a different legal system. While the Convention has a non-executive character and should be viewed in the framework of Public International Law, the Directive can impose much more specific obligations on the Member States of the Union, which are then, under European Law, obliged to implement its provisions into national law.

The provisions of Chapter III of the Directive can be summarised as follows:

- Article 22, Remedies, states that the Member States of the European Union should provide for the right of every person to a judicial remedy for any breach of his/her rights concerning the processing in question. This judicial remedy should exist in addition to any administrative remedy prior to referral to the judicial authority that might exist under national law, for instance before the supervisory authority.

- Article 23, Liability, obliges Member States to provide in their national law for the right of data subjects to receive compensation from the controller[7] for any damage suffered as a result of an unlawful processing operation or of any act incompatible with the national law implementing the Directive. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

- Article 24, Sanctions, establishes the obligations of Member States to adopt suitable measures to ensure the full implementation of the provisions of the Directive and in particular to lay down sanctions to be imposed in case of infringement.

The comparison of these provisions with Article 10 of the Convention shows the following:

- Despite the differences in extension and level of detail, a number of elements are common. Both texts address the issues of remedies and sanctions.

- The Directive leaves quite some freedom to the Member States as to the nature of the sanctions, as does the Convention, but is much more specific as to the type of remedies that should be available to data subjects: in any case judicial remedies, in addition to any prior administrative remedy that might exist.

- Article 24 of the Directive places the issue of sanctions in the framework of the measures taken by the Member States to guarantee full implementation of the Directive. The explanatory memorandum of the Convention refers to the notion of effective protection of the data subjects.

- The whole question of the liability of the controller, dealt with in Article 23 of the Directive, is absent from the Convention. This is not strange however, as the controller, although defined in its article 2, letter d, does not play a very important role in the context of the Convention. The text of the Convention focuses on the rights of the data subjects far more than on the other side of the coin: the obligations of the controller.

Article 28 of the Directive pays attention to an issue not dealt with in the Convention: the role of the data protection authorities, referred to in this text as supervisory authorities. It is a very long article that refers to several aspects of the nature and activities of these authorities.

[7] Article 2.d, of the Directive defines the controller as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

In the first place, it establishes that the Member States should provide for one or more authorities responsible for monitoring the application within their territory of the national provisions implementing the Directive.

Subsequently, one extremely important point concerning the nature of the authorities is stated: the authorities shall act with complete independence in exercising the functions entrusted to them.

The core of the article contains a list of the powers and tasks entrusted to the supervisory authorities:

- They should be consulted when drawing up administrative measures or regulations relating to data protection.

- They should have investigative powers, effective powers of intervention and the power to engage in legal proceedings in case of violation of the provisions of the national data protection legislation or to bring these violations to the attention of the judicial authorities.

- They should hear claims lodged by any person or association representing this person concerning his/her rights with regard to the processing of personal data.

- They should draw up public reports of their activities at regular intervals.

Other specific matters related to the functioning of the authorities are defined as well, such as:

- The decisions of the authorities that give rise to complaint may be appealed against through the courts.

- Each authority is competent on its territory, without regard to the law applicable to the processing in question. It may be requested by an authority of another Member State to exercise its powers.

- Supervisory authorities shall cooperate with each other to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

- All members and staff of the authorities should be subject to a duty of professional secrecy even after their employment has ended.

Article 29 of the Directive sets up a Working Party on the Protection of Individuals with regard to the Processing of Personal Data in which all supervisory authorities of the European Union are represented. As we shall see in the second chapter of this report, this Working Party plays an important role in strengthening co-operation at European level. The tasks of this body are enumerated in Article 30 of the Directive.

The Additional Protocol to the Convention

An Additional Protocol to the Convention was adopted by the Committee of Ministers on 23 May 2001[8]. The main purpose of this Protocol is to improve the application of the principles contained in the Convention by adding two substantial new provisions, one on supervisory authorities and one supplementing Article 12 of the Convention on transborder data flows.

[8] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) regarding supervisory authorities and transborder data flows, ETS no. 179.

The explanatory report to the Protocol explains in its preamble[9] that the envisaged improvement of the application of the principles has become necessary because of the increase in exchanges of personal data across national borders between states which are Parties to the Convention and states or entities which are not.

Constant effort is needed to improve the effective protection of the rights guaranteed by the Convention[10]. Effective protection in turn requires international harmonisation not only of the basic principles of data protection but also, to a certain extent, of the means of implementing them in such a rapidly changing, highly technical field and of the conditions in which the transfers of personal data can be made across national borders.

The principles contained in Article 10 of the Convention, the need for adopting appropriate sanctions and remedies for the effective application of the principles of the Convention, are also emphasised in the Explanatory Report[11]. Most countries which have data protection laws have set up supervisory authorities, generally in the form of a commissioner, a commission, an ombudsman or an inspector general. These data protection supervisory authorities provide for an appropriate remedy if they have effective powers and enjoy genuine independence in the fulfilment of their duties. They have become an essential component of the data protection supervisory system in a democratic society.

The Additional Protocol contains only three articles. Article 1 of the Protocol, dealing with the issue of the supervisory authorities, reads as follows:

> Article 1: Supervisory authorities
>
> 1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.
>
> 2.a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.
>
> b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.
>
> 3. The supervisory authorities shall exercise their functions in complete independence.
>
> 4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.
>
> 5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Article 1 of the Additional Protocol is, although inspired to a great extent by it, intentionally less detailed than Article 28 of the Directive concerning the data protection authorities. This is because the Drafting Group of the Consultative Committee considered that, depending on the national legal system, the composition, powers and *modus operandi* of the data protection

[9] Paragraph 3 of the Explanatory Report to the Additional Protocol.

[10] Paragraph 4 of the Explanatory Report to the Additional Protocol.

[11] Paragraph 5 of the Explanatory Report to the Additional Protocol.

authorities might differ considerably from one country to another[12]. Parties should also have considerable discretion as to the powers which the data protection authorities should be given for carrying out their tasks[13].

The text of the Protocol makes it very clear however that supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions. These could include the composition of the authority, the method of appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority, the adoption of decisions without being subject to external orders or injunctions[14].

The role of the data protection authorities in Europe: differences and similarities

As mentioned in the previous section, the Drafting Group of the Consultative Committee considered that some differences exist in practice in the composition and way of operation of data protection authorities and that Parties should have some discretion in that respect.

In practice these differences clearly exist. The results of the annual questionnaire on data protection authorities presented in the Spring Data Commissioners Conference in Athens[15] last May illustrate this point regarding the European Union supervisory authorities:

- All European Member States have a data protection authority. The first one was established in 1973 in Sweden, the most recent in 1997 in Italy and Greece.

- As to the organisation, ten of the authorities operate with a collective model (a commission) and five with a one-person model (ombudsman).

- There are also differences with regard to the scope of responsibilities in the public and private sectors. Twelve authorities have the same responsibilities in both sectors. Austria and France deal with both sectors but with some differences in competences and powers. The German Federal DPA deals only with the public sector.

- The staff working for the authorities varies from 2 persons in Luxembourg to 130 in the United Kingdom. Six authorities had increased their staff in 2000 while the staff had decreased in four of them.

- The biggest group within the staff are legal professionals while the number of IT professionals is increasing in most countries.

- Thirteen DPAs maintain a register of notifications. Finland does not, and in Luxembourg the Ministry of Justice maintains the register.

- Thirteen authorities give decisions. In ten cases it is possible to appeal against these decisions.

- The number of advisory services given to data subjects in 2000 varies from 800 in Austria to more than 37,000 in the United Kingdom. For data controllers it goes from 400 in Austria to more than 36,000 in the United Kingdom.

[12] Paragraph 9 of the Explanatory Report to the Additional Protocol.

[13] Paragraph 11 of the Explanatory Report to the Additional Protocol.

[14] Paragraph 17 of the Explanatory Report to the Additional Protocol.

[15] Revised summary of the results of the questionnaire referring to the year 2000, Spring Conference of European Data Protection Commissioners, Athens, 10-11 May 2001.

- Eight authorities have contacts with the press on a daily basis, five of them every week and two of them once a month.

- Eleven authorities have approved codes of conduct after the entry into force of the Directive.

- Thirteen authorities undertake data protection audits.

A number of important similarities also deserve mention:

- They all deal with complaints from the general public.

- They all give advice to data subjects and controllers.

- All the European data protection authorities have experience with international cooperation. In addition to the formal meetings, the amount of informal contacts is increasing.

- All DPAs are presently devoting a great deal of attention to informing the general public about the new legislation concerning data protection. They all have their own websites.

- All European Union authorities regularly publish a newsletter or other publications such as an annual report of activities.

- They all participate in the Article 29 Working Party for the Protection of Individuals with regard to the processing of personal data.

Conclusion: Would it be necessary or desirable to amend the rules of the Convention concerning implementation mechanisms?

After examination of Article 10 of the Convention and Article 1 of the Additional Protocol, consideration could be given, in the light of the 20th anniversary of the Convention, to whether it would be necessary or desirable to amend the rules of the Convention concerning this issue.

One of the considerations that could offer valuable elements of reflection is whether countries that have ratified the Convention could be considered to offer "adequate protection" in the sense of Article 25 of the Directive[16]. Such a positive adequate finding has very important consequences for a given country as it facilitates the free flow of personal data from the European Union to that third country.

The Article 29 Working Party dealt with the notion of adequate protection in a document of 24 July 1998[17]. Practice has shown that all Community decisions taken in this field up to now have used the criteria defined in this document as the basis for the analysis of the situation in a given country.

The Working Party's document develops a functional approach to this matter basing its conclusions not on the nature of the existing rules but on the practical results achieved in a country. It departs from the fact that data protection rules only contribute to the protection of individuals if they are followed in practice. Therefore, any meaningful analysis of adequate

[16] Article 25.1 of the Directive reads as follows: The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

[17] Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. WP 12. A summary of this document is contained in the letter of the Minister of Justice to the Second Chamber of 9 March 2000; Tweede Kamer, vergaderjaar 1999-2000, 27 043, nr. 1.

protection must comprise two basic elements: the content of the rules applicable and the means for ensuring their effective application.

As far as this report is concerned, our analysis should be focused on the three criteria listed in order to assess the effectiveness of the data protection substantive rules:

- *Good level of compliance with the rules*: Some elements such as the level of awareness of controllers and data subjects and the existence of effective and dissuasive sanctions play an important role in order to deliver a good level of compliance with the rules.

- *Support and help to individual data subjects*: An individual should be able to enforce his/her rights rapidly and effectively and without prohibitive cost. To do so there should be some sort of institutional mechanism allowing independent investigation of complaints. Within the European Union this role is played by the independent supervisory authorities but other systems are also admissible in a third country as far as the support and help to the data subjects is guaranteed.

- *Appropriate redress to the injured parties*: appropriate systems should be in place to provide redress to the injured party where rules are not complied with. This is an essential element that must involve a system of independent adjudication or arbitration that allows compensation to be paid and sanctions imposed where appropriate.

The Article 29 Working Party's document devoted its chapter two to the application of the approach explained to countries that have ratified Convention 108. As far as the procedural mechanisms in place to ensure that the basic principles are rendered effective are concerned, the paper emphasises the fact that the Convention requires its principles to be embodied in domestic law and that appropriate sanctions and remedies for violations of these principles be established. This should be sufficient to ensure a reasonable level of compliance with the rules and appropriate redress to data subjects where the rules are not complied with (objectives 1 and 2 of the data protection compliance system).

However, the Convention does not oblige contracting parties to establish institutional mechanisms allowing the independent investigation of complaints, although in general ratifying countries have done so. This is a weakness, as without such institutional mechanisms appropriate support and help to the individual data subjects in the exercise of their rights (objective 2) may not be guaranteed.

As both Switzerland and Hungary had, before the approval of the Additional Protocol, already put in place independent supervisory authorities, this weakness of the Convention did not play a negative role in the examination of their national legislation at European level.

Positive decisions concerning their level of opinion were adopted in 2000 and bear the date of 26 July 2000[18].
The Additional Protocol of May 2001 has in the meantime addressed the weakness found in the Convention as to the lack of provisions on independent data protection supervisory authorities. Countries having ratified the Convention and the Protocol and implemented these provisions in an appropriate way will therefore in principle be considered as having adequate protection.

Furthermore, if Article 1 of the Additional Protocol is correctly put in practice at national level, the data protection authorities of these countries will comply with the requirements for accreditation agreed at the 23rd International Conference of Data Protection Commissioners in Paris in September 2001 and they will therefore be allowed to participate in such international conferences in the future[19].

[18] Official Journal of the European Communities, L 215, Volume 43, 25 August 2000.

[19] Accreditation procedure for data protection authorities, approved during the closed session of the 23rd International Conference of Data Protection Commissioners in Paris, 25 September 2001.

The accreditation principles agreed by the DPAs during the closed session at the Paris conference can be summarised as follows:

1. Legal basis: The data protection authority must be a public body established on an appropriate legal basis.

2. Autonomy and independence: The data protection authority must be guaranteed an appropriate degree of autonomy and independence to perform its functions.

3. Consistency with international instruments: The law under which the authority operates must be compatible with the principal international instruments dealing with data protection and privacy, such as the OECD Guidelines, Convention 108, the European Directive and so forth.

4. Appropriate functions: The authority must have an appropriate range of functions with the legal powers necessary to perform those functions.

Article 10 of the Convention might at first sight seem very short and too general. Nevertheless, if correctly put in practice at national level and in combination with the provisions of the Additional Protocol to the Convention, it seems to offer sufficient guarantees of effective protection to the data subjects. In our view, an amendment of these provisions is, for the time, being not necessary.

2. INTERNATIONAL CO-OPERATION MECHANISMS FOR PROTECTING PERSONAL DATA IN A GLOBALISED INFORMATION WORLD

Introduction

In the present globalised information world the needs for international co-operation in the field of data protection have become greater than ever. Personal data are often transferred from one country to another using the electronic highways or international databases frequently put in place by multinationals operating worldwide.
Moreover, as most of the European countries have included provisions in their legislation similar to Article 4 of the European Directive[20], situations can arise where the processing operations taking place in one country in fact fall under the scope of application of the legislation of another country.

In all these situations co-operation between the authorities, and often the data protection authorities of the countries involved, is of vital importance for effective data protection.

---

[20] Article 4 of the European Directive reads as follows: National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

The obligations in the Convention

Chapter IV of the Convention deals with the issue of mutual assistance between the Parties to the Convention[21] and the assistance to data subjects resident abroad (Articles 13 to 17).

Article 13 establishes the general principle that Parties agree to render each other mutual assistance in order to implement the Convention. For that purpose, each Party should designate one or more authorities, in practice often the data protection authorities of the country in question.

The designated authorities should at each other's request furnish information on their law and administrative practice in the field of data protection and should where necessary take all appropriate measures for furnishing factual information relating to specific automatic processing operations carried out on its territory.

As explained in the explanatory memorandum to the Convention[22], the authorities will render each other general assistance for controls *a priori* as well as specific assistance for controls *a posteriori*. The information might be of a legal or factual character.

The exchanges of legal information have in the meantime become less important as this kind of information is often available on-line through the websites of the data protection authority/ies of the country in question.

Article 14 pays attention to the cases where a data subject residing abroad requests assistance. In these situations the main principle is that each Party shall assist any person residing abroad to exercise his data protection rights. This is a direct consequence of Article 1 of the Convention securing protection to "every individual, whatever his nationality or residence…".[23]. The data subject has the option of submitting his request through the intermediary of the authority designated in the territory of the country where he resides.

Article 15 regulates specific details related to the assistance requests such as the fact that the authorities may only use the information for the purposes specified in the request for assistance and that those acting on behalf of the authorities shall be bound by professional secrecy rules. This provision is of fundamental importance for mutual trust, on which mutual assistance is based.

Article 16 deals with the limited situations in which a designated authority may refuse to comply with a request for assistance: only if the request is incompatible with its powers, does not comply with the provisions of the Convention or would be incompatible with the sovereignty, security or public order of the Party or with the rights and fundamental freedoms of persons under the jurisdiction of that Party. The grounds for refusal to comply are enumerated exhaustively and correspond generally with those provided for by other international treaties in the field of mutual assistance[24].

Article 17 spells out the details concerning the costs and procedures for assistance. The provisions of this Article are similar to those found in other international conventions on mutual assistance[25].

---

[21] See also chapter 5 of the paper of Jean-Philippe WALTER, *La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, published in A. Epiney/M. Freiermuth (edit.), *La protection des données en Suisse et en Europe*, Fribourg 1999, p.83ss.

[22] Paragraph 71 of the Explanatory Report to the Convention.

[23] Paragraph 77 of the Explanatory Report to the Convention.

[24] Paragraph 80 of the Explanatory Report to the Convention.

[25] Paragraph 82 of the Explanatory Report to the Convention.

In addition to Chapter IV, Chapter V of the Convention also contains clauses of relevance to international co-operation. Articles 18 to 20 regulate the role, composition and functions of the Consultative Committee.

This Consultative Committee is composed of representatives of the Parties to the Convention and its functions are defined in quite general terms by the Convention, including the right to make proposals with a view to facilitating or improving application of the Convention or for amendment of the Convention, to formulate its opinion on any proposal for amendment and, at the request of a Party, to express an opinion on any question concerning application of the Convention.

The text of the European Directive

The European Directive also contains provisions dealing with international co-operation, in particular, between the data protection authorities of the countries of the European Union.

Article 28.6 of the Directive reads as follows:

> Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
>
> The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

This article has in practice regularly been used as the legal basis for a request for assistance between DPAs of several Member States in specific cases. The Directive departs from the fact that national Data Protection Authorities should assist one another in performing their duties in order to ensure that the rules of protection are properly respected throughout the European Union[26].

The Directive created in its Article 29 a new body called the *Working Party on the Protection of Individuals with regard to the Processing of Personal Data*[27]. The second paragraph of Article 29 specifies that the Working Party will be composed of a representative of the supervisory authority or authorities designated by each Member State, a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

One of the important features of the Article 29 Working Party is the fact that it is completely independent in the performance of its functions. Article 30 of the Directive enumerates the tasks entrusted to the Working Party:

- examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;
- give the Commission an opinion on the level of protection in the Community and in third countries;
- advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

[26] See the preamble to the Directive, recital number 64.

[27] See for more information the article by ALONSO BLAS, D., *Towards a uniform application of the European Data Protection Rules: The role of the Article 29 Working Party* in Privacy & Informatie, 4e jaargang, nummer 1, February 2001.

- give an opinion on codes of conduct drawn up at Community level.

The Working Party may also, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

The Working Party has issued during recent years a good number of documents of great significance for the interpretation and uniform application of the European data protection rules. All public documents approved by the Working Party are available on the website of the European Commission in all official languages of the European Union[28].

The Additional Protocol

Article 1.5 of the Additional Protocol reinforces the co-operation obligations between Parties foreseen in Chapter IV of the Convention by including specific obligations for the data protection authorities of the countries. It reads as follows:

> In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Strengthening co-operation between the supervisory authorities must contribute to the development of the level of protection in the Parties' practice under the Convention. This co-operation is in addition to the mutual assistance provided for in Chapter IV of the Convention and the work of the Consultative Committee. Its purpose is to provide improved protection to the people concerned. With increasing frequency people are directly affected by data processing operations which are not confined to one country and therefore involve the laws and authorities of more than one country. The development of international electronic networks and increasing cross-border flows in the service industries and the work environment are examples. In such a context international co-operation between supervisory authorities ensures that people are able to exercise their rights on an international as well as a national level[29].

Practical co-operation

In practice, two forms of international co-operation for data protection authorities can be distinguished: formal and informal.

In addition to participation in the Consultative Committee of the Convention (T-PD) and the Project Group on Data Protection (CJ-PD), which are well known to the participants in the conference, other fora can be mentioned as means of formal co-operation:

- Participation in the Article 29 Working Party: Up to now participation in this group has been limited to those mentioned in Article 29 of the Directive, data protection authorities of the European Union or the European Economic Area. Discussion is, however, at present going on within the group with a view to allowing accession countries to be observers to the Working Party. This would allow a number of the Council of Europe countries to participate and benefit from these discussions.

- Participation in the European Data Commissioners Conference: This Conference was originally limited to the European Union DPAs but in recent years other DPAs have been invited to participate. In the first place, Switzerland and Hungary, as countries with a positive adequacy finding. In 2001 the authorities of Poland and the

[28] All documents approved by the Working Party are available on the website of the European Commission: http://www.europa.eu.int/comm/privacy

[29] Paragraph 20 of the Explanatory Report to the Additional Protocol to the Convention.

Czech Republic have also participated, so there is good reason to assume that other well-functioning DPAs from countries having ratified or about to ratify the Convention will in the future be able to participate.

- Participation in the International Data Commissioners Conference: As already mentioned, the International Conference has recently approved the criteria for accreditation of DPAs willing to participate in the conference. As these criteria are similar to those included in the Additional Protocol to the Convention, one can assume that Council of Europe countries which have ratified the Convention and the Protocol and which have introduced their provisions properly in their national legislation will face no problems here.

Under informal co-operation one can mention:

- In the first place, bilateral contacts of various kinds, such as informal consultation in specific cases, organisations of work-visits and seminars or co-operation in common projects with international aspects. This kind of co-operation already exists between countries of the Council of Europe but can still be improved, where possible using available funds from the Council of Europe or the European Union.

- Two years ago an initiative was started by the United Kingdom and Dutch DPAs in order to create a new informal forum for informal and frequent co-operation between staff of the DPAs. This idea was launched at the European Data Commissioners Conference and was approved by the Conference. Since then three "complaints workshops" have been organised and, from March 2001 on, a closed website for quick and easy confidential exchange of information between the participants in the workshop has been functioning. This website has proved to be a very efficient and rapid means of communication concerning international cases in which several DPAs may be involved at the same time. Up to now participation in the complaints workshops and the CIRCA website has been limited to DPAs of the European Union, European Economic Area or from other European countries with a positive adequacy finding. The intention of the author of this report is to open discussion on this issue at the next workshop in Lisbon at the beginning of November in order to discuss whether other European countries that have ratified the Convention could also participate, even before a decision on adequacy has been taken. It might be possible to report about the conclusions of this discussion during the presentation of this report in Poland.

Conclusions

The provisions of the Convention regarding mutual assistance and co-operation have been substantially improved and completed with the approval of the Additional Protocol. Ratification of this Protocol and its correct implementation under national law will, in combination with ratification and correct implementation of the Convention, pave the way for Council of Europe countries who so wish to play a more important role in the international data protection field.

It will put them in a good position for acquiring the status of countries with a positive adequacy finding and, will at the same time, facilitate their participation in several formal and informal international fora. This can bring with it a new era of reinforced international co-operation and mutual assistance in the data protection field that can allow DPAs to address correctly in a coordinated way the big challenges of our open and globalised information society.

MECHANISMS FOR IMPLEMENTATION AND INTERNATIONAL CO-OPERATION IN THE CONTEXT OF DATA PROTECTION: EXISTING MECHANISMS AND MECHANISMS TO BE ESTABLISHED

SUMMARY

This report deals with the regulation of the issues of mechanisms for implementation and international co-operation in the context of data protection in Convention 108 (1980) and in the Additional Protocol to the Convention (2001). The provisions of both instruments are analysed and, where useful, measured up against the provisions of an instrument fifteen years younger than the Convention, the European Directive of 1995.

One of the main conclusions of this report is that the Additional Protocol has substantially improved and completed the provisions included in the Convention; it is therefore extremely important that countries ratify not only the Convention but also, and preferably at the same time, the Additional Protocol.

Concerning the *first part of the report*, dealing with mechanisms of implementation of the principles of the Convention, it can be concluded that the Additional Protocol has addressed the main weakness found in the Convention in this respect, the lack of provisions on independent data protection supervisory authorities. Countries having ratified the Convention and the Protocol and implemented these provisions in an appropriate way will therefore in principle be considered as having adequate protection in the sense of the European Directive.

Furthermore, if Article 1 of the Additional Protocol is correctly put in practice at national level, the data protection authorities of these countries will comply with the requirements for accreditation agreed at the 23rd International Conference of Data Protection Commissioners in Paris in September 2001 and they will therefore be allowed to participate in such international conferences in the future.

Article 10 of the Convention might at first sight seem very short and too general. Nevertheless, if correctly put in practice at national level and in combination with the provisions of the Additional Protocol to the Convention, it seems to offer sufficient guarantees of effective protection to the data subjects. In our view, an amendment of these provisions is for the time being not necessary.

Concerning the *second part of the report*, dealing with the provisions of the Convention and the Additional Protocol regarding mutual assistance and co-operation, it can be concluded that ratification of this Protocol and its correct implementation under national law will, in combination with ratification and correct implementation of the Convention, pave the way for Council of Europe countries who so wish to play a more important role in the international data protection field.

It will place them in a good position for acquiring the status of countries with a positive adequacy finding and will at the same time facilitate their participation in several formal and informal international fora. This can bring with it a new era of reinforced international co-operation and mutual assistance that can allow DPAs to address correctly in a coordinated way the big challenges of our open and globalised information society.

REPORT

THE PLACE OF THE INDIVIDUAL IN A WORLD OF GLOBALISED INFORMATION: RIGHTS AND OBLIGATIONS

Report by

Ms Nathalie MALLET-POUJOL
Head of Research at the CNRS
ERCIM-UMR 5855
University of Montpellier I
France

TABLE OF CONTENTS

II – THE CONSENTING INDIVIDUAL

A. The ability to object

1. Nature of the objection

1.1 Partial objection

1.2 Complete objection

2. Grounds for objection

2.1 Assessment of the grounds

2.2 Intrinsic validity of the objection

3. Forms that the objection takes

3.1 Off the Internet

3.2 On the Internet

B. Explicit consent

1. Cases in which explicit consent should be obtained

1.1 Consent and sensitive data

1.2 Consent and sensitive processing

2. Means of obtaining explicit consent

2.1 Off the Internet

2.2 On the Internet

3. Limits of consent

3.1 Consent and public policy (*ordre public*)

3.2 Consent and contractual practices

CONCLUSIONS

INTRODUCTION

1. The globalisation of the economy has brought an increase in the circulation of personal data for the purposes of commercial exchanges and international co-operation. This nomadism of data is to be seen on all communication systems and networks. However, we must remember that the expression "world of globalised information" brings to mind principally the symbolic network manifested by the Internet. The concept of the "global village" evidenced by the plan for a "planetary information society" has nurtured thoughts of an "information revolution" of a kind that will bring people together and lead to the building up of a "collective intelligence" in the interests of free circulation of knowledge and ideas. But it has at the same time rekindled the fears of an encroachment on privacy and freedoms that were aroused in the 1970s by new information technology and telecommunications. The questions are not new ones, but they have changed markedly in scale. The danger to liberty lies in the extent to which this means of communication makes information available worldwide.

2. A means of scrutinising individuals is now available which knows no barriers. The Internet is becoming the common system for international data exchange, whether specific (the transfer of data files) or potential (the interrogation of external web sites). This electronic device is all the more formidable in that the computer memory is generally concealed and able to function without the knowledge of the data subject. The Internet, a gigantic database nurtured by the

suppliers of its contents, is in fact being transformed into an instrument for the collection of data concerning the Internet user, giving rise both to visible "traces" (data delivered to the site operators), and at the same time invisible ones (linked data, Internet protocol and DNS addresses, cookies, etc.). And within this vast data reservoir, the search engines make it possible to ascertain a person's profile within a few minutes, by means of a simple keyword search based on data disseminated on the Web. The obvious threats of such practices being misused makes it all the more essential to protect privacy and freedoms.

3. Certainly, international and national legislation on personal data protection in the widest sense has lost none of its relevance. It "ages" rather well. It did not take the arrival of the Internet for the issue of trans-border data flows to be addressed. The principles of purpose and proportionality, loyalty and transparency and of mutual protection have lost none of their acuteness. Not being restricted to any particular technology, such principles have stood the test of their adaptability to fresh problems, despite the need to make adjustments here and there to the specifics of the Internet. More and more steps are being taken to tighten up the rules governing protection. But, it might well be asked, either somewhat naively or with too penetrating an insight, where does the individual feature in such provisions? Can he really assert his rights or even his point of view? And, if so, how? Do the legal instruments available to him still work? Does the globalisation of data exchange in fact make the assertion of his prerogatives somewhat illusory?

4. I propose to concentrate in this study on the remedies that are available to the individual whose personal data are collected, processed and disseminated. The emphasis will be on the means whereby he may, moreover, control the use of data relating to him without having to take his case to a supervisory authority or to embark upon the ramifications of possibly long, costly and risky legal proceedings within a context of international law. What is required is something firmly preventive and pragmatic and by choice limited to the main prerogative of the data subject. This will of necessity be something that has been simplified, as an "isolated" or "lone" individual is under consideration, with no help from a data protection authority, an authority whose pressing necessity is, of course obvious. What is required is also something on a modest scale, as it is often linked to defence of "everyday" freedoms, such as those of the cyber consumer or the net surfer, a matter sometimes more of the right to peace or the right not to be used as a guinea pig for marketing purposes. This is a strictly legal study aimed at the discovering the way in which these questions are put, having regard to the European data protection legislation and in the light of French experience.

5. With legal data protection legislation, the prerogatives of the data subject essentially pertain to, on the one hand, the right to information (and, where appropriate, consent, its corollary) and on the other hand, the right of access and rectification, as set out in Article 8 of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter referred to as Convention 108), under the heading "additional safeguards for the data subject". We should, then, evaluate the practical implementation in a world of globalised information by examining in turn how the individual can hope realistically to be informed that processing is taking place (I) and to be able, in certain cases, to have the option of giving or withholding his consent (II).

I. THE INFORMED INDIVIDUAL

6. The issue of informing the individual should be considered over and above the automatic processing itself in terms of making individuals aware of the extent of "Information Technology and Freedoms" by means of public education. There has never been much awareness of the risks associated with computerisation. This is even more the case with the Internet. The younger generations are growing up with this prodigious means of communication, in a world often perceived as solely virtual and recreational, without necessarily being aware of the potential dangers associated with the visible or invisible traces which it generates. There is a need for data protection authorities to increase the means of communication on the subject both

in the educational sector and in business and the town[1] generally, with the assistance of the professional organisations involved. It is vital to equip them with conceptual instruments such as, for example, the annex to Recommendation No. R (99) 5 of the Committee of Ministers to Member States on the protection of privacy on the Internet entitled "Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways which may be incorporated in or annexed to codes of conduct".

7. Further consideration should also be given to the conditions for informing the data subject. Article 8.a of Convention 108 clearly states that "any person shall be enabled to establish the existence of a personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file". In the absence of any legal derogation to the requirement to inform[2], the effectiveness of the information conditions the implementation of other personal prerogatives, such as the right of objection, access or rectification. Information as to the existence of such rights should be supplied at the same time as information concerning the existence of the data file.

8. The right to prior notification, as a guarantee of the transparency of automatic data files, is one of the pillars of the legal systems for personal protection, but its provisions must be carefully thought out and adapted in relation to the very diverse methods of data collection and processing. The circumstances in which this right to information must be made available are not always clearly anticipated and often result in a neutralisation of this right, particularly where automatic data files are transferred. A way must be found to remedy this. A distinction must be drawn between two possible situations, according to whether the collection is primary (A), that is to say, undertaken directly or indirectly in association with the data subject, or secondary (B), that is to say undertaken on the basis of a previously constituted data file, before any mention of the right of access and rectification (C).

A. Right to information and primary collection

9. Primary collection for the purposes of setting up a file can be undertaken through direct contact with the data subject by means of an interview or a written questionnaire. It can also be undertaken "automatically", in the so-called indirect way, by means of smart cards, telephone charge cards, swipe cards, biometric processes or after connection to automatic systems. The Internet world generates, for example, a proliferation of methods of data collection without the knowledge of the data subject (by means of cookies, electronic addresses, etc.). The setting up of all those systems requires, in the same way as for a direct collection, information regarding the data subject, information in relation to which the nature (1) and the methods (2) will be specified.

1. Nature of the information

10. Information is typically directed, apart from the existence of rights of access and of rectification[3], to the purpose of the processing (1.1), but it might well be wondered whether in relation to some types of processing more specific information should be given as to their inherent risks (1.2).

---

[1] See, for example, the CNIL publication: Vos traces sur Internet – Découvrez comment vous êtes pistés sur Internet www.cnil.fr

[2] For exceptions to the right to information, see Article 9 of Convention 108, which provides for a possible derogation when it "constitutes a necessary measure in a democratic society in the interests of: a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences (…)"; see too Articles 11(2) or 9 of Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJCE no. L281/31 of 23 November 1995

[3] infra no. 36

1.1 Information on the purpose of the processing

11. The information supplied by the controller of the file on the nature of the automatic processing relates to the purpose of the processing (a) and the details of controller of the file (b). It is also essential to specify whether the replies asked for are obligatory or voluntary (c) and to whom they are to be communicated (d), not to mention, of course, the reference to the right of access and rectification[4].

a) Purpose of the processing

12. It is impossible to overstate the importance of the explanations given in relation to the purpose of the processing. The principle of purpose is one of the cornerstones of the personal data protection legislation. It presupposes, as set out in Article 5(b) and 5(c) of Convention 108 that the data have been, on the one hand, "stored for specified and legitimate purposes and not used in a way incompatible with those purposes" and that they are, on the other hand, "adequate, relevant and not excessive in relation to the purposes for which they are stored".

13. This principle requires, moreover, at the time of deciding on the automatic processing, very careful thought as to the nature of the data collected and processed and, above all, the relevance of doing it, bearing in mind the inherent risks. In an "ideal" world, the perfect grasp of the principle of purpose by those undertaking the processing should have a correspondingly diminishing effect on the reluctance and objections of the data subjects in relation to the information sought.

14. But this should not prevent, where the need arises, a challenging of the legitimacy or the appropriateness of the intended processing. One thinks, for example, of processing operations where the plan was abandoned because it did not contain sufficient safeguards for the data subjects[5]. One thinks too of the new concerns aroused by the Internet, the trans-border dimension of the data carrier rendering it no longer possible to think in the same way in relation to data made available on local, more secure, networks. In any event, the information provided to the data subject on the purpose of the processing enables him to exercise his essential control, and indeed, his right of objection. For objection to be made it must be extremely precise and specify in particular the nature of the data collected, the characteristics of the processing, the length of storage of the data and all forms of communication of the data.

b) Details of the controller of the file

15. Over and above the information on the purposes of the processing, the nature of the data stored and the uses to which they are applied, the data subject must be enabled, in order to assert his rights, to know "the identity and habitual residence or principal place of business of the controller of the file" as laid down in Article 8.a of Convention 108.

16. Article 5 of the Directive[6] on electronic commerce of 8 June 2000 contains a typical list of the type of information that might be given, such as "(a) the name of the service provider; (b) the geographical address at which the service provider is established; (c) the details of the service provider, including his electronic mailing address, which allows him to be contacted rapidly and communicated with in a direct and effective manner; (d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number or means of identification in that register; (e) where the activity is subject to an authorisation scheme, the particulars of that relevant supervisory authority(…)".

---

[4] infra no. 36

[5] See Decision of the CNIL of 10 September 1996 concerning motorway cameras: CNIL, 17º rapport d'activité 1996. Doc.fr. 1997, p. 102

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJCE no. L 178/01 of 17 July 2000.

This instrument shows a real concern to make such information operative in anticipation of any possible legal action.

17. It might be suggested, as has been done in France by the National Commission for Information Science and Liberties – CNIL, that the business name and registered office of the site be shown "on the home page or under a heading that is accessible from the home page (for example, under the title "Who are we?"[7])". In the same way, the Commission recommends Internet site holders to ensure that visitors to the site are "on reaching the home page (…) clearly informed of the name of the body in charge of the site, its electronic and physical address, together with the name, postal address and e-mail address of the service (or the person) enabling the right of access[8]".

c) Obligatory or voluntary nature of replies

18. Information on the purposes of the processing has as its natural corollary of whether it is obligatory or voluntary to supply the data being collected. This obligation is in a number of cases included in national legislation and has been laid down by Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as Directive 95/46/EC), Article 10(c) of which provides that the processor must provide the person with full details as to "whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply".

19. This specification is all the more vital in that more and more pressure is being put on the individual (particularly in his capacity of consumer and/or Internet user) to provide intimate personal details in exchange for various offers (the supply of additional services, discounts, shopping vouchers, etc.), all being proposals intended to make him lose sight of the voluntary nature of his replies. In electronic trading it is, for example, recommended that every electronic data collection form should show whether replies are obligatory or voluntary by means of an asterisk[9].

d) Recipients of data

20. Proper information as to the purpose of the processing will include an indication of the intended recipients, that is to say the persons who alone will be entitled to have access to the data contained in the file. Those recipients are, moreover, generally designated by the controller of the file when taking the initial steps.

1.2 Information on the risks of processing

21. The idea of informing people of the risks inherent even in processing has increased in sensitivity as it involves the protection of the Internet user. The latter is not always aware of having imparted data, nor, *a fortiori,* of the sensitive nature of those data when, put together, they make it possible to build up his profile. Thus, in its Guidelines of 23 February 1999 cited above (Art. III.2) the Council of Europe makes the following recommendation: "Inform users of privacy risks presented by use of the Internet before they subscribe or start using services. Such risks may concern data integrity, confidentiality, the security of the network or other risks to privacy such as the hidden collection or recording of data.".

22. Similarly, the CNIL recommends that electronic commerce websites should make Internet users better informed of the use of cookies, their functioning and the uses to which they might be put[10]. All these initiatives are to be encouraged and such warnings could be accompanied

[7] Decision no. 2001/011 of 8 March 2001 adopting a recommendation on health sites for use by the public: JORF of 12 April 2001

[8] See the recommendations shown on the site of the CNIL: www.CNIL.fr

[9] CNIL, 20º rapport d'activité 1999, Doc.fr.2000, p.104

[10] CNIL, 20º rapport d'activité 1999, Doc. Fr. 2000, p. 105

with information on the technological means for reducing such risks, such as encryption, digital signing, anonymity (pre-paid access cards…) or possibly the use of pseudonyms.[11]

2. Means of information

23. The means of information will vary according to whether the data collection is direct (2.1) or indirect (2.2), collection taking place on Internet sites calling for special interpretations (2.3).

2.1 Direct collection

24. Direct collection of data from data subjects is clearly the most simple case. It is undertaken in the presence of the individual, through an interview or by correspondence, by means of a questionnaire. The obligation to inform beforehand is fulfilled either by the person collecting the data, or by the questionnaire, which should contain the items of information required by law. There should be monitoring of the interviews or questionnaires as to their quality and the clarity of their presentation. In this connection one could cite the instance of the CNIL Decision of 18 February 1997 in relation to "mega databases" concerning the consumption habits of households and recommending in particular "that the presentation of the questionnaires distributed should be wholly unambiguous as to the purpose of the data collection and, in particular, that the use of any term or reference of such a nature as to cause confusion in the minds of the public, such as the description "Institute" or the term "opinion poll", which might give an incorrect impression of a statistical or, indeed, official purpose, or which is intended to conceal the commercial reality of the operation, should be avoided[12]".

2.2 Indirect collection

25. Indirect data collection, undertaken without the knowledge of the data subject, by means of machines such as automated teller machines, implies a global information on the very implantation of the system in the company or organisation concerned. The information will usually be given through the display or "dissemination of an explanatory note before the operation[13]"of the machine.

2.3 Internet sites

26. On Internet sites collection can be both direct and indirect. Direct collection involves the transaction data submitted by the Internet user when he completes electronic forms. He states, for example, his name, forenames, date of birth, address, profession and all information relevant to the transaction or the service provision offered by the site. Indirect collection involves the "famous" invisible traces comprising the connecting data that are necessary for the completion of the transaction.

27. These two types of collection require the setting up of information processes on two levels. An initial information must be given on the data collection form, to call the attention of the Internet user to specific points, such as the voluntary or obligatory nature of the replies (by means of an asterisk, for example) or the right of objection (by means of clicking on a box on the electronic form). A further information must be included on the home page or in a heading that is accessible from that page[14], by reference to a specific page on the menu. That wording is to contain more general information on the nature of the processing, its purposes and its

[11] See Articles III.3 and III.4 of the Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways which may be incorporated in or annexed to codes of conduct" annexed to Recommendation No. R (99) 5 of the Committee of Ministers to member states for the protection of privacy on the Internet.

[12] Decision no. 97-012 of 18 February 1997 making a recommendation concerning behavioural databases on consumer habits of households made for purposes of direct marketing, JORF of 9 September 1997

[13] Article 8 of the CNIL Decision of 20 December 1994 on the simplified rule on telephone charge cards: CNIL, Les libertés et l'informatique, Vingt délibérations commentées, Doc. Fr. 1998, p. 123

[14] supra no. 17

risks, together with the details of those doing the automatic processing and the exercise of the right of access and rectification[15]. Information may also be given on the general provisions of data protection law.

28. In its Guidelines of 23 February 1999, the Council of Europe also addresses service providers (Art III.11): "You are responsible for proper use of data. On your introductory page highlight a clear statement about your privacy policy. This statement should be hyperlinked to a detailed explanation of your privacy practice. Before the user starts using services, when he or she visits your site, and whenever he or she asks, tell him or her who you are, what data you collect, process and store, in what way, for what purpose and for how long you keep them. (…)." Similarly the CNIL suggests that electronic commerce websites should "use a column that is accessible from the home page or the collection form, for the protection of personal data and privacy[16]".

B. Right to information and secondary collection

29. When data previously collected from data subjects are subsequently passed on to third parties, the question of informing the individual concerned becomes a more vexed one. It is however a situation that is being exponentially evolved as the result of the development of marketing techniques, such as "geomarketing", with yearbooks, or the behavioural segmentation, with client files. Admittedly where the creation of processing is subject to an officially published regulation the result will be a general information procedure. But it is also important to make information processes directly available to data subjects (1), apart from excluding, in the case of certain files, any possibility of transfer. (2). The term "transfer" is broadly interpreted and includes any form of sale, lease, dissemination or passing on of data, either for payment or free of charge.

1. Obligations associated with the transfer of files

30. The transfer of files will inevitably give rise to an obligation to provide the data subject with information. In this respect the obligations on the part of the transferor (1.1) and on the part of the transferee (1.2) are not always clearly established.

1.1 Obligations of the transferor

31. In order to enable the data subject to assert his rights, it would appear perfectly logical for the transferor to inform him of the transfer of his data to a third party, without derogation from the duty in law to inform[17]. This obligation is not clearly included in national legislation, despite the fact that it frequently imposes a duty to inform the supervisory authority of the transfer. It would appear to be more binding on the transferee than on the transferor. However, it might nevertheless be seen as arising from the need, on the part of the controller of the file, to inform the data subject of the recipients of such data and that it should be done each time the data subject has not been informed initially, at the time that the data were collected, of such a transfer. Article 11.1 of Directive 95/46/EC sets this out in a specific hypothetical situation: "Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it". But this obligation to provide information could be further extended to cover any transfer of data not initially known to the data subject, even if the data were directly collected from the data subject.

[15] infra no. 36

[16] CNIL, 20º rapport d'actvité 1999, Doc. Fr. 2000, p. 104

[17] supra nº 7

1.2 Obligations of the transferee

32. The transferee of data should be obliged as a matter of course to inform the data subject of the processing that is being effected on the basis of a previously assembled file. Such an obligation is, as we have seen, set out in Article 11(1) of Directive 95/46/EC and the obligation lies with the controller, where data have not been collected from the data subject "at the time of undertaking the recording of personal data" or when the controller, in his turn, is in a position of transferring the data. This is clearly a major step forward which should be maintained through rendering the relevant legislation more explicit, particularly as to the time when this obligation becomes binding, depending on the way in which the data were collected and whether or not a transfer was planned. But it must be emphasised that there are inherent dangers in the exceptions[18] to this obligation to inform, arising in particular from the difficulties of tracing a particular individual, and the assessment of the "disproportionality" of the effort involved is highly subjective.

2. Restrictions on the transfer of files

33. Inasmuch as it is not always easy for the individual, for psychological or practical reasons, to refuse certain uses of his data, consideration should be given to the possibility of legal restrictions on the transfer of certain files. Such measures would respond to the need to introduce public policy (*ordre public*) provisions for the protection of the individual (including protection against himself). It would be impossible to circumvent such provisions, even with the consent of the data subject. The way in which this could be achieved could range from merely restricting transfers (1.1) to prohibiting them (1.2).

2.1 Restricted transfers

34. It is vital to make provision for restrictions on the transfer of data, where the transfer of data would only be permitted for certain categories of data or for certain recipients. An example of this is the controversy engendered in France by the government Bill on data companies concerning the transfer of connection data. Article 14 III of the Bill provides that they can only be transferred to "third parties directly involved in billing or debt enforcement. ".

2.2 Prohibited transfers

35. Similarly, it would be beneficial to consider cases where the transfer could be prohibited outright. The prohibition could be imposed on account of the particularly sensitive nature of data, such as health data[19] or by the lack of adequate standards of protection where the transfer is to a third country.

C. Right of access and rectification

36. Under the provisions of Article 8.b of Convention 108, any person shall be enabled "to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the data file as well as communication to him of such data in an intelligible form". He must furthermore, under the provisions of Article 8.c, be enabled to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention". There are, however, exceptions to this right, as specified in Article 9 of the Convention.

37. The right of access is one of the aspects of the right to information of the data subject. It enables him to ascertain the accuracy of the information held by the controller of the file, and, as

[18] See Article 11.2 of Directive 95/46/EC cited above.

[19] See Decision no. 2001/011 of 8 March 2001, cited above, which expresses the desirability of "the principle of the direct or indirect commercialisation of registered health data being prohibited by law(…)".

the case may be, require rectification. It provides a control process, monitored by the individual himself, and is a token of his potential involvement in the implementation of data protection provisions.

38. However, in relation to the majority of automatic processing, this personal prerogative is very seldom used, a worrying sign of a degree of resignation or of an excessive level of pessimism or discouragement as to the efficiency and benefits of the right of rectification. In a world of globalised information, the right of access will remain a dead letter if it is not possible to guarantee the "tracking" of automatic processing by the individual (1). Paradoxically, the Internet world can enable this (2).

1. The tracking of automatic processing

39. For the right of access to be implemented, it must be possible to trace the transfer of data to third countries. It is thus dependent on the successful implementation of approved information procedures in the case of data transfer[20]. It would, however, not be taking things too far to reinforce such an information procedure by other means of establishing the existence of files. The tracking would happen naturally as the result of the individual noting its effects. This is the classic case of mailing lists where it is sometimes possible to trace the original where a misprint has occurred in copying the name and address!

40. On the Internet, the power of the research engines is an illustration of the possibility of tracing files. Which of us has not shuddered on discovering, using one's surname as a keyword in a research tool, the number of times it occurs on the Internet? Which of us has then not cursed at the site providers for the lack of information? The display of the Internet address of the listed site enables one, however, as an odd kind of compensation, to express one's strong objection, and indeed, to facilitate one's right of rectification!

41. It would, of course, be less haphazard for there to be a processing register. But there one runs into the great debate on the minimal requirements for the creation of files by a supervisory authority in order to enable the carrying out of the control[21], leaving aside the question of the feasibility of such a register at international level….

2. Procedure for the right of access

42. The right of access is typically exercised by writing to the person or service whose details must be shown by the controller of the file when he informs the data subjects. On the Internet, this right can facilitated by arranging for its on-line application by e-mail addressed to the webmaster.

43. For electronic commerce websites, it is recommended that a "column should be set up, accessible from the home page or the collection form, for the protection of personal data and privacy, in which the existence and the location of the right of access could be specified[22]". In such a case, e-mail correspondence should be encouraged.

II. THE CONSENTING INDIVIDUAL

44. The question of the consent of the data subject[23] to the use of his data is a very sensitive issue in data protection legislation. Protection is not necessarily bound up with consent, in that some processing is either obligatory or simply essential for smooth operation. In such a case it

[20] Supra no. 29

[21] See the discussions on the exceptions to the obligation to notify the supervisory authority, as set out in Article 18 of Directive 95/46/EC

[22] CNIL, 20º rapport d'activité 1999, op.cit. p.104

[23] See the current discussion on the consent of minors and the Internet.

is inconceivable, or barely conceivable, for its existence to be subject to the agreement of the individual. One thinks, for example, of public sector files that are set up on public interest grounds on the basis of legal or statutory provisions, or a file relating to the active management of a business (such as a computerised payroll) and in which it is hard to see where any concession could be made.

45. In this regard Convention 108 does not make any explicit mention of seeking the consent of the person whose data are undergoing automatic processing. There is an oblique reference to it in Article 6, which relates to "Special categories of data".

46. However, when considering the reinforcement of personal rights in a world of globalised information, the matter of personal consent comes immediately to mind as the most significant aspect of the control that the individual would have over the use of his data and of his power of self-determination. It might well be, for example, that consideration should be given to furthering the generalisation of personal consent as a last resort measure of protection in the face of an internationalisation of data exchange.

47. Moreover, the indication of consent cannot be modulated by means of stakes, whereby one can choose to opt out or opt in. The response cannot be categorical, but should be adapted to the nature of the data that are being processed on the Internet. The risks of encroachment on privacy and freedoms are evidently not the same in the case of marketing data as in that of medical data. Hence the ability to withhold consent[24] (A), frequently introduced by national systems, to require explicit consent for processing in some cases (B).

A. The ability to object

48. The ability to object marks a major "victory" for data protection. This was clearly not something to be "tolerated", as it put the individual in a position to change the optimisation of automatic processing intended by the promoter of a computer application. Of all the possible ways in which the data subject could express his wishes, it nevertheless remains the least restrictive procedure for the controller of the file. The mechanism does not suffer from the same restraints as the seeking of consent, as it enables the controller of the file to avoid waiting for a positive reply.

49. While Convention 108 does not make explicit reference to the right to object, the ability to object is, on the other hand, mentioned in Article 14 (a) of Directive 95/46/EC, which provides that: "Member subjects shall grant the data subject the right: at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data; b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses (…)".

50. This right will vary enormously according to the interpretation of the Directive within each Member State in view of the extreme sensitivity of the subject matter. It would therefore be as well to spend some time considering the nature of the objection (1), its grounds (2) and the forms that it takes (3).

1. Nature of the objection

51. Objection may be partial (1.1) in the sense that it relates to certain data or processing operations, and imposes a form of "negotiation" or, indeed, compromise, with the controller of

[24] See too retroactive control, by means of a request for the erasure of files, in the event of the controller of the file failing to meet his obligations.

the file, in relation to the data collected and processing undertaken. It may also be complete (1.2), that is to say, challenging the very principle of the collection of personal data.

1.1 Partial objection

52. The use of certain data (a) such as the application of automatic processing (b) or certain transfers (c), would be likely to justify an objection to their collection.

a) Objection to the collection of certain data

53. It may well be envisaged that the data subject will object to the processing of certain data, for example, data that are not required for the processing purposes. In this connection, Recommendation No. R (99) 5 of the Council of Europe of 23 February 1999 giving "Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways" advises users to give Internet providers "only such data such data as are necessary in order to fulfil a specific purpose" and underlines the danger of giving credit card numbers. It also urges Internet users to "be wary of sites which request more data than are necessary for accessing the site or for making a transaction, or which do not tell you why they want all these data from you[25]."

b) Objection to certain processing

54. The objection may well be made in relation to certain uses of data freely provided to the controller of the file. The individual may agree to be included in a telephone directory but not in an inverted directory, just as he might accept having his data included in the Intranet of a government department, but not on the Internet.

c) Objection to certain transfers

55. By the same token, an individual may agree to have his personal data collected and processed while objecting to having them transferred. He will respond, for example, to a major consumer survey, which will be subject to automatic processing by the body collecting the data, but will refuse to have all his replies passed on to third parties, particularly for marketing purposes. In this regard, the CNIL recommends that electronic commerce sites should show "in the forms as a whole whether or not the data collected will be transferred or made available to third parties unconnected with the service provided, such as commercial associates, subsidiaries, etc. and, if so, inform people of their right to object[26]".

1.2 Complete objection

56. Two forms of absolute objection to the collection of personal data are possible: anonymity (a) or a categorical refusal to supply any information (b).

a) Anonymity or pseudonyms

57. Another subtle form of objection is to be seen in the use of anonymity or pseudonyms. This is hardly available to service providers (access providers, accommodation providers or contents providers) because of their legal obligations and the risk of an action in damages. However, it is to be recommended for Internet users[27], as they will then be able to surf the Web without having to reveal their true identity. This can be the case on specialised information sites or discussion

[25] Article II.7 of the Guidelines of 23 February 1999, cited above: see too Article 11 of Directive 97/66/EC of 15 December 1997 of the European Parliament and the Council on the processing of personal data and the protection of privacy in the telecommunications sector, OJEC no. L24/01 of 30 January 1998.

[26] CNIL, 20º rapport d'activité 1999, op. cit. P.104

[27] See the recommendations of the Council of Europe in its Guidelines of 23 February 1999, cited above, on anonymous access to and use of services and payments (Art. II.3) and the use of a pseudonym (Art.II.4), so that your personal identity is known only to your ISP".

forums, for example, unlike the identification requirements implicit in placing an order or making a payment.

b) Refusal to supply any information

58. There could be an objection to the very principle of the collection and processing of data when it appears futile and threatening to the data subject. This notion has obvious limitations in some types of automatic processing the existence of which would not be subjected to individual discretion[28].

2. Grounds for objection

59. Subjected – overwhelmingly – to the reality principle, positive law has very cautiously edged the door open to admit the right of objection. It is not seen in any absolute sense, as a measure of the actual ability of the individual to escape from the digital world. That right is subject to the existence of valid grounds for asserting it, which while ensuring that reason is brought to bear in applying it, also alters its thrust, given the unfair advantage of the controller of the file over the data subject.

60. Article 14(a) of Directive 95/46/EC sets out for the data subject "compelling legitimate grounds relating to his particular situation ", which would appear to restrict the objection to very personal reasons and not to allow objection as a matter of principle. In France, for example, the validity of a refusal is subject to the existence of "legitimate grounds", which are not defined by law and the fact of which would ultimately have to be decided by the courts, which to my knowledge, with one possible exception[29], have never considered the matter….However, it may be wondered how such an evaluation may operate (2.1) and in particular if that existence of grounds for objection is always valid (2.2).

2.1 Assessment of the grounds

61. The issue of the very appraisal of the validity of an objection raises important questions relating to the identity of the body appointed to make the appraisal (supervisory authority or judicial authority or other…), the criteria for appraisal and the priorities in the event of conflict between private interest and the public interest. It has been established that the objection would be held as valid where the data are inadequate or excessive in relation to the purpose of the processing or where the processing would be pointless or dangerous.

62. It must be possible to exercise this right of objection, even in regard to data collection which the controller of the file has stated to be obligatory, unless, of course, the obligation itself is laid down by law. It should be noted, in this respect, that the right of objection is not available for all forms of processing. Article 14(a) of Directive 95/46/EC only provides for it in two instances. The existence of a right of objection is, for example, required for the processing referred to in Article 7(e), "necessary for the performance of a task undertaken in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" but not for the processing operations referred to in Article 7.c which are "necessary for compliance with a legal obligation to which the controller is subject". Likewise, French law excludes this right in the case of certain processing within the public sector to which it has been expressly said not to apply[30].

---

[28] Infra no. 62

[29] See however Cass. Crim 29 June 1999: D. 1999.IR. 244 , in which it was ruled that "the refusal of telephone subscribers to be subjected to commercial direct marketing constitutes, in that it relates to the protection of their private life, a legitimate reason for objecting to the use of their registered data for purposes of digital processing with a view to setting up direct marketing files".

[30] See Article 26 of the Law of 6 January 1978

2.2 Intrinsic validity of the objection

63. It has, moreover, become necessary to consider cases of an intrinsic validity of a personal objection for certain automatic processing, such as purely commercial processing. Such an approach has been included in Article 14(b) Directive 95/46/EC, as cited above, in recognising the right of the data subject "to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses".

64. Likewise, in its Opinion 1/2000 on certain aspects of electronic commerce in relation to data protection presented by the Internet task force[31], adopted on 3 February 2000, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 of Directive 95/46/EC) has laid down that if an electronic address is collected by a company direct from an individual with the intention of sending electronic publicity, "the person whose data are collected should also, at the very least, be asked to consent at the time of collecting and should at any subsequent time have the right to object to the use of his personal data[32](…)" Likewise, the draft label "EUP-European Union Privacy" includes in particular for the website the obligation to "enable Internet users to object on line (…) to the transfer of their data to third parties who are strangers to the transaction.[33]

65. The same course has been adopted by France and attention has been mainly concentrated on the setting up of behavioural databases on the consumption habits of households intended for direct marketing purposes"[34], on the technique of the inverted directory[35] or the matching up of files on the Internet[36]. In such cases it is not so much objection to the collection that is upheld (for often the supply of data is purely voluntary) but the objection to certain transfers of collected data or to the fact that such data are subjected to particular forms of processing.

3. Forms that the objection takes

66. It is clear that the right of objection should be exercised free of charge, but such a fact ought to be stated, as does Directive 95/46/EC in relation to direct marketing[37]. The forms it takes will vary according to whether it is done on line, on the Internet (3.2) or off the Internet (3.1).

3.1 Off the Internet

67. Objection can be made both to the collection (a) and to the transfer (b) of data.

a) Objection to the collection of data

68. Where the response is voluntary, the objection will simply take the form of refusing to reply when data are collected. This attitude is all the more significant in that there is a high risk in

---

[31] CNIL, 20º rapport d'activité 1999, op. cit. p. 343

[32] CNIL, 20º rapport d'activité 1999, op. cit. p. 346

[33] CNIL, 20º rapport d'activité 1999, op. cit. p. 107; see too Article 11 of Directive 97/66/EC cited above

[34] See Decision of the CNIL of 18 February 1997, cited above

[35] See Decision of the CNIL of 8 July 1997, making a recommendation in relation to telecommunications directories, JORF of 2 August 1997, which recommends that "subscribers should be allowed, apart from cases where this is justified to save human life or in the interests of public safety, in advance, free of charge and without having to give any reason, and at any subsequent time, to object to the use of their telephone number in an inverted search service or inverted directory"

[36] See the Decision of the CNIL of 8 July 1997cited above recommending that "subscribers should be able to object free of charge and without having to give any reason, and at any subsequent time, to the dissemination over an open international network of their personal data"

[37] See Art.14b) of Directive 95/46/EC

accepting that "the reply to voluntary questions is presumed to indicate consent, as the individuals questioned have the option of remaining silent to indicate their objection to registration or processing[38]". The refusal may be oral during an interview or by abstention when the replies are sought by a questionnaire. Where replies are obligatory, the data subject will thus have to show legitimate grounds for refusal[39].

b) Objection to the transfer of collected data

69. The right of objection given to the data subject following the collection of his data is mainly concerned with the possible subsequent transfer of such data. The individual is, for example, often asked if he would be willing for his data to be transferred to third parties, generally for direct marketing purposes. It is of paramount importance, therefore, for such a right to be exercised readily.

70. Accordingly, in the case of the questionnaire leaflets delivered to individual homes as part of major "consumer research", the CNIL has recommended that: "consumers should be able to indicate easily, without the need for any additional steps, their objection to commercial companies other than the body collecting the data receiving the registered information relating to them" and that "data subjects should be informed at the beginning of the questionnaire that they can reply to questions while at the same time objecting through the marking of a box to the transfer of their data to third parties and the consequences of their refusal to a transfer[40]".

3.2 On the Internet

71. The right of objection on the Internet is enabled through the so-called "Opt-out" process whereby the Internet user is invited to express a specific objection, failing which the controller of the file may proceed to carry out the automatic processing intended. The opt-out process covers, in reality, two distinct situations associated with the Internet set up[41], even though they sometimes overlap. One would be an objection to the transfer of data collected on the electronic form of the web site (a) and the other an objection to electronic direct mail following the collection of an electronic mail address (b).

a) Objection to transfer of data

72. On the Internet, the opt-out only occurs at data transfer level, objection to collection being made through abstention, by omitting to complete all or part of the sections of the electronic form. The fact of filling in the sections, on the other hand, immediately instigates the automatic processing of the data.

73. In practical terms, the indication of an objection to the transfer of data is undertaken by clicking on a particular box of the screen page, the page on which is displayed the information relating to the proposed use of the data collected. It should be possible to object at the time of collecting the data, when, for example, the Internet user is completing an electronic questionnaire. One could envisage cases where objection could also be expressed subsequently[42] and again, free of charge. For this it would have to be possible for the Internet user to access at any time a page on the web site where there is a section for recording the objection. Such a page should be shown on the menu.

---

[38] CNIL, Dix ans d'informatique et libertés, Economica, 1988, p. 22

[39] Supra no. 61

[40] Decision of the CNIL of 18 February 1997, cited above; as to the adverse effect on marketing economics, see CNIL, Vingt délibérations commentées, op. cit. p. 163

[41] On the parallel with the opt-out for unsolicited phone calls or faxes, see Article 12 of the Telecommunications Directive no. 97/66/EC cited above

[42] See the CNIL Decision of 8 July 1997, cited above, recommending that "subscribers should be able to object free of charge and without having to give any reason, and at any point subsequently, to the dissemination over an open international communications network of data relating to them".

74. Thus, in the matter of electronic mail, the CNIL has reminded the site controllers of the need to show on electronic data collection forms as a whole "whether or not the data collected are to be transferred or made available to third parties unconnected with the service, such as commercial associates, subsidiaries, etc. and, if so, inform people of their right to object[43]". It has recommended that they enable an objection to the data transfer to be made on line, perhaps by means of a box to click on the electronic form[44]. Similarly, in its recommendations to Internet site providers, the Commission recommends, for example, under the heading "Transfer of data": "If you are transferring the data collected or if you are using them on behalf of third parties, for example, for purposes of direct marketing, you must inform the data subjects, at the time of collection, of their right to object to such a transfer or use and to enable them to express their refusal by clicking on a box[45]".

b) Objection to electronic direct mail

75. As far as direct mail is concerned, the opt-out procedure is at two levels. It is used to object to the collection of the electronic (or e-mail) address for subsequent direct mail and/or to object to receiving unsolicited electronic messages. Attention should be drawn to the clarity and the unambiguous nature of the opt-out procedure. The danger is all the greater in that as a general rule, the Internet user who has set up his e-mail on a site is "presumed to have consented to receive commercial messages from that body[46]" unless he expresses his objection. Likewise there is a tendency to think that when the address has been given by the Internet user to a web site which has passed his e-mail file to a third party, any Internet user who has not indicated his objection to the transfer of his electronic mail address for direct marketing purposes is presumed to have consented to it.

76. Thus the CNIL is asking, in its Internet site declaration form, for users to be told, alongside the electronic message box, that they can object to the transfer of their electronic addresses. Moreover, Article 7(2) of Directive EC 2000/31 of 8 June 2000 on Electronic Commerce provides that Member States 'should take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and can respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves[47].

B. Explicit consent

77. Article 6 of Convention 108, entitled "Special categories of data" provides that "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

78. Among the appropriate safeguards that apply to the processing of sensitive data is the consent of the individual, a condition that is particularly apt to protect more strongly against the risks incurred by data subjects. Explicit consent is thus considered the most solid bulwark of protection. It should therefore be asked for whenever the collection and processing of data gives rise to substantially higher risks of invasion of privacy and personal freedom. With the globalisation of data exchange, rendering the individual more vulnerable and helpless, the time has come to overhaul this very delicate issue by examining, in turn, the cases in which explicit consent should be obtained (1), the ways in which it is obtained (2) and its limits (3).

---

[43] CNIL, 20º rapport d'activité 1999, op. cit. p. 104

[44] CNIL, 20º rapport d'activité 1999, op. cit. p. 104

[45] See the CNIL web site: www. cnil.fr, at the heading Internet

[46] C. Alvergnat, Le publipostage électronique et la protection des données personnelles, October 1999, CNIL report published on the CNIL web site, p. 19

[47] See too the more radical solution of anti-spamming software

1. Cases in which explicit consent should be obtained

79. The need for consent has been stipulated for so-called sensitive data (a) but it might be wondered whether it should not also be required for certain processing operations that are in themselves considered to be sensitive (b).

1.1 Consent and sensitive data

80. Certain data are termed "sensitive[48]" of their very nature, by reason of their "potential for discrimination[49]". Article 6 of Convention 108 is a perfect illustration of this in listing data revealing racial origin, political opinions or religious beliefs, as well as data concerning health or sexual life or personal data relating to criminal convictions. Consideration is being given at the moment to extending this category to other data such as genetic data or certain data relating to the intimate details of private life. In any event, such data "may not be processed automatically unless domestic law provides appropriate safeguards[50]". As far as appropriate safeguards are concerned, national legislation has mainly required the consent of the data subject.

81. By the same token, Directive 95/46/EC states in Article 8(1) that ""Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life". Article 8(2), however, provides for a certain number of exceptions to this prohibition, particularly when "the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent".

1.2 Consent and sensitive processing

82. Certain data, that appear harmless enough, can become "sensitive" because of the particular context in which they are used[51]. Thus the circulation of data on the Internet network together with the potentially trans-border character of exchanges have gradually given support to the concept that certain data, placed on the "web", rendered the individual particularly vulnerable and called for additional precautions. The transmission of an organigram over the Internet, for example, does not carry the same connotations as its communication in paper form, bearing in mind the possibility of conducting searches by means of keywords in any corner of the globe.

83. Of the safeguards sought to alleviate these new risks, the most popular has been the obtaining of the individual's consent. Thus the transmission over the Internet of scientific directories has taken place with the explicit written agreement of the researchers, who could ask at any point to have their details removed[52]. This requirement is reinforced by other conditions relating, on the one hand, to informing searchers of the risks of the Internet network and of personal rights, by means of a notice appearing on the computer screen, on the one hand and, on the other hand, technical security measures when consulting the directory.

84. The above examples reveal a radical approach to protection that is explained by the apprehension awakened by the Internet. Some consideration should be given to the

[48] See S. Simitis, Sensitive data revisited, Report for the Council of Europe, Strasbourg, 24-26 November 1999

[49] CNIL, dix ans d'informatique et libertés, op. cit. p.43

[50] Article 6 of Convention 108

[51] See in this context, CNIL, Dix ans d'informatique et libertés, op. cit., p.42

[52] See in particular the CNIL Decision no. 95-131 of 7 November 1995: 16º Rapport CNIL 1995, Doc. Fr. 1996, p.85

opportuneness of this and to the eventual viability of making the seeking of explicit consent general, of making its use widespread. or of confining it to certain data or certain processing[53].

85. Similarly, it is important to see how the obtaining of consent can or should be combined with other safeguards, such as those connected with trans-border flows. The potentially international character of the transmission of data on the Internet should, in fact, result in the systematic application of all the provisions governing the trans-border flows of data, particularly in relation to a "reciprocal protection" within the meaning of the Additional Protocol to Convention 108.

86. These conditions will act as a counterpoint to consent, which is not always required within the context of international transfers[54]. Legislation in fact supports the implementation of more onerous administrative procedures, together with the verification of a reciprocal or adequate level of protection. It will be observed, in this context, that Article 26(1)(a) of Directive 95/46/EC provides, among the grounds for derogating from the requirement, for a third country to ensure an adequate level of protection, the fact that "the data subject has given his consent unambiguously to the proposed transfer", thereby *de facto* removing the other safeguards, which would appear somewhat risky.

2. Means of obtaining explicit consent

87. Explicit consent can be obtained on the Internet (2.1) or off the Internet (2.2).

2.1 Off the Internet

88. The consent of the data subject can be obtained without any Internet connection, by means of an interview or by correspondence. It must in such a case be evidenced by a written and explicit agreement.

2.2 On the Internet

89. When agreement is obtained through a connection to an Internet site, the Internet user shows in a positive way that he agrees to the collection and processing of those data, by means of the so-called "opt-in" process. Contrary to the saying "silence is consent", silence on the part of the data subject must be interpreted as a refusal to have the data collected and processed. The opt-in should take place at the time when the Internet user receives such data, by completing a special section clearly displayed on the screen page. It will generally consist of clicking on a box provided for that purpose, this process being accompanied, where appropriate, by security measures in relation to the individual identity and authentication.

3. Limits of consent

90. While the obtaining of consent can provide an additional safeguard for the protection of the individual, it must also be borne in mind that the fact that the data subject has consented does not justify all forms of processing. Limits can be imposed both on public policy (*ordre public)* grounds (3.1) and on ground of contractual fairness (3.2).

3.1 Consent and public policy (ordre public)

91. The rule that the simple agreement of the parties is sufficient to bind them contractually finds a stumbling block in the notion that some types of processing must be ruled out for certain data

[53] On the notion that unambiguous consent is a main source of the legitimacy of one-to-one marketing, see T. Léonard, E-Commerce et protection des données à caractère personnel, Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet, p. 10, published on the CRID web site, Namur Law Faculty: www.droit.fundp.ac.be/crid

[54] It is not mentioned in the model clauses for inclusion in the model contract for ensuring equivalent data protection in the context of trans-border data flows, a study made jointly by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce.

and certain data carriers and that the individual must sometimes be protected against himself when he is not always aware of the risks he is running. Accordingly, Article 8(2) of Directive 95/46/EC refers, in relation to the processing of sensitive data, to the case where "(…) the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent".

92. This possibility could be used, as G. Braibant emphasises, "in relation to the processing of genetic data, where this is not undertaken within the context of medical processing, for the purposes of medical research, or in legal proceedings[55]". One thinks too of certain "advertising" formalities in connection with administrative measures[56] or public data[57] which could hardly be displayed on the Internet, even with the consent of data subjects. There is an evident need to urge a "self-censoring" policy in relation to certain automatic processing where such processing is likely to carry risks, an approach which returns to the spirit of the purpose principle.

3.2 Consent and contractual practices

93. As with any contract, consent has to be willing and informed. This means, of course, that the information given with a view to acceptance must have been precise, complete and unambiguous. It also means that agreement must have been reached without any coercion, which throws some doubt on the validity of contractual practices whereby access to the Internet is free of charge to the Internet user in exchange for certain data. Is consent to data processing acceptable when it is given in return for financial advantages, or a free subscription, or when refusal inevitably goes hand in hand with "reprisals[58]" (refusal of cookies impeding navigation)? This is certainly an issue which deserves attention in relation to Internet transactions…

CONCLUSIONS

94. The widespread use of international data exchange, and in particular the success of communication *via* the Internet network, call for a new mobilisation on the question of protecting human rights. This change of scale should be greeted as an opportunity and treated with the utmost rigour. The principles of data protection have a solid base and can cope with the difficulties. However, it requires a modulation of responses, without over-simplification, adapted to individual situations and relating to the structures to be protected within society and the risks facing the data subject.

95. This report has sought to echo the real concerns in the search for individual preventive protection measures "before the harm is done". It has avoided any examination of appeals to administrative authorities or applications to the administrative court in respect of violations of the law, despite the fact that their existence is clearly essential. The emphasis has been on the pragmatic point of view. It is hard to imagine within every Internet user-consumer a litigant well versed in the finer points of international law and with enough time, money and energy at his disposal to "do battle" against the recording of his personal data in a third country for the purposes of a commercial mailing list. … The counter attack would be out of all proportion to the purely individual interests.

96. Are we, then, to admit defeat? Certainly not. Despite the glaring difficulties and the enormity of the task, it is vital to try to provide the individual with means of self- protection. Existing regulations must be overhauled to make the individual more vigilant and active. That is why Internet users are very rightly advised to use the right of access and rectification and to "repeat

---

[55] G. Braibant, Données personnelles et société de l'linformation, Rapport au Premier ministre, Doc. Fr. 1998, p. 93

[56] such as naturalisation orders

[57] such as ministerial organigrams

[58] See T. Léonard, op.cit. no. 12, which states that "refusal of processing on the part of the Internet user cannot carry a risk of discrimination for him".

this request from time to time[59]". New rules must certainly be drawn up, for instance to cover the concept of sensitive data or the emergence of the notion of sensitive processing.

97. Consumer feed back should be encouraged. It is often "a little out of touch with reality", but should be noted. I would mention, for example, the suggestion made to the Internet user to consider moving to another ISP where dissatisfied and to inform the competent authorities or take legal action[60]. Similarly the choice to navigate only on "labelled" sites of the "EUP" label smacks of wanting to be at the receiving end of the data protection process.

98. In short, the possibilities offered by technological protection (filter software, encryption software, de-personalisation software or anti-spamming software) should be optimised together with the new means whereby the individual may exercise his prerogatives on line, for example the right of objection or the right of access *via* electronic mailboxes. The idea will be for a type of electronic "strongbox" available to every individual, "accessible to him alone in complete privacy[61]". All such technical safeguards should be reinforced in association with legal safeguards.

99. The above remarks are intended to encourage in the individual common sense responses to new practices and to instil in him, without wishing to sound grandiloquent, "survival" instincts in a "digital universe". That is why the individual is seen variously, according to the case in point, as a "conscientious objector", a "negotiator" or simply an "observer" who is mindful of the uses to which his personal data could be put. This report is in any case concerned with the defence of the individual "implicated" in the data protection provisions.

100. May these few reflections serve as a modest starting point for some fruitful work on the place of the individual in a world of globalised information, in the light of the experiences of the panellists invited to participate in the round table on "The means available to the individual in protecting his personal data and asserting his rights in the context of globalisation".

[59] See Article II .10 of the Council of Europe Guidelines of 23 February 1999, cited above

[60] See Article II .11 of the Council of Europe Guidelines of 23 February 1999, cited above

[61] M. Sapin, Intervention à l'université d'été de la communication, August 2001, p. 3, paper published on the website www.fonction-publique.gouv.fr.

THE PLACE OF THE INDIVIDUAL IN A WORLD OF GLOBALISED INFORMATION: RIGHTS AND OBLIGATIONS

SUMMARY

What means of intervention are available to the individual whose personal data are collected, processed and transmitted in a world of globalised information? How, for example, can he gain control of the use of his data on the Internet, preferably in advance and without being faced with contentious proceedings?

With the legal data protection instruments, individual prerogatives are essentially focussed on the right to information, on the one hand (and, where appropriate, on consent, its corollary) and, on the other hand, the right of access and rectification as set out in Article 8 of the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, under the heading of "additional safeguards for the data subject".

This report attempts to evaluate how this works out in practice by examining in turn how the individual may hope to be properly informed of the existence of processing and how, in certain cases, he may have the possibility of consenting or objecting to it.

The right to be informed beforehand, as a guarantee of the transparency of data files, is one of the pillars of the legal systems for data protection, but its provisions should be thought out and adapted to take account of greatly varying situations for data collection and processing. However, the circumstances in which this right to information must be implemented are not always clearly anticipated and frequently result in a neutralisation of that right, in particular when files are transferred. A way of finding a solution to this was examined by making a distinction according to whether the collection is primary, that is to say, undertaken, directly or indirectly, from the data subject, or secondary, that is to say, undertaken on the basis of a previously constituted file.

The right of access is one of the indications of the right of information of the data subject. It enables him to check the accuracy of information held by the controller of the file and, where appropriate, to ask for their rectification. However, in the majority of automatic processing, this individual prerogative remains remarkably little used, a worrying sign of a degree of resignation or of an excessive level of pessimism or discouragement as to the efficiency and benefits of the right of rectification. In a world of globalised information, the right of access will remain a dead letter if it is not possible to guarantee to the individual the "tracking" of automatic processing operations, however, paradoxically, the Internet world can enable this.

However, when considering the reinforcement of personal rights in a world of globalised information, the issue of personal consent comes immediately to mind as the most significant aspect of the control that the individual would have over the use of his data and of his power of self-determination. It might well be, for example, that consideration should be given to furthering the generalisation of personal consent as a last resort measure of protection in the face of an internationalisation of data exchange. The response cannot be categorical, but should be adapted to the kind of data and processing intended. The risks of encroachment on privacy and freedoms are evidently not the same in the case of marketing data as in that of medical data. The indication of consent may be adapted according to the interests at stake, and in particular the debate concerning the "opt-out" or "opt-in".

It is of paramount importance to try to make the individual proactive in protecting himself. Existing regulations must be revised to make the individual more vigilant and active, such as the reiteration

of the right of access. New regulations must certainly be drawn up on, for example, the emergence of the concept of sensitive processing. Consumer feedback is to be encouraged. The choice to navigate only on "labelled" sites smacks of wanting to be at the receiving end of the data protection process. The possibilities offered by technological protections must not be overlooked, and similarly the new means whereby the individual may exercise his prerogatives on line.

This report is concerned with the defence of the individual "implicated" in the data protection provisions, a modest starting point for work on the place of the individual in a world of globalised information, which will no doubt be communicated by the responses of the panellists invited to participate in the round table on "The individual's means for protecting his/her personal data and asserting his/her rights in the context of globalisation".

PAPERS

Round Table: Present and future prospects for legislation on personal data protection in particular in the countries of Central and Eastern Europe

PREPARATION OF THE DRAFT AMENDMENT TO ACT NO. 52/1998 COLL. OF THE SLOVAK REPUBLIC ON THE PROTECTION OF PERSONAL DATA IN INFORMATION SYSTEMS

Paper by

Mr Peter LIESKOVSKÝ
IT Specialist, Inspection Unit for the Protection of Personal Data
Slovak Republic

1. Objectives of the draft amendment

The draft amendment to the Act on the protection of personal data in information systems is being prepared in such a way that the result will secure fulfilment of three objectives, which are:

a) to achieve full compatibility with Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free flow of such data;

b) to consider recommendations by the experts of the European Commission who assessed the protection of personal data in the Slovak Republic; and

c) to incorporate into the draft amendment the experience gained by the state administration from practical applications during the two-year period of performing tasks provided for by the present law.

With regard to point a):
The greatest substantive differences between the EU Directive and the present law are in the area of processing of personal data and freedom of speech. The present law does not permit processing of personal data for journalistic purposes without the data subject's consent. So far, the data subject's consent has been required if the public is to have the right to true and correct information from the media. Here the principle of the right to information is restricted by the principle of personal data protection. But the spirit of the Directive goes in the opposite direction.

Further, there is not sufficient acceptance of the data subject's right of access to his personal data within the meaning of the Article 10 of the Directive. A data subject has, under the present law, a right to information about how his personal data are processed, but has no right to obtain a description of his personal data. It is thus difficult for him to check whether a controller processes correct personal data and to require correction of inaccurate and outdated data, if he does not know what data related to him are processed by the controller.

In conformity with the Directive, the amendment will increase the independence of state supervision over the protection of personal data. It is proposed that a Commissioner for the protection of personal data will be appointed by the President of the Republic on the basis of a proposal by the government and with the consent of Parliament. It is also proposed that the Council for the protection of personal data, as an advisory body for the Commissioner, will give an opinion on serious complaints regarding breach of personal data protection. It is proposed that the Commissioner and the Inspection Unit could make decisions to impose sanctions for breach of the law.

With regard to point b):
The current state of protection of personal data was examined by the EC mission (the PHARE programme) led by Mr Alex Turk, a French Senator and a member of the French national commission for supervising the protection of personal data in France (CNIL), during two visits (21–25 February 2000 and 15-18 May 2000). Although the mission was especially aimed at implementation of the Schengen acquis with regard to personal data protection in information systems operated by the police, it also paid attention to the act on the protection of personal data. A written report which summarises the results of the mission also contains several recommendations concerning improvements to the act on the protection of personal data.

With regard to point c)
Lastly, when drafting the amendment, use was made of Slovak experience with regard to practical application of the law. Many complaints relating to violation of personal data protection (more than 200), regular controls aimed at processing of personal data by large controllers revealed ambiguities in its current wording. Removal of these ambiguities is also one of the objectives of the amendment.

Approval of other laws concerning personal data had considerable influence on the amendment. Approval of the act on the free access to information (the so-called the information act) must be mentioned in this context.

Furthermore, there are substantive changes in the introduction of automatic means of data processing, in particular the development of hardware, software and telecommunication services and, in this connection, new means developed for increasing security of data.

The introduction of video surveillance and efforts to create DNA databases regulated by law influenced the draft amendment as well.

Recently discussion has started in Slovakia in the light of the latest terrorist attacks on the USA with regard to a certain form of restriction of rights and freedoms in the area of data protection with respect to increasing security of the state and its inhabitants. These factors may have additional influence on the amendment.

2. The main changes in the amendment against the present law

The most important changes and modifications which the draft amendment will bring to the Act on the protection of personal data in information systems are indicated below.

- *The first part deals with specification of the definitions and terms* that are crucial to personal data protection. New definitions are introduced as well, such as providing of personal data, accessing of personal data, publicizing personal data, making personal data anonymous, biometric personal data, and so on.

- *The second part contains a new modified § 4 – the data subject's consent to the processing of his personal data*. Here essential specifications are used, which are a particular reaction to Articles 6 and 9 of the Directive, as well as the removal of inaccuracies which were detected in the course of application of the law in practice.

- *The data subject's consent is again modified for further processing of personal data which are used for the purposes of keeping records or postal addresses* (title, name, surname, address). The regime for dealing with these data is being harmonised with the recommendations of the Council of Europe in the area of direct marketing.

- *The provisions of Article 7 are also modified once more* – processing, provision, access and disposal of personal data.

- *In accordance with Article 8 of the Directive, Article 8 of the law has been changed – special categories of personal data*, where it is defined what personal data belong to this category and *conditions of processing of these categories of data are expressly determined*. Biometric data are included in the special category as well because it is considered that, for example, DNA without doubt constitutes sensitive personal data.

- *The draft amendment extends the obligations of controllers in an essential way by securing the protection of personal data in large information* systems operated by means of computer and transmission techniques, as well as in processing special categories of personal data or in transborder data flows. In these cases *the controllers of information systems will be obliged to work out security projects for their information systems*.

- *Transborder data flow is modified in a way that provides that all conditions of securing exchange of personal data among states are met*. What is in accordance with Article 26 of the Directive will not be prohibited.

- *Substantial changes are proposed in respect of the registration of information systems containing personal data*. These changes are of an organisational and substantive nature. The most essential change consists in assigning the responsibility for registration to the State Supervisory Authority for Personal Data. All relevant activities are thus logically performed by a single organisational entity. The scope and conditions of registration of information systems are subjected to registration changes. *It is proposed to carry out central registration only of those information systems that either contain special categories of personal data or where transborder data flows of personal data are envisaged.* Other information systems are subject to the obligation that controllers should keep records directly. It is taken for granted that not only registered information systems but also non-registered information systems will be publicly accessed by data subjects.

- *More substantial change in supervising protection over personal data lies in:*

- enhancing independence of this body;
- becoming more stand-alone from the Office of the Government; and
- in creating of the Council on the protection of personal data as an advisory body for the Commissioner.

At the same time it is proposed to appoint inspectors on the protection of personal data who with their powers and status will enhance independence of execution of state supervision. In this regard there will also be the possibility to impose sanctions for breach of provisions laid down by the law.

The amendment contains in addition a change in the power to impose fines, vesting it directly in the State Supervisory Authority for the Protection of Personal Data. *The State supervisory authority will be allowed to impose sanctions for breach of the law directly without co operation with the Office of the Government*. The amount of fines was brought in line with the fines imposed in neighbouring countries. The upper threshold of fines imposed for the breach of personal data protection legislation in EU countries is equivalent to around SKK 7 million. It is proposed to multiply the amount of fines by ten; The Slovak Republic will thus reach a comparable level with European countries.

3. Process of preparation of the draft amendment

It could be said that work on the amendment began already during the when carrying out the tasks of state supervision, that is to say since October 1999 when inaccuracies in the present law were detected and note was taken of what would be needed to change or specify in the amendment.

Lack of harmony, or direct discrepancy, with the Directive, which needed to be removed was, of course, acknowledged. The European Commission provided information on some of the shortcomings.

The process of preparation of the amendment *can be divided into the following steps:*

- preparation of the first version of the draft amendment (6/2001);
- transmission of the text to all relevant public bodies for comments;
- publishing of the amendment on the Internet;
- transmission of the first version of the draft amendment to Mr Alonso Iriarte who proposed co-operation in evaluating the draft amendment to carry out analyses (7/2001);
- evaluation of the comments received from the relevant public bodies and preparation of the second version of the draft amendment (9/2001);
- submission of the draft amendment to the required legislative process (the Legislative Council of the Government) (10/2001).

Adoption of the amendment is proposed for 1 January 2002. As parliamentary elections will be held in 2002, it is more than probable that the amendment will enter into force during the first half of next year.

DATA PROTECTION LAW: PRESENT AND FUTURE RESPONSES TO THE CHALLENGES OF THE INFORMATION SOCIETY

Paper by

Vaida LINARTAITĖ
Chief inspector
State Data Protection Inspectorate
Lithuania

The human being is a part of society, a social being, although he keeps his individuality to some extent in reticence and solitude. The scope of privacy for each individual may not infringe the rights of others. The balance between public life and privacy has changed during the existence of humanity. Different economic and social conditions influenced this balance all the time. Under the present conditions of the information society, new kinds of dangers arise for a person's private life. The recent history of Eastern and Central Europe has shown many examples where the State made great efforts to control the individual's every word and step. It led towards the destruction of the society itself. The creation of a free and open society requires protection of freedom, individuality and diversity of each member of this society. The guarantee of his privacy is essential for a person to feel free and safe.

Both the Constitution of Lithuania and the Convention for the Protection of Human Rights and Fundamental Freedoms deal with the privacy issue, which is the crucial for data protection. Data protection issues are rather new in Lithuanian society, many people do not know about their rights and guarantees offered by laws for the protection of their rights. Now we confront the tremendous development of information technology. The creation of the information society has proved to be of great influence on the growth of the economy. Private business is strengthened, public services provided by the State are achieving new quality and quantity; a new generation of educated people equipped with useful knowledge applies it in practice. The development of the information society is a global process, which does not exclude Lithuania. Although the progress made in information technology is making the processing and exchange of personal data considerably easier, it should not be forgotten that this occurrence also creates and increases new ways of violations of the right to privacy. It offers not only new possibilities to society but new dangers to privacy. Such evolution of technologies imposes on the State an obligation to create and implement effective legal safeguards for the protection of privacy from such new infringements. The right to respect for private and family life and also the right to freedom of expression are not absolute and can be restricted. It is extremely important in legislation and application of the law in everyday life to impose a reasonable balance and proportionality of those constitutional values for the prevention of the misuse of law.

The definitions of "private life" and "right to respect for private life" are rather new in the Lithuanian legal dictionary. The Constitution of the Republic of Lithuania establishes the right of inviolability of the person's private life (Article 22) and the right to seek, obtain, or disseminate information or ideas, and freedom to express convictions, as well as to obtain and disseminate information; this right may not be restricted in any way other than as established by law, when it is necessary for the safeguard of the health, honour and dignity, private life, or morals of a person, or for the protection of constitutional order (Article 25). These guarantees were established in October 1992 at constitutional level. In 1995 Lithuania ratified the Convention for

Protection of Human Rights and Fundamental Freedoms, which establishes the right to respect for private and family life and the right to freedom of expression. As it was ratified by the Seimas and entered into force the Convention became a component part of the Lithuanian legal system and is directly applied.

The Council of Europe Convention ETS No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data is one of the most crucial international legal instruments, which had and still has a profound effect around the world on the enactment of laws concerning data protection. The preamble of Directive 95/46/EC of the European Parliament and of the Council clearly indicates that: ”the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention ETS 108.”

Lithuania is no exception and established the main European requirements by adopting the Law on Legal Protection of Personal Data. The Law on Legal Protection of Personal Data was adopted in June 1996. The purpose of the Law was to establish the rights of data subjects and the manner of protection of those rights, and guarantees of the rights to data protection during processing of personal data in information systems. The new version of the Law on Legal Protection of Personal Data was adopted in 2000 and entered into force on 1 January 2001. On 20 February 2001 the Seimas ratified Convention ETS 108 and it came into force on 1 October 2001. The Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows was signed on 8th November 2001.

Although the Convention was adopted twenty years ago, it is still of great importance. Since 1981 the basic principles and requirements of data processing are the same and are valid despite the tremendous development of the information society and technology. The present main objective of our State is accession to the EU and we need to make our data protection laws more consistent with European standards and in balance with the level of information technology. For the achievement of this objective a number of supplements were made to the laws. The Administrative Code was supplemented with regulations related to unlawful processing of personal data in 1998. The new Civil Code, which has been in force since 1 July 2001, has been supplemented with regulations on the protection of the right to privacy, honour and dignity. The Penal Code, although not in force, deals with illegal activities in the informatics field (cyber crimes), crimes against privacy, illegal usage of smart cards.

Data protection plays a role of great importance in the development of the information society in a democratic state. The development of data protection is part of the development of a safe information society.

In view of the recent progress of technology-based systems and new kinds of infringements of human rights related to this development we must:

(1) Improve the legal basis, the administrative capacity of public institutions, in response to the challenges arising from information technology development, while paying attention to the balance and proportionality of constitutional rights, protecting people from new dangers to their privacy, and create a trustworthy and effective data protection system corresponding to the EU requirements.

(2) Create favourable conditions for the protection of the constitutional right to the private life of the data subject in the information society.

(3) Stimulate the development of these technologies that strengthen the security of data protection and make conditions for the development of e-Commerce.

(4) Inform society about data protection, the right to privacy, and new ways of possible infringements arising from the progress of technologies.

DATA PROTECTION PRESENT AND FUTURE IN THE COUNTRIES OF CENTRAL AND EASTERN EUROPE*

Paper by

Mr Karel NEUWIRT
The Office for Personal Data Protection
Czech Republic

Council of Europe

- 43 member States
- 19 member States from the countries of Central and Eastern Europe (CEE)
  Albania, Armenia, Azerbaijan, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Hungary, Latvia, Lithuania, Moldova, Poland, Romania, Russia, Slovakia, Slovenia, "the former Yugoslav Republic of Macedonia", Ukraine

Signature and Ratification of Convention 108

- Signature - 12 member States of CEE
  1st – Hungary, 13 May 1993

- Ratification - 7 member States of CEE
  1st - Slovenia, 27 May 1994

Harmonisation with basic European legislation has been strong motivation. When talking about European legislation we have in mind Convention 108 and Directive 95/46/EC. The Czech Republic, as candidate state for membership of the EU, had to adopt the Directive into national legislation. Immediately after adoption of the new legislation the Czech Cabinet approved signature and ratification of Convention 108. Ratification has been adopted by the Parliament.

Just two weeks ago the Office obtained comments on harmonisation from the European Commission.

Supervisory Authorities

- CEE parties to Convention - 8
  Czech Republic, Estonia, Hungary, Latvia, Lithuania, Slovak Republic, Slovenia,

  Poland (unfortunately not party to Convention 108, but has a supervisory authority that functions well)

In the effort for harmonisation of Czech law with European law, one of the important issues has been to establish an independent supervisory authority. The Office has been established by Article 2 of the law and today has about 65 members of staff. In addition to the chairman of the Office, 7 inspectors have also been nominated by Senate and appointed by the President, Mr Havel.

*This paper is taken from a PowerPoint presentation given by Mr Neuwirt during the Conference.

The Czech Republic has no experience of independence of state authorities. Some of them have been created by the Czech Constitution (for example the Supreme Control Office). “Independece” problems continue.

Staffs and Competency

Czech Republic	- 68 (resp.90) - independent
Hungary	- 120 - independent
Latvia	- (?)
Lithuania	- 8 - independent
Slovak Republic	- 12 - independent / dependent
Slovenia	- 2 - dependent on the Ministry of the Interior
Estonia	- 15 (resp.23) - independent
Poland	- 98 – independent

The competences of the Office are stipulated in Articles 28 and 29 of the law. In accordance with the provisions of Article 16 everybody who intends to collect and process personal data is under the obligation to notify this intention to the Office. Today more than 11,000 controllers are registered who have notified about 15,000 processed databases.

CEE experiences
Problems in CEE countries
(no history, no legislative practice, no experience of supervision, legal constitution of independent authority)

Domestic law is not harmonised with data protection principles (it is necessary to amend many domestic laws). It is a new legislative area and many people must be educated in this matter.

Many other laws (sectoral) are not harmonised with data protection principles. It will be necessary to amend many laws. As regards new legislative regulations, the Office is requested to provide comments and advice.

One very important experience in the Czech Republic is lack of willingness to apply data protection principles in daily practice.

When the law was adopted by the Parliament everybody was satisfied that the legislation was in European quality. But in order to apply this quality many formerly existing habits, practices and methods will need to be changed. And many civil servants, state institutions and private companies are unwilling to change their working methods. This is a crucial issue and a long time will be needed to change the minds of many people.

Problems with application of the law in daily practice

- no relevant data collection
- consent of data subject
- data transfer
- no knowledge among citizens
- lobby effort to amend the law

Little willingness to change bad practice of controllers and processors
(long routine of work, lack of motivation,
lack of knowledge of data protection principles,
customs in administration)

Excessive amount of data collected, use of data collected in excess of the purpose originally established, and so forth.

CEE countries have similar problems

- national public registries (citizens, economic activity, properties, debtors)
- data sharing

- conflict with public access to information
- statistical service (census)
- abuse of citizen's national ID number
- health and social sectors
- access to documents of former State Security Services

Overview of some frequently observed problems in the public sector.

The theme of this conference includes public access to information. In the Czech Republic there is no authority competent to explain the act on free access to information. It will be necessary to debate whether the Office could be this authority (as in Hungary, the United Kingdom and Germany).

Council of Europe and CEE
Can the Council of Europe help the CEE?

- Legislation
- Implementation in practice
- Supervision
- Reports on harmonisation with Convention 108
- International co-operation

Legislation

- Help to create new legislation on data protection in CEE countries
- Give advice on transfer of Convention 108 principles into domestic law
- Effort for harmonisation of domestic legislation among Council of Europe countries

Implementation in practice

- Legislation versus application in daily practice
- Data protection principles shall be respected in practical life not only in legislation

Supervision

- CEE countries do not have experience of "independent" authorities
- Council of Europe position on application of Article 1 of the Additional Protocol in CEE Convention 108 Parties
- Council of Europe help to non-Parties to Convention 108

Reports on harmonisation with Convention 108

- Council of Europe observations and comments on data protection level in CEE countries
  (similar to the EC report on progress towards accession)

International co-operation
To give the opportunity of working in Council of Europe expert groups
Bilateral and multilateral contacts between supervisory authorities
Council of Europe conferences, workshops, seminars, etc.
Support CEE activities

Supervisory Authorities
Problems in the private sector

- direct marketing
- insurance, banking sectors
- register of bad payers
- public transport
- telecommunication providers

A lower number of problems are observed in the private sector than in state sector.

Terrorist attack

- What 11 September means for data protection
- Council of Europe – Declaration on the fight against international terrorism (12 September)
- New debate on human rights and data protection (Germany, United Kingdom, France, Czech Republic)
- Is it necessary to reduce data protection principles?

Professor Bullesbach has just mentioned this problem in his speech.

Germany – Minister of Interior Mr.Schilly

United Kingdom – to issue a citizen's cards

France – Prime Minister Lionel Jospin at the international conference in Paris the week before last.

Czech Republic – The Vice Prime Minister, Mr.Spidla, talked about reduction of data protection and creation of new legal rules for sharing public (state) databases. President Havel mentioned this issue in his speech but he is persuaded.

Human rights must be more strongly preserved.

I wish to interrupt my speech with a question – is it necessary to reduce European data protection principles in the interest of fight of international terrorism?

Thank you for your attention.

- Amendment of legislation on security services, police, internal security
- Desire for respect
  Declaration of the Committee of Ministers (12 September)
  Resolution no.1 of EMJ Conference (5 October)
  Joint T-PD and CJ-PD Communication (created by J-.P. Walter) and other Council of Europe documents

- some effort has been observed to amend and modify legislation on security services, police and internal security bodies to give them more competence to defend human rights and data protection
- it is necessary to respect the Declaration of the Committee of Ministers on the fight against international terrorism (12 September 2001), Resolution no.1 of the 24th Conference of European Ministers of Justice (Moscow, 5 October 2001) and the Communication on data protection and the fight against terrorism

Contacts

The Office for Personal Data Protection
Havelkova 22, CZ-130 00 Prague 3
Czech Republic
tel.: +420 2 2100 8288
fax: +420 2 2271 8943
info@uoou.cz
www.uoou.cz

Thank you for your attention and for the invitation to this excellent conference, which gives me the opportunity to present data protection in the Czech Republic.

Round Table: the fundamental principles of Convention 108 and their relevance now, in particular the role of information technologies in implementing data protection principles

---

THE FUNDAMENTAL PRINCIPLES OF CONVENTION 108 AND THEIR RELEVANCE NOW, IN PARTICULAR THE ROLE OF INFORMATION TECHNOLOGIES IN IMPLEMENTING DATA PROTECTION PRINCIPLES

Paper by

Mr Graham SUTTON
Head of the Data Protection Convention
Lord Chancellor's Department
United Kingdom

1. In looking at the continuing relevance of the Convention, I want to pick up a couple of points that have already been made by previous speakers: the rapid technological developments that we have seen in recent years; and the need for a balance to be struck.

2. In the last 20 years developments in IT have come on apace. The IT world is a vastly different place now from what it was 20 years ago. In 1981 how many of us could have had even the remotest conception of the wide-ranging opportunities offered by the Internet? How many of us would have thought that we could sit at our desks in front of a personal computer and send messages around the world at the click of a mouse? Nor have we seen the last of it. I have heard it said that the processing power of computers doubles every two years. Personally, I cannot conceive what the IT world will look like in two years time. But we can be certain that it will be vastly different from today.

3. The second point is the need to strike a balance. I find that there are very many things which need to be weighed. This morning Judge Safjan talked about a balance between the right to information and the right to privacy. As one who works on both freedom of information and data protection I can recognise that tension. But there are other balances too. Crucially, there is the balance between our right as individuals to have data about us protected, and organisations' legitimate need to use those data in order to deliver the services that we all demand. A particular aspect of this can be seen in the aftermath of the events of 11 September. How far is it legitimate to go in intruding upon individuals' privacy rights while working towards the elimination of terrorism with the aim of giving citizens the security which is our right? This is another point that Judge Safjan made this morning. There is also a balance between different types of processing. As Sören Öman has suggested - and I agree with his analysis and his proposed approach - some types of processing operations are inherently less threatening to individuals' privacy than others.

4. Where does all that leave us in terms of the relevance of the Convention? It is clear that the fundamental rules introduced by the Convention are sound. The data protection principles are based on good information handling practices. Efficient organisations would probably want to do what the principles require them to do in any event, because they represent good business practice. And individuals' rights created by the Convention - especially the core right of subject access - must continue to underpin any structure for protecting personal data. So the essence of the Convention remains relevant. But 20 years on, in the context of the changes in information technology that we have seen, I believe that there is a strong case for reviewing the

way in which the Convention operates. We need to test whether it still strikes the right balances.

5. As Sören Öman said, is there not a case for seeing whether a "light touch" approach would be sensible in some cases? Technology has evolved and continues to do so. It plays an ever-increasing part in all our lives. Sometimes it can pose real threats to our privacy. But often it provides virtually risk-free ways - as regards privacy - of improving the efficiency of our business or assisting us in our domestic activities. I believe that we need to look at how we apply the Convention in the light of these changes to ensure that its application matches the particular circumstances in which personal data are processed. It would be unfortunate - to put it no higher than that - if the benefits of IT were diminished by a heavy-handed approach to enforcement of the Convention.

The fundamental principles of Convention 108 and their relevance now, in particular the role of information technologies in implementing data protection principles: Paper submitted by Mr Sören ÖMAN

THE FUNDAMENTAL PRINCIPLES OF CONVENTION 108 AND THEIR RELEVANCE NOW, IN PARTICULAR THE ROLE OF INFORMATION TECHNOLOGIES IN IMPLEMENTING DATA PROTECTION PRINCIPLES

Paper by

Mr Sören ÔMAN
Senior Legal Adviser
Ministry of Justice
Sweden

Mr Chairman, Ladies and Gentlemen,

The fundamental principles contained in Convention 108 aim at protecting the privacy of individuals concerning information. Each of the principles seems reasonable in itself. In my mind, there is no doubt that the principles today are as relevant and adequate as when they were adopted twenty years ago. The principles work well when it comes to automatic processing of large amounts of personal data contained in traditional registers where the data are structured in order to facilitate retrieval of personal data. In those cases the principles should be applied in a strict manner. If that is the case, the public's confidence in the processing carried out by state authorities and large corporations such as banks and insurance companies is enhanced. I would like to argue that the principles were developed with such cases in focus. Twenty years ago, the automatic processing of personal data was almost exclusively conducted in the form of traditional registers by authorities and corporations with large resources.

But the principles are applicable to all automatic processing of personal data. As soon as a single piece of information relating to an identifiable individual is typed on a keyboard of a computer, all principles are to be applied. Today, word processing of text, which has not been structured in order to facilitate retrieval of personal data, is one of the most common forms of automatic processing of personal data. Such processing is at present carried out every day by almost all enterprises, large and small, and by almost all the millions of office employees in Europe. The text produced could be for correspondence, for publication on the Internet or for an internal memo or a draft decision.

When the principles in Convention 108 were developed twenty years ago, the bulk of the word processing of text was conducted by non-automatic means and therefore not covered by the principles. But the technological development has moved also the everyday production of text into computers. Thus, the scope of application for the principles has been extended to an area for which they were not developed. As I see it, the question is whether the principles are suitable for the now so common everyday production of text by millions of employees or whether a different approach is more feasible.

The principles are *per se* adequate also for the production of text containing personal data. Who could for example argue that personal data in the text should *not* be adequate and relevant in relation to the purposes for which they are stored? But the proper application of the principles requires a bureaucracy and that the employee producing the text for every piece of personal data goes through all the steps required by the principles. In my opinion, it is not reasonable to

have such a bureaucracy, or the costs that are connected with it, for the everyday production of text. I also believe that the principles in practice are not, and will never be, strictly applied when it comes to such processing. In fact, several of the respondents to a recent survey in Sweden believe that the application of the principles every time someone is producing text is absurd. The overall respect for the principles and their acceptance is thus threatened in Sweden.

For those reasons I believe that we need a different approach for data protection as regards the production by automatic processing of text, which has not been structured in order to facilitate retrieval of personal data. What we need is a system that gives an effective protection for the vital interests of the data subjects' rights to respect for private and family life *and* at the same time is easier to handle on an everyday basis. I think that a new system for data protection should concentrate on preventing abuse of personal data rather than on regulating every step in the processing of such data. As I see it, there must be a shift in focus from the handling of every piece of personal information to the ultimate goal, preventing abuse. I would like to give you some examples of what I mean.

The internal handling by the controller of the file of text containing personal data, which has not been structured in order to facilitate retrieval of personal data, is seldom problematic. If the controller in fact is using the text to search for and compile information about an individual, the original principles should apply. But otherwise it is principally two situations that come into focus. Firstly, a controller should not be allowed to collect an unreasonably large amount of text about an individual without a legitimate reason. The second situation is when the controller is using text containing personal data to base a decision which significantly affects the data subject. In this situation the data subject could use his or her right of access to the data to control what personal data have been used as a basis for the decision. What is required is a right for the data subject to have the decision re-evaluated by the controller in the light of any objections raised by the data subject.

A more problematic situation is when the controller disseminates text containing personal data. I believe that most countries already have legal protection against defamation, slander and libel. What is necessary apart from that is a general protection against the dissemination of personal data to a wider audience in a way that harms the data subject. The dissemination should however be allowed, if the controller was obliged to give an opinion or if the dissemination is otherwise justifiable having regard to the public interest. As is the case today, this protection must also be balanced against the right to freedom of expression and freedom of the media.

I believe that a system construed along these lines affording protection against abuse of text containing personal data is easier to apply and understand and therefore could be respected and practiced. Twenty years ago, the production of text was excluded from the application of the principles in Convention 108 because such text was produced by non-automatic means at that time. In the same way such production, which nowadays is done by automatic processing, should be excluded today but instead be subject to more suitable rules preventing abuse. The challenge for the future is to identify such suitable rules.

Thank you for your attention.

Round Table: The regulation of transborder data flows – an appropriate guarantee?

THE REGULATION OF TRANSBORDER DATA FLOWS - AN APPROPRIATE GUARANTEE?

Paper by

Mr Ulf BRÜHANN
Internal Market
Directorate-General
Commission of the European Communities

Introduction

The issue of transborder flows of personal data is of course one of the main reasons why the European Community legislated in the area of data protection in 1995, at a time when international instruments such as Convention 108 already existed. It touches on the classic conflict between protection of personal data, that is to say, restricting the use and dissemination of such data, and the development of globalised markets which require free flow of information, including personalised information.

Is there a need for regulation of transborder data flows and, if so, which regulations provide adequate guarantees?

Need for transborder data flow regulation

The Council of Europe Convention 108 of 1981, which is at the heart of this Conference, although it saw such a need, at that time only partly answered the problem, leaving the remaining problems to be dealt with in future instruments.

It looked only at the data flows from parties to other parties of the Convention, providing for free circulation in principle but allowing for some exceptions. The Explanatory Report pointed out that this solution should be “seen in close conjunction with Chapter II which ensures that the processing of personal data is subject in all countries concerned to the same fundamental rules ("common core")”[1].

As regards the data flows to other countries, not parties to the Convention, it did not contain a rule or regulation and left it to the parties to decide whether these flows should be restricted or not. However, the absence of a rule about transfers to non-parties created the need for an exemption from the rule of free movement for transfers between parties. This was considered necessary to prevent circumvention of national restrictions of transfers to non-parties by sending personal data first to such parties which did not have similar restrictions and transferring them freely from there. Interestingly the explanatory report warned about a systematic use of this exemption and added that Parties to the Convention having a system of authorisations of transborder data flows “may decide to renounce such authorisations for example because the non-Contracting State in question has a satisfactory data protection regime”[2].

[1] Par. 21

[2] Par. 70

It is clear that in view of this situation the European Community, which was obliged by its Treaty not to provide for mere governmental co-operation on an international level, but for integration of the Member States creating a real internal market without frontiers, had to take further action to achieve this result. There could be no doubt about the route to take: if the lack of harmonisation of rules on transborder flow of data to third countries created the need to maintain restrictions on the free flow within the Internal Market, Community legislation would also need to harmonise the existing rules on transborder flow in Member States' laws and regulations. As far as the Community is concerned, this meant that because some of our Member States had existing rules which provided for restrictions of transborder flows of data, the Community had to find a harmonised solution to this problem in order to be able to ensure free circulation of data within the Internal Market.

Of course, there were good reasons for Member States to have regulated the free flow of personal data in such a way which have nothing to do with the Community, but with the concern to provide effective protection of personal data to their citizens in an open world, where data could be freely exported and re-imported using them in ways circumventing the national protection system. Another problem was the distortion that could arise where domestic companies were put in a position to compete on the domestic market with companies which did not respect similar standards of protection of personal data.

Only after the adoption and entry into force of the European Directive, an Additional Protocol to the Convention was negotiated which contained similar rules, without however deleting the exemption to the free flow as between parties to the Convention.

Adequate guarantees

If there is a need to regulate transborder data flows, there are only two solutions: either the export of the data is restricted or the destination provides in some way - which we need to discuss below - guarantees in relation to the protection of the data after the transfer.

Adequate protection systems in third countries

The first possibility was the only realistic alternative in the early days of data protection. That has changed dramatically in recent years. The European Data Protection Directive may have contributed to this development. Eminent authors argue that by combining the two solutions into a package the Community manifested its readiness to compromise. This added good reasons for many States still hesitating to go forward to provide for a system of data protection of their own. Many of the former Communist countries have enacted data protection laws including restrictions on transborder data flows. Hungary was the first of these, other countries such as the Czech Republic, Poland, Latvia, Lithuania, Slovakia and Slovenia have enacted new data protection laws.

In North America, the United States have agreed on a Safe Harbour system that is designed specifically to protect personal data received from Europe. Canada recently adopted a law providing for protection in the private sector.

In Latin America, many of the newly enacted Constitutions include *habeas data* provisions guaranteeing citizens a right to access their personal information whether held by the private or the public sector. Data protection laws are now in effect also in Argentina, Chile, Paraguay and Peru and a draft bill is pending in Brazil.

In the Asia-Pacific region, New-Zealand and more recently Australia have already adopted a law providing for data protection in the private sector. Many countries are improving protection for privacy. Japan, Malaysia and Thailand currently all have draft data protection laws under consideration.

Of course, the adequacy of such systems depends entirely on their content in terms of rights for the individuals and obligations for the organisations which have to respect them. The fact that

the Commission has already recognised the adequacy of the systems in Hungary, Switzerland and the United States does not mean that the others are not adequate, but simply that it has not yet been possible to take a decision.

In the absence of such adequate protection systems in the countries of destination, what other guarantees may provide adequate protection?

Contractual guarantees

Already in 1992, the International Chamber of Commerce, together with the Council of Europe and the European Commission developed model contractual clauses, designed to be used to provide for sufficient guarantees for individual transfers of personal data between individual exporters and importers of such data.

More recently the European Commission adopted a decision[3] which provides model contractual clauses readily usable for individual transfers of data world-wide and by companies in all sectors of economic activity. The purpose of these clauses is to create obligations by contract which have the effect of providing privacy protection for the persons whose data are transferred. In order for the protection to be appropriate – or adequate in Community language - these clauses must provide for substantive data protection rules applicable to the processing of the data after the transfer where the provisions of the directive no longer apply and measures to render the substantive rules effective. These must deliver a good level of compliance with the rules, provide support and help to the data subjects and, as a key element, provide appropriate redress to the injured party when the rules are not complied with. The model contract clauses therefore include a third-party-beneficiary clause for the data subjects to be able to enforce respect by the parties of the protective clauses of the contract, joint and several liability of the parties for any wrongdoing which has caused damage to the data subjects and a jurisdiction clause allowing the data subjects to choose among several possibilities in cases where a conflict cannot be amicably solved, for example, after intervention of the data protection authority.

The effect of the decision of the Commission is that companies can make use of the contractual clauses without authorisation from national authorities, or if such authorisation is still required, it must be given in an automatic way.

Let me finish by mentioning two alternatives for providing guarantees in view of transborder data flows:

Technological solutions

Technological solutions can make a substantial contribution to the problem of enforcement of data protection principles. If properly incorporated in soft- or hardware, users of the equipment will have little choice other than to follow the privacy guarantees provided by it – irrespective of the regulatory system applicable to them. To give just one example: Privacy filters in Microsoft's new Internet Explorer 6 force Web-sites to post new privacy policies, coded in a technical language called P3P. The filters punish Web-administrators who fail to publish properly coded privacy policies by blocking or impeding their cookies. Cookies are an important Web-feature allowing monitoring of the use of the Web-sites. The catch is that, under certain legal systems, publishing a privacy policy exposes the organisation to liability in cases of breach of the policy. However, the appropriateness of the protection provided depends of course entirely on the content of the policy in each case.

[3] Commission decision of 15 June 2001 on standard contractual cluses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ L 181 of 4 July 2001, 19 - 31

International Convention

Finally, in view of the global nature of data flows, the International Conference of the Data protection Commissioners in Venice in 2000 called for the development of an international convention which would make binding a common set of data protection principles for all those countries which would adhere.

BUSINESS PROPOSES ALTERNATIVE MODEL CONTRACT CLAUSES FOR DATA TRANSFERS FROM THE EUROPEAN UNION

Paper by

Mr Christopher KUNER[*]
ICC Special Adviser on
Data Protection, Privacy and E-business Issues
International Chamber of Commerce

The European Commission has attempted to deal with the legal uncertainty concerning international data transfers from the EU by approving on 15 June 2001 "model contractual clauses" for the transfer of personal data to data controllers outside the EU.[1] However, on 17 September, seven leading business organisations (International Chamber of Commerce (ICC), the Federation of European Direct Marketing (FEDMA), the EU Committee of the American Chamber of Commerce in Belgium (Amcham), the Japan Business Council in Europe (JBCE), the Confederation of British Industry (CBI), International Communications Round Table (ICRT), and the European Information and Communications Technology Industry Association (EICTA)) submitted an alternative set of model contract clauses to the European Commission for approval; the alternative clauses have since been formally supported by other major business organisations, such as the Union of Industrial and Employers' Confederations of Europe (UNICE).[2] This article describes the legal background of the model clauses, gives an overview of the Commission's clauses, and explains why dissatisfaction with the Commission's clauses led the business groups to submit an alternative set of clauses for approval.

The Legal Background

The EU Data Protection Directive (Directive 95/46/EC, the "Directive") restricts transfers of personal data to countries outside the European Union which are deemed by the EU not to provide an "adequate level" of data protection. It has long been clear that, as it presently stands, the law of most non-EU countries (such as the United States) does not grant "adequate protection" in the view of EU data protection regulators. Transfers of personal data outside the EU are generally allowed under the Directive only under a limited number of circumstances with commercial relevance, in particular (1) if the legal system of the country to which the data is to be transferred is deemed to offer "an adequate level of protection" for the data; (2) when the data subject has consented unambiguously to the transfer of his personal data; (3) when data controllers in Europe and controllers or processors in third counties to whom the data are transferred have concluded contracts on an *ad hoc* basis which provide adequate protection for the data, and which in many Member States must be approved by the local data protection authorities; and (4) when the transfer is deemed to be "necessary for the performance of a

[*] ckuner@mofo.com. The author was involved in drafting the alternative model clauses as a member of the ICC Working Party on Data Protection.

[1] See http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2.htm for the text of the Commission's clauses, and http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm for FAQs on them.

[2] The alternative clauses are available at http://www.iccwbo.org/home/news_archives/2001/dataflow.asp.

contract" between the data subject and the data controller.[3] Enforcement of these restrictions can range from hefty fines, to blocking the transfers.

Since all of the above solutions are either unwieldy in practice, overly expensive, or limited in their usefulness, businesses around the world have been appealing for more flexible, innovative legal bases for data transfer. One of these models is the so-called "safe harbour arrangement", which is an informal agreement between the United States and the EU concluded in the summer of 2000 which provides that transfers to United States companies adhering to certain data processing principles would be deemed to provide "adequate protection" for data transferred from Europe. However useful it is, the safe harbour cannot be the complete answer to problems arising from EU restrictions on international data transfers, since safe harbour only applies to data transfers to the United States, and businesses in Europe need to transfer data to a variety of countries around the world. Even for transfers to the United States, companies from certain important business sectors (such as many financial services companies) are explicitly excluded from joining safe harbour as it presently stands.

Background of the Model Clauses

The model clauses are designed to cure the problems arising from companies having to negotiate separate contracts between data exporters and importers and have them approved by Member State data protection authorities *ad hoc* as discussed above. Rather, the model clauses would be deemed to provide adequate protection for the transfer of personal data, so that data exporters in the EU and non-EU data importers that signed the clauses or incorporated them into their commercial contracts could be sure that that their data transfers from any EU Member State would be deemed to provide adequate protection. It is important to note that the model clauses discussed here are those for *controller to controller transfers*, that is, for transfers to a "data controller" (defined in Article 2(d) of the Directive as the entity "which alone or jointly with others determines the purposes and means of the processing of personal data"), and that they cannot be used for transfers to "data processors" (defined in Article 2(e) as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"). It is not always easy to determine whether a party to whom data will be transferred is a "controller" or a "processor", but the distinction, which is well established in EU data protection law, means, for instance, that separate contractual clauses would have to be used for transfers to a company which merely processes the data based on the instructions of the EU-based data controller (since this would be a data processor). The Commission has since proposed a separate set of model clauses to cover transfers to data processors,[4] which had not been approved at the time this article went to press.

The Commission's proposed model clauses were controversial from the beginning, not so much because of a single major problem, but because of a host of uncertainties that have, since their approval, made businesses around the world reluctant to use them. It is true that the clauses may rein in some of the more exorbitant practices of the Member States in approving *ad hoc* contract clauses, so that in effect they probably lower the present legal requirements in some Member States as well as raise them in others. Nevertheless, the clauses have so far proved broadly unacceptable to many businesses (particularly to data importers outside the EU). This is because the clauses have been drafted from a purely data protection point of view, without taking into account the commercial issues which businesses need to consider when engaging in international commercial transactions. In addition, the clauses will have to be interpreted by courts and administrative agencies in countries outside the EU with little or no experience with EU law, and it is therefore necessary that they be drafted in a way which will gain international acceptance.

The following are some of the concerns which businesses have had with the Commission's model clauses:

---

[3] In addition to the requirements for transfer under EU law, Member State legal requirements regarding notification and consent must be respected before data is transferred.

[4] Available at http://europa.eu.int/comm/internal_market/en/dataprot/news/sccprocessors.htm.

- Confidentiality concerns. The clauses do not sufficiently protect confidential data that are included in them, since they allow data subjects to be represented in complaints by "associations", which could potentially allow any sort of group to gain access to the confidential business information of the contracting parties.
- Lack of commercial viability. A number of the provisions seem out of touch with commercial reality. For instance, it is provided that the parties may never amend any detail of the contract, no matter how insignificant.
- Conflicts with domestic law of the importer. In some cases, obligations on data importers under the clauses may clash with requirements to which they are subject under their domestic law.
- Liability concerns. The Commission's draft provides for joint and several liability of the data exporter and importer in certain cases, and grants to data subjects as third party beneficiaries wide-ranging rights to sue either or both of the contracting parties on the basis of obligations which are not entirely clear. It also seems that the effects of joint and several liability may be different in legal systems outside the EU than what the Commission intended.
- Further requirements by the Member States. The clauses seem to go out of their way to invite the Member States to require that the contracting parties provide substantial additional detail about the transfer.
- Requirements going beyond the Directive. The clauses contain a number of provisions that are required by some Member States but which seem to exceed what is required in the Directive (for instance, the excessive emphasis placed on the Exporter and Importer informing the data subject that his data will be transferred to a country without an "adequate level of protection").

It was against this background that the business groups submitted the alternative model clauses to the Commission on September 17. As the Commission has always stated that approval of its model clauses is not meant to exclude the possibility of other model clauses being approved, there is no reason that the alternative clauses cannot coexist with the Commission's clauses. The alternative clauses are in no way meant to be a "light" version of the Commission's clauses; rather, the drafting approach was to begin with the Commission's clauses, but to adopt more flexible, pragmatic approach which would result in the same level of protection but using different means. The following are a few of the major differences between the Commission's clauses and the proposed alternative clauses:

- A number of extra protections for data subjects have been included. For instance, there are extra obligations on data importers (e.g., II.e: importer will, upon request, provide the exporter with evidence of adequate financial resources) and exporters (e.g., II.b: exporter must use commercially reasonable efforts to determine that the importer can comply with its obligations). Moreover, the dispute resolution clause includes an obligation on the parties to abide by a decision of a competent court or data protection authority, once all appeals have been exhausted.
- The obligations on the Exporter and Importer have been revised to exclude obligations which go beyond the Directive.
- The exporter and importer can agree that the importer will respond to requests from data subjects or authorities, but the exporter always remains ultimately responsible for doing so if the importer can not or will not (II.d).
- Provisions on auditing and inspection of the importer are more flexible and pragmatic (e.g., II.f: exporter's request must be "reasonable", more flexibility in selecting inspection agents, etc.).
- There is a more realistic provision for onward transfers (II.h).

- The liability rules reflect existing data protection law (i.e., each party is liable for damages it caused, III.a), and there is no joint and several liability. However, the combination of this principle with the extra protections included (see the first bullet point in this list) results in a level of protection which is more than adequate.
- The indemnity clause, inclusion of which is a commercial decision for the parties to make, is left as an option rather than being obligatory as in the Commission's clauses.

- The termination clause (VI.) has been brought into accord with commercial practice, also allows the possibility of temporarily suspending data flows as a step short of termination.
- Variation of the clauses is allowed to the extent it does not adversely affect data protection obligations to data subjects (VII).
- The clauses explicitly allow further transfers and multiple transfers to be covered.

The way forward

The business groups have begun negotiations with the European Commission on the alternative model clauses, and time will tell whether they will be successful. However, it is already a significant achievement that a wide variety of business groups from around the world representing different sectors were able to agree on a single set of model clauses which grant protection to data subjects that is more than "adequate" under EU law, yet still retains the flexibility which business needs if the clauses are to be used in practice. It is also possible that the same business groups may propose an alternative draft to the controller-to-processor model clauses which are presently being considered by the Commission. Just as governments work together to solve regulatory problems, so it is important that businesses from around the world have been able to agree on a single set of clauses which serve the interests of data exporters, data importers, data subjects, and data protection regulators.

LA RÉGLEMENTATION DES FLUX TRANSFRONTIERES DE DONNÉES : UNE GARANTIE APPROPRIÉE ?

Communication par

Mme Anne CARBLANC
Administrateur Principal
Division Information, Informatique et Communications
OCDE

Merci au Conseil de l'Europe et à nos hôtes polonais d'avoir organisé cette conférence importante relative au présent et à l'avenir de la Convention 108 du Conseil de l'Europe pour la protection des données à l'égard du traitement automatisé des données à caractère personnel. La valeur de la Convention 108 est largement reconnue et son approche de la protection de données, à la fois juridique, sociale, et éducationnelle demeure un modèle pour des nombreux pays.

L'Organisation de Coopération et de Développement Économiques (OCDE) a elle aussi une longue expérience de la protection de la vie privée.

Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (lignes directrices sur la vie privée) adoptées par l'OCDE en 1980 représentent un consensus international sur les principes fondamentaux relatifs au traitement des données personnelles.

Les *lignes directrices* comportent plusieurs parties relatives 1) aux huit principes fondamentaux applicables au plan national pour le traitement des données personnelles, 2) aux flux transfrontières de données, thème central de ce panel, 3) à la mise en œuvre des *Lignes directrices* au niveau nationales, 4) et enfin à la coopération internationale. Les *Lignes directrices* ont gardé leur fort potentiel international pour deux raisons essentielles : tout d'abord, parce que les principes qu'elles contiennent sont simples et technologiquement neutres, ensuite parce que le respect de ces principes par les pays membres de l'OCDE n'est pas subordonné à la mise en oeuvre d'instruments juridiques particuliers, ce qui favorise leur appropriation par des cultures différentes fondées sur la réglementation ou l'autorégulation. Cette flexibilité dans l'application des *Lignes directrices,* qui englobe l'utilisation de la technologie, a permis aux ministres de l'OCDE réunis en 1998 à Ottawa, de s'engager à assurer la protection de la vie privée sur les réseaux mondiaux de communication en co-opération avec les autres acteurs du secteur privé et de la société civile.

S'agissant des flux transfrontières de données, les *Lignes directrices* énoncent le principe de la "libre circulation" des données et l'assortissent de "restrictions légitimes". L'objectif clairement affiché dès 1980 est de concilier les valeurs fondamentales que sont la protection de la vie privée d'un côté et la libre circulation de l'information de l'autre et d'éviter ainsi de créer des obstacles injustifiés au développement des relations économiques et sociales entre pays membres de l'OCDE.

La libre circulation des données est ainsi liée au respect d'obligations positives par le pays exportateur. Ainsi les *Lignes directrices* mentionnent expressément que :

1. la sécurité des transferts doit être assurée (par référence au *Principe des garanties de sécurité* des *Lignes directrices*).
2. les pays membres doivent respecter leurs intérêts réciproques en matière de protection des données, de même que la vie privée et les libertés individuelles de leurs ressortissants.

Trois cas de "restrictions légitimes" sont prévus :
1. un pays membre peut de ne pas se conformer aux *Lignes directrices*.
2. Les données transmises vers un pays membre peuvent ensuite être réexportées (et ceci peut permettre de contourner la législation nationale).
3. Les flux peuvent concerner des données spécifiquement réglementées en raison de leur nature et pour lesquelles il n'existe pas de protection équivalente dans le pays importateur. La notion de "protection équivalente" doit s'entendre d'une protection dans les faits et pour l'essentiel semblable à celle du pays exportateur mais pas forcément identique à celle-ci, ni dans la forme, ni a tous égards. C'est en fait à une appréciation au cas par cas, qui tient compte des différences culturelles, qu'il convient de se livrer.

Les *Lignes directrices* ne font pas mention explicitement des flux entre pays membres de l'OCDE et pays non-membres. Néanmoins une interprétation *a fortiori* des dispositions mentionnées plus haut paraît raisonnable. A l'appui d'une telle interprétation peut aussi être cité le principe de responsabilité issu du paragraphe 15 des *Lignes directrices,* aux termes duquel les pays membres doivent se soutenir réciproquement dans leurs efforts en vue de s'assurer que les données personnelles ne cessent pas d'être protégées du fait de leur transfert à des territoires et des installations où le contrôle est lâche ou inexistant.

Cet ensemble de recommandations moins détaillé que la Directive européenne ou même que la Convention 108 du Conseil de l'Europe ne comporte pas pour autant de dispositions fondamentalement diffèrentes. L'approche des flux transfrontières de données adoptée dans ces trois instruments est basée sur un objectif de prévention des difficultés et non pas sur un objectif de réparation de problèmes qui seraient avérés. Cela signifie que des contrôles *a priori* et *a posteriori* sont nécessaires qui peuvent mener à une certaine bureaucratie. Mais à l'inverse, cette approche limite les grands conflits de détermination de la loi applicable au niveau international qu'entraînerait une approche uniquement fondée sur le contrôle *a posteriori*.

J'en viens à la question posée à notre panel : la règlementation des flux transfrontières des données est-elle encore une garantie appropriée ?

Certains intervenants au cours de cette journée et dans ce panel ont souligné qu'il fallait éviter de se perdre dans des détails trop juridiques et, plus spécifiquement, qu'aucun des différents moyens (y compris le consentement de la personne concernée) prévus pour garantir la protection des données personnelles en cas de transfert transfrontières ne donnait véritablement satisfaction.

Pour ma part, faisant écho à ces remarques, je dirais que la réponse à la question de savoir si les approches traditionnelles des flux transfrontières des données sont encore une garantie appropriée appelle une réponse variable selon que l'on s'attache aux flux transfrontières entre gouvernements, entre gouvernements et entreprises, entre entreprises (à l'interieur d'une même compagnie ou entre différentes compagnies) ou bien encore entre gouvernements et utilisateurs individuels ou entre entreprises et utilisateurs individuels, et enfin selon que ces échanges et ces flux ont lieu hors ligne ou en ligne.

Par exemple, l'utilisation de contrats peut être une solution appropriée, satisfaisant de manière effective à la réglementation (a priori) des flux transfrontières de données, dans le cadre de transferts inter-entreprises hors ligne ou en ligne. Il n'est pas évident en revanche que l'utilisation d'un tel outil juridique soit adaptée à la protection des données dans le cadre une relation nouée entre une entreprise et un consommateur en ligne. De même, dans cette dernière circonstance, le consentement donné par un consommateur au transfert de ses données, pour être prévu par la Directive européenne, ne constitue pas pour autant en soi une

protection réelle et suffisante. Il se peut fort bien que l'utilisation d'une technologie protectrice de la vie privée en ligne offre une garantie plus efficace et pratique.

Est-ce à dire que toute réglementation des flux transfrontières de données, notamment entre entreprises et consommateurs en ligne serait inefficace ? Non. Mais certainement faut-il aussi et en priorité :

1. Éduquer les entreprises, les personnes physiques et les gouvernements, en matière de protection de données personnelles. Il faut éduquer inlassablement sur la base de principes simples, clairs, et les plus « universels » possible. Seuls des principes de cette nature ont le potentiel d'être acceptés au plan international. Il ne faut en effet pas oublier que si la coopération entre organisations internationales est importante (OCDE/COE/CE), elle est également, à l'époque de la société de l'information, primordiale avec les pays "non-membres" de ces organisations.

2. Il faut aussi promouvoir la flexibilité dans la mise en œuvre des principes de protection des données. Enrichir les approches règlementaires traditionnelles d'une bonne dose d'autorégulation et de technologie (et vice versa) permet de préserver les sensibilités culturelles et de ce fait d'augmenter la "couverture géographique" des principes de protection des données personnelles à l'échelle mondiale sur les réseaux de communication. Il faut aussi favoriser l'échange d'informations sur ce qui marche ou sur ce qui ne marche pas.

Je conclurai que l'une des questions de base dans tout processus de négociation internationale est celle du degré d'ajustement que doit consentir chaque pays pour le « bien commun » de tous - en l'espèce la protection des données personnelles des usagers des réseaux, quel que soit leurs pays d'origine. Ce degré d'ajustement suppose un message clair, venant des pays les plus avancés dans le domaine de la protection des données, et une politique d'intégration, non pas une politique de ségrégation.

Je vous remercie.

THE REGULATION OF TRANSBORDER DATA FLOWS. AN APPROPRIATE GUARANTEE?

Paper by

Rafael Andrés LEÓN CAVERO
Lawyer and Economist
Office of the State Attorney of the Government
Ministry of Justice
Spain

I. Introductory remarks

The study of the alternative ways that legal systems may use to tackle the intricate problems posed by transborder flows of personal data is a source of passionate debate in academic and governmental fora nowadays.

In order to frame the aforementioned question, it is necessary to clarify briefly what is the social need that calls for a legal response in order to issue a proper answer.

It is widely recognised that those powers in charge of establishing and maintaining a legal system must endeavour to accomplish the difficult task of updating law and law enforcement mechanisms in order to respond to a social need, or even to try to provide a remedy against foreseeable future social problems. Otherwise grave harm to social peace and justice may arise.

Accordingly, the first question to cope with is that of determining whether there is or there may be in perspective some social need which demands a legal solution which, if left unattended, may pose grave risks to the stability of modern democratic societies. The second task must be to design the best legal answer to the problem that has been pointed out.

II. Identification and description of the social concerns with regard to transborder personal data flows

It is said that information is power. Therefore knowledge of personal data may confer their owner, if used improperly, the possibility to inflict serious harm on the life and dignity of any individual.

1. The use of personal data by governments.

As wide access to personal data was once confined to governmental organisations, the first reaction against that social problem was the fight for privacy as an individual fundamental right. It was felt that governments should have the right to gather and process personal data only on behalf of legally defined public interests, or to protect prevailing rights of their citizens and subject to scrutiny by parliament and the judiciary, but not in other cases or for different purposes.

This social need deepened as States became more and more organised and technical means began to ease processing of personal data on a large scale.

World history has dramatically recalled on several occasions that this problem was unfortunately not far from becoming a nightmare. All totalitarian governments since World War II have made extensive use of personal data to infringe the human rights of those individuals that supported different political or intellectual ideas or belonged to certain ethnic groups.

Witness to this social demand is George Orwell's famous novel "1984", written in the late 1940s. The author prophesies a future world where knowledge about personal activities and data on people becomes an ominous source of strength and power in the hands of the Government, ironically called "Big Brother". For the individual,"ignorance -of the State - is strength".

Realistically it can be concluded that this danger exists, that it has shown its potential harm in the past as it does in some parts of the world today. But, on the other hand, democratic societies have reacted by establishing safeguards to prevent it from becoming a real threat: namely by legal definition of what public interests merit an endowment of powers to the State, by setting in motion parliamentary and internal administrative activities to control the Government, and by guaranteeing a fundamental right of privacy – that may be extended progressively by jurisprudence, *consuetudo* or law to protect all personal data and confers on individuals access to the courts of justice and independent supervisory authorities in order to enforce it.

Nevertheless, it must be noted that these democratic safeguards are not properly established or strong enough in at least half of the world, so that in many parts of our planet problems on the grounds of personal data protection are still posed because governments are involved in intrusive activities without legitimate grounds.

2. The use of personal data by individuals and corporations

Lately a second concern has generated social reaction on this issue. The latest technological developments have led to the access to information by individuals and companies beyond reckoning just a few years ago. All other tasks in the processing of information have also become easier and quicker.

Moreover, the globalisation of economic and financial markets has led to the expansion of big corporations, aimed at seeking worldwide coverage of their range of activities. The largest international corporations manage budgets that are bigger than those of many countries or international organisations. Information, and specifically personal data about actual or potential customers, is - for them - money and, therefore, strength. One must not forget that market rules bluntly point to the fact that businesses need to be profitable to remain alive.

Of course this is a legitimate endeavour for a corporation that brings economic wealth to the societies where it operates so that, subsequently, it will be appreciated and protected. But it must not be forgotten that fundamental rights always take precedence over economic rights, so that the latter must never override the former. Consequently, a delicate balance must be maintained.

The risks involved in this new reality are:

a) Due to the commitment of companies to lower operational costs:

- that global businesses operate worldwide and may tend to locate processing in places where personal data protection is not ensured by the legal system and is menaced by governments. Data subjects may live in countries where data protection is guaranteed, but their personal data may "travel" to places where this is not the case. It tends to happen that in those "processing countries" labour costs

are lower, as are compulsory security measures on processing –their implementation costs-are thus low or simply do not exist. And it must be taken into account that compulsory public laws issued by those Governments may overrule any conditions that corporations may have agreed in contracts based on the general rule of civil law "*pacta sunt servanda*".

- that companies rely on short term profit schemes in order to ensure long term prevalence, so that personal data protection, regarded as an additional and not strictly necessary operational cost – what is technically known by economists as "external costs" - may not be very appealing to their leaders.

  This has happened in the past, for example, with environmental protection costs, that did not bother many industries until consumer protests and legal actions forced them to take a long-term view - if the damage was not already irreversible.

  Along these lines, we can also recall the deprivation of labour rights linked with fundamental human rights that have been recorded in factories located in poor countries, and which led to consumer protests.

b) Due to the anonymity of private corporations:

- that corporations are easy to create and the anonymity of stakeholders' identity, in some of them, may be used as a vehicle to process personal data on seemingly legitimate grounds with the secret intention of using them unlawfully. In countries that ensure an adequate level of personal data protection this does not pose greater risks than those involved in any criminal activity, but if this adds to data processing and storage in countries whose legal systems do not offer that level of protection the potential danger grows significantly. The use of "legal" corporations as cover for terrorist organisations is an undeniable and frightening reality nowadays.

- that triangular relationships via onward transfers may be used to circumvent personal data protection legislation.

These facts lead to a new social concern that has been reflected in modern culture. We can recall here, for example, the 1998 American film "The Net" by Irwin Winkler, in which a terrorist group tries to control world information sources through a company and almost ruins the personal life of the main character.

In her worst moment of anguish she affirms:

Angela: *" Ils savaient tout de moi, absolument tout. Ce que j'aime manger, ce que j'aime boire, quels films je vais voir. Ils savaient tout! Ils savaient tout! D'où vient ma famille, quelle marque de cigarettes je fumais! Ils savaient tout! Ils ont dû me surveiller sur Internet, noter le numéro de ma carte de crédit. Toute notre vie est dans des fichiers. Ces gens ont réussi à m'effacer sans qu'on s'en aperçoive... "*

We could even think forward to the potential problems posed by the development of artificial - intelligence that may lead to automated computerised decisions affecting individuals. We can recall here the impact of the confrontation between human beings and a computer in Kubrik´s film "2001, A Space Odyssey".

III. The best legal approach to answer democratic societies' concerns

From all that has been considered above we can conclude that:

- there is no danger - at least no more than that of any other activity - in countries that ensure an adequate level of personal data protection by means of an efficient response by the legal system, so that transfers between those countries should be

authorised. There is an efficient response by the legal system when public and private organisations are bound by internal and external controls to ensure compliance with enforceable personal data protection principles.

- the danger starts when personal data are to be transferred to public or private bodies that operate in countries that do not ensure a defined adequate level of personal data protection.

Hardly anyone objects to the description of the problem expressed above. The differences appear when designing the best answers that must be provided by legal systems in order to ensure personal data protection with regard to transborder personal data flows.

We will refer below mainly to transfers to private bodies operating in countries that do not offer an adequate level of data protection, which are now regarded as the main controversial issue because of the need for a balance between commercial freedoms and the fundamental rights of the individuals.

The basis of the problem is the role that democratic countries are called to play in relation to commercial activities and horizontal - individual to individual - enforcement of fundamental rights.

Those who defend the merely ancillary intervention of governments in society, only where private initiative proves insufficient because it would be unprofitable or affect the defence of the State, are in favour of a “self-regulatory” approach provided voluntarily by private corporations.

The main reason adduced by these authors is that it is unrealistic to think about future worldwide protection based on uniform detailed public and compulsory legal instruments that establish specific rights and obligations on personal data protection, because we are confronted by a global market operated by global subjects with no possible territorial boundaries.

These reasons are, in my view, not consistent, in view of the following:

- Mere internal codes of conduct, issued by private bodies, are insufficient, by themselves, to guarantee respect of data protection principles because of their lack of enforceability before the courts or the public administration when damage to the data subject has resulted from their breach.

- If we recall how the protection of human rights has spread in the past we must conclude that it began to be incorporated in the constitutional texts of very few countries (the United Kingdom, France, the United States) and that it took more than two centuries for them to expand in terms of content and enforcement mechanisms. What may have seemed an utopia in the past is now a reality in democratic countries. And we must underline that this tendency has gained significant momentum in the last thirty years. It is not true that this may not happen with respect to personal data protection when there is a social will and demand to do so.

- It is not accurate to say that it is not possible to act by means of national legislation against unlawful acts committed in an international environment. First of all, this is a typical problem of international private law. The solution has been found by establishing a link between the transaction and a national legislation. It is easy to establish that link concerning personal data, for example taking into account the place of residence of the data subject concerned or the residence of the processor established in a country that offers an adequate level of protection. The issue then becomes that of determining which are the best criteria for setting up that link. Secondly, the universal vocation of Convention 108 and its Additional Protocol could be envisaged, in the medium term, as a way of expanding data protection by actively promoting its signature worldwide.

- Private bodies that operate in a country that offers adequate personal data protection and have an international network must commit themselves to respecting rights of the individual with

the same standards of data protection when they operate in other countries. This is a way of ensuring that, in the long run, consumers will not turn their backs on them once problems have arisen due to processing conducted in dangerous political environments with lower levels of protection. It must be noted that, unlike public bodies, private bodies rely mainly on data subjects' consent in order to gather personal data, so that an adverse social climate against giving data voluntarily may result in management difficulties for companies in the long run. In fact this "consumer against business" fight has taken its first steps in developed countries that have proved reluctant to enforce personal data protection principles by law[1].

- These concerns are targeted in recent work carried out in the Council of Europe and the European Union on the use - in addition to the commercial arrangements of a transaction - of sets of contractual clauses for transborder data flows. These clauses are designed to ease data flows in a way that will expand data protection principles taking advantage, in an original legal approach, of the universal civil law principle *pacta sunt servanda*, achieving - in a way - extraterritoriality of data protection legislation of the data exporter's country. If applied properly[2], these clauses may develop customs and practices in the recipient countries that will serve social justice, helping to favour the generation of international customs on personal data protection as an additional step towards worldwide constitutional recognition of personal data protection principles as fundamental rights.

[1] We must cite e.g. the campaigns held in the USA by the Electronics Privacy Information Center against the identifier in Intel Pentium III and against abusive publicity banners on the internet by Doubleclick Co.

[2] We must remark on this issue the approval ,on 15th June 2001, of the EU Commission Decision on standard contractual clauses for the transfer of personal data to processors established in a third country that does not guarantee an adequate level of personal data protection, that deals with the key problems: applicability of the contract in the third country, third party beneficiary clause on behalf of the data subject to protect his rights, liability before him/her in case of data protection principles inserted in contractual content, access to a jurisdiction accessible to him/her.

Round Table: Mechanisms for implementing principles relating to data protection, in particular the position of supervisory authorities

THE SUPERVISORY AUTHORITY: OMBUDSMAN OR REGULATOR?

Paper by

Mr David SMITH
Assistant Information Commissioner
Office of the Information Commissioner
United Kingdom

1. Article 1 of the Additional Protocol to Convention N° 108 commits each party to providing for one or more supervisory authorities, amongst their other duties:

- to "hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence".

European Directive 95/46/EC contains a similar provision in Article 28 requiring supervisory authorities:

- to "hear claims lodged by any person, or by an association representing that person concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim".

2. What does it mean to "hear claims"? A variety of interpretations are possible but two models illustrate some of the differences in approach. The supervisory authority might act as an "ombudsman" or as a "regulator":

- *Ombudsman*: The supervisory authority concentrates on the position of the particular person from whom it receives a claim. If the authority considers there has been a breach of data protection law it seeks a remedy for the individual for example by requiring amendment to the personal data held about the individual and possibly by awarding compensation. It does not concern itself more widely with the practices of the data controller.

- *Regulation*: The supervisory authority concentrates on compliance with the law. When it receives a claim and concludes there has been a breach of data protection law it considers not only the position of the individual but a range of factors in deciding what, if any, action to take. Its concern is primarily to secure compliance with the law rather than provide a remedy for the person who makes the claim.

These models are only illustrative. Other possibilities exist and many supervisory authorities may adopt an approach somewhere between the two.

3. There are advantages and disadvantages to each model. The ombudsman may provide the greatest assistance to those who actually make claims but may find it difficult to control the allocation of resources to hearing claims. An increase in the number of claims without a corresponding increase in resources will cause backlogs and other problems. This

approach also leads the authority to concentrate its efforts on those issues it receives most claims about which may not necessarily be the most significant issues affecting data subjects as a whole. The regulator is more able to concentrate its efforts on the compliance issues that it considers of greatest significance but this may not actually address the problems faced by individuals and could leave many of those who are adversely affected by unlawful processing of personal data without an effective remedy.

4. In the United Kingdom the number of claims received has increased from under 1000 per year in the first few years of the original Data Protection Act to nearly 9000 in 2000/01. In the early years the Data Protection Register (now the Information Commissioner) was keen to raise awareness of the Act and thereby encourage claims. He was also keen to examine widely the practices of data controllers. This was understandable but meant that each claim received extensive consideration, an approach that was unsustainable as numbers increased. The approach therefore changed gradually to concentrating on the specific issue raised by the claimant and seeking to obtain a remedy for them. With the new Act, which implements Directive 95/46/EC, the approach has moved more towards the regulatory model. When claims are received the Information Commissioner determines whether it is likely or unlikely the Act has been complied with. The data subject can then use this determination in seeking a remedy from the data controller but any further action from the Commissioner depends on her assessment of the broader significance of the issues at stake.

5. This paper does not attempt to suggest which model is best only to stress the importance of a supervisory authority being clear what its role is in hearing claims. A real risk for a supervisory authority is that those asking it to hear claims expect far more from it than it is either capable of or willing to deliver. It needs to manage expectations but can not do so unless it is clear about its own role. In deciding what this role should be a range of factors need to be taken into account. These include:

- striking the right balance between encouraging individuals with data protection problems to help themselves and providing assistance to those who genuinely need it;
- understanding what those making claims actually want from the supervisory authority;
- establishing the relationship with other regulators and ombudsman, for example in the banking sector, whose remit also covers data protection issues;
- ensuring that the resources available to the supervisory authority are used to best effect;
- bearing in mind that the issues raised by those making claims may not reflect the most significant data protection issues facing the population as a whole;
- keeping the claims handling process manageable so that it is able to cope with variations in numbers;
- understanding the relationship between the enforcement powers of the supervisory authority, the rights of individuals to seek their own redress through the courts and the process of hearing claims.

6. The obligation of a supervisory authority to “hear claims” can be approached in a variety of ways. This paper does not try to suggest which is the right way. This will vary from country to country and must depend on many variables such as the extent of other rights of redress given to individuals, the enforcement powers of the supervisory authority, the legal system within which it operates and the resources available to it. What is important is that the supervisory authority knows what it is trying to achieve when it hears claims and has a system that is designed to deliver this. Without such clarity there are real risks that those making claims will expect far more than the authority can achieve and that the authority may end up concentrating its efforts disproportionately on hearing claims at the expense of its other important duties.

Round Table: International co-operation mechanisms for protecting personal data in a globalised information world

MECANISMES DE COOPERATION INTERNATIONALE POUR LA PROTECTION DE DONNEES A CARACTERE PERSONNEL DANS UN MONDE D'INFORMATION GLOBALISEE

Communication par

Juan Manuel FERNANDEZ LOPEZ
Directeur de l'Agence de Protection de données
Espagne

La coopération internationale, dans ses diverses manifestations destinées à relever les défis de la protection de données à caractère personnel, dans un monde où les notions de temps et de distance ont changé, voire perdu le sens qui leur était attribué jusque très récemment, est un sujet capital pour tous ceux qui ont la responsabilité de veiller au respect du droit fondamental à la protection de données à caractère personnel de nos concitoyens.

Cette coopération a des filières générales que nous connaissons tous et qui ont été mises en relief dans le rapport de Mme Alonso Blas: les comités établis par la Directive 95/46/CE, la Convention 108 et les Conférences Européenne et Internationale qui se tiennent tous les ans, chacune selon leurs propres règles d'admission, constituent des moyens incontournables pour la connaissance mutuelle et la coopération entre les différents acteurs intéressés par la protection de données à caractère personnel. L'Agence espagnole de la protection de données que j'ai l'honneur de diriger y a participé et y participe activement.

Mais, outre ces forums, il existe d'autres mécanismes, d'autres formes de coopération que l'Agence de protection de données a développées et qui nous semblent constituer des voies très efficaces pour augmenter les niveaux de coopération internationale.

Je parlerai tout d'abord de la coopération bilatérale avec d'autres autorités de contrôle et organismes de différents pays. Pour commencer, permettez-moi de faire référence à un événement qui s'est produit pour la première fois l'an dernier et qui va se tenir à nouveau à la fin de ce mois. Je veux parler de la Première Rencontre Ibérique des Autorités de Protection de Données que les organismes de contrôle espagnol et portugais ont tenue l'an dernier au Portugal et qui s'est avérée d'une utilité extrême, puisque pendant deux jours, dans une excellente ambiance de travail, nous avons passé en revue, d'un point de vue absolument pratique et basé sur les actions et les décisions que les deux organismes avaient menées à bien auparavant, tous les sujets les plus actuels dans les deux pays, dans le cadre de l'Union européenne et en Amérique Latine. Cette année, l'Agence de Protection de Données aura l'honneur d'organiser la II Rencontre, à la fin de ce mois.

Une autre possibilité de coopération bilatérale extrêmement intéressante est la définition d'un projet conjoint entre les autorités de contrôle et leur exécution, moyennant l'élaboration de techniques et de normes communes. Sous cet aspect, les autorités de contrôle espagnole et hollandaise ont eu l'occasion d'expérimenter les bénéfices mutuels de cette technique dans le projet sur les normes communes d'audit de protection de données qui a abouti à la réalisation d'un plan d'inspection des fournisseurs de services d'Internet ; je ne reviendrai pas sur ce plan

qui a été présenté lors des conférences européennes de Helsinki et de Stockholm et dont les résultats sont à votre entière disposition. Simplement vous dire que la coopération entre les deux équipes d'audit espagnole et hollandaise a été très fructueuse, tant en ce qui concerne l'amélioration de la connaissance mutuelle entre les deux équipes, qu'en ce qui a trait à la définition d'une méthodologie commune qui a permis et permettra aux deux autorités de comparer et de partager leur information.

Un autre mécanisme de coopération qui se développe souvent, que ce soit en vertu des prévisions d'un instrument juridique international (Directive 95/46/CE, Convention 108, Convention de Schengen) ou d'une demande d'aide provenant d'une autre autorité de contrôle et devant être traitée selon le Droit national, est celui que justifie la résolution d'un fait spécifique, une dénonciation ou une réclamation d'un citoyen, ou encore un sujet d'intérêt général affectant plusieurs pays.

Sur ce point et à titre d'exemple, l'Agence de Protection de données a eu l'occasion de collaborer avec la C.N.I.L. française pour de nombreuses demandes effectuées devant cet organisme sur l'inclusion, de la part des autorités espagnoles compétentes, de données à caractère personnel de certaines personnes, dans le Système d'Information Schengen. L'Agence espagnole a effectué les vérifications nécessaires et informé ses collègues français des résultats.
D'intéressants échanges d'information se sont produits avec d'autres autorités de contrôle, ainsi que des prestations d'assistance de nombreuses autorités de contrôle de l' Union européenne concernant les problèmes de citoyens espagnols dans l'exécution des droits d'accès, de rectification et d'annulation.

D'autre part, lors de ces contacts, nous avons pu constater l'existence de différences juridiques entre les pays, qui doivent nous obliger à poursuivre nos efforts d'harmonisation sur leur application, au sein de plusieurs forums internationaux comme le Conseil de l'Europe ou le Groupe de l' Article 29.

Puisque nous nous trouvons aujourd'hui à Varsovie, je me dois de mentionner ici la très agréable et fructueuse relation qui s'est établie au cours de ces dernières années entre l'Agence de Protection de Données et l'Inspection générale polonaise. La coopération entre nos deux autorités a culminé dans les deux visites de travail effectuées à Varsovie et à Madrid, par les délégations respectives de l'Agence espagnole et de l'Inspection Générale polonaise.

Des rencontres se sont tenues au cours de ces visites entre toutes les unités de nos deux institutions ; nous nous sommes informés sur nos méthodes de travail, notre cadre juridique et les moyens dont nous disposons pour mener à bien notre mission et bien évidemment, les carences que nos deux organismes observaient ont été abordées de façon à offrir un meilleur service à nos sociétés.

Toujours concernant la coopération avec les pays candidats à l'entrée dans l'Union européenne, je tiens à aborder ici un autre projet de coopération qui nous remplit de satisfaction. Je veux parler du Projet, qui est en fait une réalité, de Jumelage entre les autorités espagnoles de protection de données et les autorités tchèques, dans le cadre du programme PHARE.

Ce projet signifiera la présence pendant un an d'un expert espagnol en République tchèque, en qualité de Conseiller pré-adhésion, ainsi que diverses visites d'étude à l'Agence espagnole de la part de plusieurs délégations tchèques et la présence à Prague d'un nombre important d'experts à court terme, tant espagnols que d'autres états de l'UE et représentants des institutions communautaires pour leur participation à des séminaires, des ateliers et des conférences.

Ainsi, deux experts de l'Agence ont récemment dispensé un séminaire de trois jours en Bulgarie, dans le cadre d'un autre projet PHARE auquel ont participé les Ministères de l'Intérieur des deux pays.

Il convient aussi de signaler qu'il existe un flux constant d'informations par le biais d'échanges informels réalisés au cours des dernières années entre divers membres des organismes de contrôle; j'espère que ce flux augmentera encore dans l'avenir. Ces contacts informels se sont déroulés sur la base de la connaissance mutuelle acquise au cours de la participation aux divers forums internationaux et ont beaucoup augmenté grâce à l'implantation progressive d'outils qui, comme le courrier électronique, permet une communication agile et rapide entre les personnes.

Indépendamment de tout ceci, le défi auquel doit faire face la protection de données à caractère personnel est l'élargissement de l'approche que nous pourrions appeler "européenne", à savoir la considération de la protection de données à caractère personnel comme un droit fondamental de la personne humaine et donc digne d'être défendu par une législation qui en préciserait les principes essentiels et établirait les droits des citoyens dans d'autres zones géographiques.

En ce sens, les pays latino-américains sont une région du monde avec laquelle l'Europe en général, et l'Espagne en particulier, ont une relation privilégiée. Cette situation a poussé l'Agence de Protection de Données à tenir en 1997 une Conférence à laquelle ont participé des représentants de toutes les autorités de contrôle de l'Union Européenne et de la Commission Européenne. L'objectif primordial était de promouvoir une rencontre entre experts permettant des échanges d'opinions, d'idées et d'expériences sur le processus d'élaboration de dispositions juridiques et réglementaires en cette matière, qui devait se développer dans les pays latino-américains et contribuer dans le même temps à l'expérience européenne en la matière.

A la suite des délibérations ayant eu lieu, il a été décidé d'impulser devant les gouvernements des différents pays, le développement de mesures concrètes en matière de protection des personnes physiques en ce qui concerne le traitement de données à caractère personnel et de solliciter devant la Conférence des Ministres de la Justice des pays latino-américains, qu'elle introduise dans son agenda l'étude de la possibilité d'adopter une loi type relative à la protection des personnes physiques sur le traitement de données à caractère personnel et à la libre circulation de ces données.

Ces initiatives ont déjà porté leurs fruits et ces deux objectifs ont été atteints. Lors de la Conférence ministérielle des Ministres de la Justice tenue en 2000 à la Havane, une loi type en matière de protection de données à caractère personnel fut approuvée. En ce qui concerne l'adoption de législations sur la protection de données, contrairement à la situation actuelle, il n'existait pas en 1997 d'exemples de lois de protection de données dans cette région. En effet, plusieurs pays ont adopté des normes générales et sectorielles sur la protection de données et il convient de mentionner la Loi argentine de "Habeas Data" qui est actuellement en examen devant les institutions communautaires, de façon à promouvoir la déclaration d'adéquation de ce pays.

J'ai personnellement eu l'occasion de constater le sérieux de ces efforts lors d'un récent voyage de travail que j'ai réalisé dans ce pays, à l'instance du gouvernement argentin, pour participer aux débats sur l'adoption de la législation de développement de la Loi "Habeas Data" et en particulier, de celle que l'autorité de contrôle établirait dans ce pays. J'ai également eu l'occasion de visiter le Paraguay, en réponse à une invitation de l'Institut des Etudes Constitutionnelles. Nous y avons tenu des réunions avec des autorités publiques et des membres du Parlement paraguayen qui a récemment adopté une Loi de Protection de données dans le secteur de la solvabilité patrimoniale et le crédit.

Enfin et en guise de conclusion, je voudrais renouveler à toutes ces institutions liées à la protection de données à caractère personnel et tout particulièrement à toutes les autorités de contrôle, notre encouragement à rechercher une meilleure coordination capable de palier les différents niveaux de protection existant actuellement.

Comme vous pouvez l'observer, le domaine et les possibilités pour la coopération internationale sont multiples et variés et j'espère avoir pu apporter quelques éléments au débat ultérieur, sur la base de la perspective et des actions réalisées par l'autorité de contrôle espagnole.

LA CLAIRVOYANCE DES ORIGINES, DES ENSEIGNEMENTS TIRES DE L'EXPERIENCE, QUELQUES REFLEXIONS SUR LA DYNAMIQUE QUI CONSTRUIT L'AVENIR

Communication par

Mme Marie GEORGES
Chef de la Division des affaires européennes, internationales et de la prospective, Commission Nationale de l'Informatique et des Libertés (CNIL)
France

Des hommes clairvoyants, une volonté politique qui ne peut laisser pas de répit

Qu'il me soit permis, en cette année du 20ème anniversaire de la convention 108 et précisément parce que le sujet de cette table ronde concerne l'information globalisée et la coopération, de rendre un hommage particulier au Conseil de l'Europe qui dès la fin des années 70 a constitué, au-delà de la convention de sauvegarde des droits de l'homme, le laboratoire et le ferment historique de la protection des données dans le monde, en l'érigeant au plan international au rang d'un droit des personnes garanti par la loi. La réunion d'aujourd'hui dont l'hôte est l'autorité de protection des données de Pologne, prouve également qu'il a su poursuivre cette œuvre depuis la chute du mur de Berlin en direction des pays d'Europe orientale et centrale notamment par des programmes d'assistance sur le plan du droit en général et en particulier en matière de protection des données personnelles.

Mais permettez-moi aussi de rendre hommage à la coopération clairvoyante et à la qualité tant morale qu'intellectuelle et politique de ceux qui ont été les artisans de la convention 108, alors que pour la plupart d'entre eux ne sont pas parmi nous.

Une vision de l' internationale

Parce qu'il s'agissait d'établir une protection des personnes à l'égard du traitement de l'information qui s'appuyaient déjà sur des *technologies à vocation internationales*, et alors qu'ils étaient impliqués dans leur processus législatif national, les pères de la convention *ont immédiatement œuvré, en parallèle, à l'élaboration d'instruments internationaux* provoquant, dans le même temps, une synergie dès l'origine entre les lois nationales naissantes et la prise en compte de la nécessaire continuité de la protection au plan international en intervenant sur la base des mêmes principes *dans plusieurs forum internationaux au rayonnement géographique différents*. Ils ont ainsi établi des principes universellement reconnus aujourd'hui grâce à l'adoption de la convention élaborée au sein du conseil de l'Europe. Ils ont aussi, puisque les Etats Unis avaient quitté les réunions de travail du Conseil de l'Europe au motif qu'ils n'étaient qu'« observateurs » pour porter le sujet dans un cadre moins contraignant mais plus large, investi cette enceinte en vue de l'adoption de principes minimum de même nature, lignes directrices de l'OCDE. Chacun de ces instruments inclut de manière logique le principe de la coopération entre les parties. Mais quid des flux vers d'autres Etats? La convention a répondu à l 'époque en prévoyant qu'elle pouvait être ouverte à des Etats non-membres du Conseil de l'Europe

Dans un monde globalisé il peut paraître illusoire d'arrêter les flux transfrontaliers de données. Pourtant, comment accepter au plan national que la protection soit abandonnée en cas de flux

de données vers des pays non dotés de protection? Dès lors, il n'était pas inutile que l'Union européenne, en même temps qu'elle posait le principe de la protection adéquate en cas de transfert de données vers des pays tiers, ait œuvré avec succès, entre 1991 et 1994, pour obtenir au niveau le plus global, dans le cadre de l'Organisation Mondiale du Commerce, le droit d'empêcher l'accès au marché pour cause de protection des données (article XIV de l'accord général sur les tarifs et le commerce des services de 1994).

Cette dérogation au principe de la libre circulation des services a posé en réalité mondialement la question très dynamique de devoir un jour parvenir à une harmonisation mondiale sur ce sujet et donc l'obligation morale d'étendre les coopérations dès que l'opportunité se présente. Le principe de la poursuite de cette protection a été cette année également consacrée par le protocole additionnel à la convention 108 protection. Cette approche, pour nous français, paraît quasi naturelle depuis l'adoption de notre loi « informatique et libertés » en 1978 qui postule dans son article 1er « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »

La pertinence des principes élaborés toujours d'actualité

Ceux qui ont élaboré avec ténacité la convention *ont su définir des concepts et des principes de nature préventive des abus potentiels parfaitement pertinents au regard du traitement de l'information en général et donc neutres vis à vis des technologies qui le mettent en œuvre* (principe de finalité, de proportionnalité, de transparence, de sécurité…) Aussi bien nous pouvons reposer sur eux aujourd'hui encore, alors que les technologies particulières ont évolué : apparition des micros et des ordinateurs personnels, puis apparition des cartes à puces, de la télématique et de l'Internet plus récemment.

La mise en oeuvre des principes par des autorités indépendantes

Dans un tel schéma, la question de la prise en compte des situations concrètes et des technologies particulières relève de l'application des principes généraux et donc de ceux qui en ont la charge. Or, nos précurseurs ont presque tous, si ma mémoire ne me trompe pas, au-delà de l'élaboration des textes internationaux, *pris également des responsabilités importantes dans chacun de leur pays d'origine dans la mise en œuvre des principes ainsi établis, au sein des autorités indépendantes de contrôle*, Ce mécanisme qui s'est révélé essentiel, mal connu de la culture juridique européenne à l 'époque, a été reconnu tout d'abord dans les lignes directrices de l'ONU de 1990, puis en 1995 par la directive européenne et aujourd'hui par le protocole additionnel à la convention.
Outre le fait que nos précurseurs ont pu éprouver ainsi la validité des textes qu'ils avaient contribué à élaborer, ils ont donc contribué à leur *donner chaire en* les appliquant non sans *assurer d'emblée de manière efficace des coopérations entre autorités dont ils relevaient*. La convention a 20 ans, la conférence internationale des commissaires à la protection des données a 23 ans.

Leur œuvre est poursuivie. Plus de 40 pays disposent d'ores et déjà d'une législation dans le monde qui se réclament de ces instruments internationaux. *L'évolution* rapide du monde et des technologies *ne laisse pas de répit à leurs successeurs*. Chaque approfondissement de l'informatisation et de l'usage des réseaux dans tous les secteurs d'activités, chaque étape dans leur extension géographique requiert d'eux le même engagement personnel et la même acuité morale et prospective que celui qui avait animé leurs prédécesseurs.

La coopération entre autorités est indispensable et diversifiée

La coopération entre les autorités de protection des données n'est pas indépendante de la nature de la norme à faire appliquer.

Il s'agit, tout d'abord, dans *la phase d'installation d'une autorité* de coopérations destinées à ce qu'elle puisse tenir compte de l'expérience des plus anciens, tant elle est isolée, en charge

d'un droit nouveau qui s'applique à tous les secteurs d'activité sur son territoire de compétence, tant ses tâches sont diversifiées, ses interlocuteurs nombreux et ses moyens réduits. Quelles procédures mettre en place pour éviter la bureaucratie, comment s'organiser, quels personnels recruter, quels relations établir avec l'administration, les acteurs économiques, les associations, qu'elle pédagogie développer, qu'elle importance accorder aux des relations avec la presse ? etc. sont les premières questions auxquelles une nouvelle autorité doit répondre. Je me souviens d'avoir à cet égard été accueilli pendant quatre jours par l'autorité suédoise en 1979. Ultérieurement ce fut notre tour à la CNIL de recevoir ainsi des délégations, de représentants de nouvelles autorités. Dans cette phase d'installation qui peut être assez longue (peu d'autorités ont trouvé leur rythme avant plusieurs années selon mon expérience), voyage d'étude, visites, incorporation de collègues étrangers dans les équipes, opération de jumelage se sont toujours avéré des méthodes très utiles. Ces démarches doivent être encouragées et soutenues.

Unique sur son territoire de compétence, l'autorité a besoin ensuite de *confronter ses vues avec celles de ses homologues sur l'application des principes généraux aux situations concrètes et sur ses méthodes pour apprécier la justesse ou enrichir ses vues et ses démarches nationales*. Mais à quel niveau ? La réponse des commissaires a été très pragmatique. La première conférence internationale des commissaires à la protection des données s'est réunie en 1978. Mais très rapidement aussi des rencontres plus régionales se sont mises en place, entre les pays nordiques, l'élaboration de la directive européenne a également suscité le besoin d'une conférence européenne, plus récemment les autorités des pays d'Asie et du Pacifique ont formé un forum, plus récemment encore dans le sud de l'Europe des réunions se sont instaurées entre les autorités de protection des données de 'Espagne et du Portugal. La proximité de certaines difficultés qui ressort des exposés présentés au cours de cette conférence par les autorités des Pays d'Europe centrale et orientale me laisse penser que sans doute de telles coopérations entre elles pourraient s'avérer utiles et être encouragées. Mon expérience à cet égard est que contrairement à certaines idées reçues, les vues des autorités sur un même sujet sont très rapidement convergentes dans la quasi-totalité des cas. Par contre la nécessité d'établir des priorités dans les travaux à mener conduit les autorités à ne pas toujours pouvoir travailler au même moment sur les mêmes sujets. Dès lors, elles ne devraient pas hésiter à faire connaître périodiquement aux autres la liste des sujets sur lesquelles elles travaillent de manière à susciter l'intérêt des autres à leurs propres travaux. Au sein du Groupe des autorités institué par la directive européenne une telle information mutuelle se réalise grâce aux réunions tenues plus que trimestriellement qui suscitent des travaux en sous-groupe de travail composé de délégations volontaires dont il est fait rapport pour approbation au groupe dans sa formation plénière. Ces réunions sont aussi l'occasion de susciter des travaux bilatéraux : telle autorité ira par exemple, présenter devant le personnel de telle autre autorité la manière dont elle a organisé le travail interne pour l'application des principes, par exemple, aux traitements liés à l'usage d'Internet (identification des priorités, formation du personnel, contrôle sur site etc.).

Un second motif conduit à de telles coopérations. En effet les acteurs qui mettent en œuvre des traitements de données à caractère personnel opposent souvent aux autorités nationales des exemples étrangers. Dès lors *l'échange d'informations précises et la réflexion commune conduisant à l 'élaboration de doctrines partagées sont absolument nécessaires*._Cette préoccupation a été à l'origine de l'organisation de coopérations particulières sous forme de groupes de travail entre autorités en Europe dès années 80-85 dans deux domaines d'activités dont les interventions ont permis notamment dans le domaine des coopérations policières que soient inclus des principes de protection des données (accord Schengen) qui d'ailleurs font référence à la recommandation élaborée dans ce domaine au sein du Conseil de l'Europe, et dans celui des télécommunications où leurs travaux préparatoires, notamment dans le groupe de travail initié et présidé par le Commissaire de Berlin ont grandement facilité l'élaboration en parallèle de la recommandation du Conseil de l'Europe et dans l'Union européenne la première proposition de directive « télécom ».

Cette coopération en matière d'élaboration de « doctrines » communes est devenue très régulière dans tous les autres domaines notamment dans ceux les plus exposés à l'influence

l'international. Il faut constater cependant qu'actuellement en matière de « recommandation ou d'avis communs » l '*épicentre parait se déplacer vers l'Union européenne* du fait de l'institutionnalisation, dans ce cadre, d'un groupe consultatif composé des autorités de contrôles ayant un pouvoir d'initiative. *Cette coopération a été essentielle* dans les deux dernières années *pour fournir des points de repère aux acteurs et à nos gouvernants* sous forme de recommandation ou d'avis *dans les trois domaines relatifs à Internet qui nécessitaient des arbitrages non seulement nationaux mais également européen, voire mondiaux : le spam ou prospection commerciale par e mail, les données rendues publiques sur internet, la conservation des données de connexion à des fins de prévention des crimes et délits*.

Des ponts sont entrain d'être établis entre les autorités européennes des Etats de l'Union européenne et celles des Etats qui n'en font pas encore partie de manière qu'elles puissent participer à ces travaux en vue de leur accession. C'est une très bonne chose.

A l'heure de l'information globalisée et *en l'absence d'un forum mondial spécialisé*, comme il en existe dans d'autres domaines, tel que dans celui des droits d'auteur, par exemple, les autorités de contrôle de la protection des données se devaient, au-delà de la seule Europe, de s'organiser au plan mondial. De manière très pragmatique enfin lors de sa 23ème édition, *la conférence annuelle internationale des commissaires à la protection*, qui réunissait cette année à Paris 30 délégations nationales, soit des représentants de 42 autorités si l'on tient compte des Etats à structure fédérale, *s'est dotée* non d'une organisation en tant que telle, mais du moins *de règles lui permettant à l'avenir d'élaborer des positions communes sur des sujets d'intérêt général*. Celles ci, bien sûr, n'auront pas de valeur juridique, mais elles constitueront, à ce stade de la coopération internationale, pour ces autorités et la société mondialisée, des points de référence.

Enfin, ainsi que prévu dans les différents instruments régionaux et internationaux et de plus en plus fréquemment, c'est la coopération entre autorités de contrôle qui est requise pour *traiter au mieux et au quotidien les plaintes et demandes d'information des citoyens portant sur des traitements de données à caractère personnel transnationaux*. Cet exercice n'est pas toujours simple. Il dépend des pouvoirs particuliers de chaque autorité qui diffèrent assez largement mais aussi des priorités de chacune d'entre elles qui sont le plus souvent nationales. J'observe cependant de nettes améliorations en Europe. D'une part ces autorités s'attachent à mieux comprendre ces différences par des travaux en cours dans le cadre du groupe de travail « plaintes » institué par la conférence européenne des autorités de protection des données, d'autre part chacune tend à donner une plus grande priorité aux traitements des plaintes ou demandes de renseignements transmises par leurs collègues. Peu à peu, d'ailleurs, s'établit en leur sein un service dont la mission spécifique est d'assurer l'activité d'interface internationale. Ces services se connaissent entre eux de mieux en mieux et l'échange d'information sur le fond et sur les méthodes de travail s'organise.

Ceux à qui il revient de décider des budgets des autorités sont ou doivent être conscients que cette activité requiert des ressources en personnels qui ne sont pas négligeables car, on l'aura compris, la maîtrise des effets de la mondialisation signifie en pratique multiplication des travaux dans de multiples enceintes régionales et internationales et multiplication des activités quotidiennes de coopération bi ou multilatérale.

De nouvelles initiatives des Etats européens et l'intervention des organisations internationales sont également plus que jamais nécessaire et opportunes pour promouvoir la coopération dans le monde entre des pôles régionaux solides

Une quarantaine d'Etats à ce jour a pris à bras le corps dans le monde la question de la protection des données en se dotant d'instruments nationaux contraignant. Ce nombre dépasse largement celui des pays les plus industrialisés qui à diverses reprises se sont engagés encore récemment à coopérer dans ce domaine (G8 de février 1995, conférence d'Ottawa organisée avec l'OCDE en 1998).Une accélération a été constatée depuis les années 95 en relation avec *trois évènements : l'adoption de la directive européenne, les suites de la chute du mur de Berlin*

et les efforts conjugués du Conseil de l'Europe et de l'Union européenne en direction des pays d'Europe centrale et orientale, la privatisation et l'essor rapide de l'utilisation d'Internet.

Pour autant, nous ne pouvons pas nous en arrêter là. *La zone de « confiance »* ainsi créée ne suffit pas, même si elle *s'étend* déjà au-delà des pays concernés, comme par tâches d'huile, grâce aux techniques du *contrat où de l'engagement unilatéral*, inaugurées par l'autorité française en 85, reprises par le Conseil de l'Europe, consacrée ensuite, tout d'abord par la directive européenne et cette année dans le protocole additionnel à la convention 108. Ces techniques sont largement utilisées par les entreprises y compris pour établir des normes de protection des données dans les groupes d'entreprises multinationaux. J'ajoute d'ailleurs que c'est sur la base de l'engagement unilatéral conforté par les pouvoirs de la Federal Trade Commission que le système du *« Safe Harbour »* établi par le Département américain du commerce a pu être reconnu par la Commission européenne comme assurant une protection adéquate, ce qui laisse présager une coopération future avec la FTC. C'est également sur la base de *l'engagement unilatéral d'entreprises* que nous avons pu en France *donner satisfaction à des plaignants à l'égard de sites Internet établis dans des pays tiers y compris à Doubaï*. Mais dans ces cas il s'agissait de sites de très grande importance ayant établis une politique de protection des données. Qu'en serait-il s'il s'agissait de petites entreprises ou de pays n'ayant qu'une culture naissante dans ce domaine?

C'est ici que prend toute son importance l'intervention dans les phases pré législatives sous forme de coopération entre Etats que les organisations supranationales ou internationales peuvent catalyser et soutenir en s'appuyant sur l'expertise technique et l'expérience pratique accumulée par les autorités nationales de contrôle. Cette expertise est mobilisée d'ores et déjà par le Conseil de l'Europe et la Commission européenne dans des programmes d'assistance et d'expertise des projets de lois dans les pays de l'Europe centrale et orientale. Je tire de la participation à de telles missions deux enseignements : ces *missions* sont utiles mais doivent faire l'objet d'un suivi, ce qui est en général prévu tout au long du processus d'élaboration législatif. Elles conduisent à de meilleurs résultats si la mission *s'adresse à des représentants de plusieurs administrations dont les intérêts peuvent être antagonistes*. Ces missions pourraient pour un plus grand bénéfice des pays en cause, me semble - t – il, *s'adresser également au secteur privé, au milieu associatif ainsi qu'à des responsables parlementaires*.

Je voudrais aussi insister sur *deux questions qui paraissent des plus difficiles à faire mûrir lors de ces missions* alors qu'elles sont primordiales en pratique, tout d'abord celle de *l'indépendance des autorités de contrôle*, peu précisée pour des motifs évidents dans la directive européenne 95/46 mais pour laquelle certains critères utiles ont été précisés dans le protocole additionnel à la convention 108. Pour autant sur le terrain ces notions sont essentielles. La seconde l'application des principes de protection des données *dans le secteur de la sécurité et des fichiers de police* alors même que leur couverture n'est pas obligatoire dans la convention 108 et qu'elle est hors champ du droit communautaire. Ces missions doivent prévoir un temps suffisant pour traiter de ces questions.

Enfin, la préparation de la 24ème conférence internationale qui s'est tenue fin septembre à Paris, malgré les événements du 11 septembre, a été l'occasion de constater que dans la perspective ouverte par les accords du GATTs, par les dispositions relatives aux pays tiers de la directive et du protocole additionnel, la prise de conscience des dirigeants de ce monde en matière de protection des données dépassait aujourd'hui largement le cercle de ceux des pays nantis ou occidentaux. Des témoignages de telles préoccupations émergent en effet en Amérique latine mais également en Afrique, par exemple au Burkina Fasso, au Mali, au Sénégal, en Afrique du sud. Sans doute sommes-nous aussi nombreux ici à pouvoir témoigner des nombreuses visites reçues de délégations de pays des plus éloignés, comme la Corée et même la Chine. Mon sentiment est que la période paraît tout à fait favorable pour une extension géographique de la problématique de la protection des données *sous le double effet des progrès de la démocratie et de l'informatisation des administrations d'une part, d'autre part du commerce électronique, mais également d'un « réflexe » protection des données qui appartiendrait maintenant à la culture au moins des dirigeants de la quasi-totalité des pays de la planète.* Dès lors *il conviendrait d'examiner les mécanismes de coopération qui devraient être*

développés en direction des pays des continents pour le moment encore peu impliqués. Passer du « réflexe », en effet, à la compétence n'est pas simple et mérite assistance comme nous le savons ici. L'Europe détient une très grande responsabilité dans le soutien à cette extension du mouvement non seulement du fait des dispositions qu'elle a adoptées en matière de flux vers les pays tiers mais également de la très grande expérience qu'elle a accumulée dans le domaine.

Nos gouvernants et les organisations internationales peuvent compter, j'en suis sûre, sur toutes les autorités de protection des données pour contribuer au plan technique à toute initiative diplomatique et de coopération allant dans ce sens et contribuant à constituer dans le monde des pôles régionaux solides. Ces pôles régionaux pourront par la suite coopérer entre eux pour l'élaboration de « doctrines » communes d'application des principes de protection des données et la résolution des problèmes soulevés par les plaintes transfrontalières au plan mondial comme nous le faisons d'ores et déjà entre nous en Europe.

www.cnil.fr, www.paris-conference-2001.org
www.europa.int.eu/comm/internal_market rubrique « protection des données »
www.legal.coe.int/dataprotection

INTERNATIONAL CO-OPERATION MECHANISMS FOR PROTECTING PERSONAL DATA IN A GLOBALISED INFORMATION WORLD

Paper by

Giovanni BUTTARELLI
Secretary General of the
Garante per la protezione dei dati personali
Italy

We are approaching the conclusion of this conference. Many legal provisions and national experiences were commented on, both today and yesterday, either orally or in writing. Therefore, you should now be well aware that providing mutual assistance and cooperating between ourselves are veritable obligations for *all* of our authorities – not only in the light of Article 13 of Convention 108, but in the spirit of the Additional Protocol to the Convention
.
For this reason, it may be more profitable to spend the ten minutes allotted to my intervention in submitting for your attention – also with a view to the final session this afternoon – a few simple proposals concerning co-operation mechanisms rather than to continue commenting on this or that provision in force within the framework of the Council of Europe, the EU, OECD or the various conventions on joint supervisory bodies.

We are invited, day after day, to participate in a number of meetings and initiatives, in particular in Strasbourg, Brussels and Paris – so much so that one might say jokingly that we are practically in a permanent European meeting with some intervals at national level. And I am not referring here to the other various European, regional and worldwide conferences of data protection authorities.

Seriously speaking, and keeping in mind the last ten years' experience, it is high time we considered whether our practical mechanisms for co-operation are actually the best possible ones.

My impression is that in an increasingly globalised world, we are like good cousins in a very friendly club, whose membership increases year by year; however, we are not fully familiar with what happens in different countries.

What I now would like to suggest is to ameliorate our co-operation from two standpoints, that is to say in terms of knowledge and of protecting privacy.

What do I mean by co-operation in terms of knowledge? We are in general sufficiently informed as to the existence of a legal system of data protection in other countries and of its main features – that is to say, the existence of a data protection act, its scope of application, data subjects protected, and so forth. There are, however, a few difficulties in obtaining precise information rapidly as regards details and technicalities if we need – as we often do – to go into detail.

For example, how many colleagues are familiar with the existence of provisions recently enacted in Italy concerning historical research, or private investigators, genetic data, access to evaluation data, right of access to traffic data related to telephone calls?

You all know how difficult it may sometimes be to agree on the contents of a questionnaire intended for circulation, or even to obtain information from a colleague in another authority. This means that it is as yet rather difficult to disseminate information in other countries on a legal model that has been tested successfully in a specific sector and in an individual country.

In other words, it is high time we devised additional solutions rather than the exchange of oral and written information during a conference or a *tour de table*. Furthermore, there is another reason why we should be thoroughly informed about the operation of other legal systems. Only think, for instance, of the fact that under the European directive, in particular under the principle of establishment and Article 4 a) and c), each data protection authority is competent in its respective territory even if domestic law is not applicable to the processing of personal data.

And let me finally tell you that we are sometimes left alone, at national level, in taking decisions on complaints that are related to important issues.

I have no magic recipe to propose. I would only like to share a few suggestions that might "make the difference" in the near future. What I propose is to open a discussion on *certain* instruments and tools, which might help improve our co-operation.

Firstly, the globalised processing of personal data requires the establishment of a new *network* of data protection authorities. In this perspective, we suggested bilaterally to a few colleagues that an Intranet could be set up including all European data protection authorities based on pre-defined classification codes applying to the most important regulations, documents and court decisions at national level. This project would not appear to be excessively difficult to implement, also in the light of the support that could be possibly provided by EU institutions.

Secondly, many efforts are expected to be made in order to achieve stepwise harmonisation of our external Web sites - with particular regard to their overall structure and the possibility of publishing online workshops and pre-recorded lectures concerning scheduled issues; the latter would be somewhat larger in scope than the traditional FAQs, being short interactive classes in which a specific topic would be addressed from a legal standpoint.

Thirdly, common dossiers and booklets might be published jointly in order to promote the concept of a common European right to privacy – a sort of *droit commune à la protection de la vie privée*. Can you imagine, for instance, the impact of a booklet or book published jointly in different languages by all European data protection authorities, and subsequently circulated in each country?

As I said before, I am also convinced of the need to ameliorate the mechanisms put into practice to cooperate in protecting privacy. We need to increase and improve the exchange of opinions and information in this sector of our activity as well.

There is no need to stress how important it is today to be provided with timely, updated information on national findings concerning the adequacy of protection in a third country system. This information will also be crucial, in the near future, in connection with applying the Commission's decision on contractual clauses – for instance, in order to check whether the data importer actually complies with the clauses agreed upon.

Additionally, I am especially mindful of the efforts that will have to be made in the next few months once the panel of data protection authorities has been established as provided for by FAQ No. 5 in the Safe Harbour Privacy Agreement.

Thus, in order to enhance our co-operation in protecting privacy, I would consider that the greatest importance should be attached to identifying a single contact point at national level, within each of our authorities, so as to simplify relational activities and the exchange of information and communications. This may appear a poor suggestion, but let me tell you that much time is often wasted in establishing telephone or e-mail connections when there are no

personal, friendly relationships in place. I think that the Council of Europe could play an important role in this context, beyond and apart from the fact that this is provided for by Article 13 of Convention No. 108.

I would now like to add a final suggestion.

When I started toying professionally with data protection, over ten years ago, I was struck by the prestige and moral standing of the various groups at the Council of Europe – which were supported by the competence of really independent minds, people who had been working for years on the development of important principles and concepts. I still believe that the Council of Europe should continue playing this role in the near future, as it gives real added value to data protection. For this reason, I hope that a few physiological, fully understandable difficulties – of a budgetary nature, or else related to delegates' turnover – will be presently overcome.

At the same time, I feel it necessary to call upon each Authority to enhance the quality and level of its contribution to the activities and meetings of the Council of Europe in order to make its action even more effective.

In this sense, I am sure that we all agree that the Council of Europe is not regarded as a foreign body, but as a living organism born out of the passionate commitment and the intellectual efforts of all of us.

Round table: The individual's means for protecting his/her personal data and asserting his/her rights in the context of globalisation

LA PROTECTION DES DONNEES ET LA CONVENTION EUROPEENNE DES DROITS DE L'HOMME. ENTRE EFFECTIVITE ET COMPLEMENTARITE

Communication par

Mme Françoise TULKENS
Juge à la Cour européenne des droits de l'homme*

Je remercie très vivement le Conseil de l'Europe et Mme Kulesza, Inspecteur général de la Pologne pour la protection des données à caractère personnel de cette invitation à participer à l'anniversaire de la Convention 108 à laquelle je souhaite longue et belle vie. Je vous remercie aussi d'avoir organisé ce séminaire dans cette belle ville de Varsovie, une ville du cœur et de l'esprit.

Dans votre cénacle d'experts - dont je ne suis pas, puisque dans ma vie professionnelle antérieure, avant de rejoindre la Cour, j'étais professeur de droit pénal et de criminologie à l'Université de Louvain (Belgique)- j'interviendrai au départ des préoccupations qui sont les miennes aujourd'hui. Ce sont celles des droits de l'homme *inscrits* dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et *garanti*s par la Cour européenne des droits de l'homme que j'ai le redoutable honneur de servir comme juge à la « nouvelle » Cour européenne qui est entrée en fonction le 1er novembre 1998.

Dans ce contexte, je diviserai cette brève intervention en deux parties. La première partie sera générale et tentera d'identifier les points de rencontre entre la Convention européenne des droits de l'homme et la protection des données à caractère personnel. La seconde partie sera particulière et présentera les orientations récentes de la Cour en cette matière, à partir de l'arrêt *Rotaru contre Roumanie* du 4 mai 2000.

Je voudrais toutefois présenter mon intervention dans un certain esprit. La reconnaissance des droits de l'homme est inséparable des mécanismes qui permettent d'en assurer le contrôle, d'en assurer la mise en oeuvre. A cet égard, il y a pour moi deux points forts : l'effectivité dans la protection des droits fondamentaux et la complémentarité entre les instruments qui contribuent à cette protection.

I. Les points de rencontre entre la Convention européenne des droits de l'homme et la protection des données à caractère personnel

La Convention européenne des droits de l'homme se déploie sur un double registre : les droits garantis (A), la garantie des droits (B).

* Cour européenne des droits de l'homme, 67075 Strasbourg Cedex.
Tel. +33.3.88.41.35.83 - Fax. +33.3.88.41.27.30 - E-mail : Francoise.Tulkens@echr.coe.int

A. Les droits garantis

1. En ce qui concerne, tout d'abord, le contenu des droits garantis, il n'y a pas dans le texte de la Convention européenne des droits de l'homme de droit propre, général et déterminant à la protection des données à caractère personnel. Toutefois, cette matière ou, plus exactement, ce domaine est susceptible d'être interrogé au regard d'autres dispositions de la Convention : l'article 6 qui concerne le procès équitable, l'article 8 qui concerne le droit au respect de la vie privée et familiale, l'article 10 qui concerne la liberté d'expression (même si certains estiment que cette disposition est utilisée à l'excès), l'article 13 aussi qui prévoit le droit à un recours effectif. Par ailleurs, conformément aux principes généraux qui dominent la Convention, ces dispositions sont appelées à faire l'objet d'une interprétation dynamique, ouverte, évolutive de ces droits, interprétation qui est au coeur de l'effectivité des droits fondamentaux (art. 1er).

Dans ce contexte, la question qui se pose ici est la suivante. Faut-il, en ce qui concerne la protection des données à caractère personnel, un droit propre dans le cadre de la Convention européenne des droits de l'homme ? Cette question est à « lire » à la lumière des raisons qui, historiquement, ont justifié la création de la Convention 108 et des considérations qui sont actuellement développées quant au futur ou l'avenir de celle-ci[1]. Quelle que soit l'issue de ce débat, il convient de rappeler qu'un triple critère s'impose à la reconnaissance d'un droit fondamental : son importance, son universalité et sa justiciabilité.

2. En ce qui concerne, ensuite, les obligations que le respect de ces droits impose, si traditionnellement, ce sont des obligations négatives qui incombent aux États - ne pas entraver l'exercice des droits et libertés-, nous savons que la Cour reconnaît de plus en plus des obligations positives afin d'accroître le caractère effectif des droits reconnus. Ainsi, pour prendre un arrêt récent, l'intérêt majeur de l'arrêt Z. contre le Royaume Uni rendu par la Grande Chambre le 10 mai 2001, qui confirme aussi que l'article 3 de la Convention est applicable aux relations interindividuelles, est précisément de faire peser sur l'état l'obligation positive de protéger les personnes placées sous sa juridiction contre les mauvais traitements administrés par les particuliers. Mais il y a d'autres exemples de ces obligations positives qui sont des compléments naturels à l'effectivité des droits garantis. Ainsi, dans certains cas, une aide juridique s'impose pour que l'accès au droit soit réel (art. 6), une enquête effective sur les circonstances de la mort est nécessaire pour s'assurer qu'il y a eu respect du droit à la vie (art. 2) ou encore une obligation de donner des informations est essentielle pour donner sens au droit au respect de la vie privée.

3. Enfin, à qui ces obligations s'imposent-elles ? La Convention s'applique, bien sûr, de manière verticale, en ce sens qu'elle doit assurer la protection de l'individu par rapport à l'État. Toutefois, dans la jurisprudence récente de la Cour, nous voyons des exemples de plus en plus nombreux d'application horizontale de la Convention, lorsque la violation des droits garantis provient de groupes privés : la responsabilité de l'État peut, dans certains cas, se trouver engagée lorsqu'il y a des manquements des pouvoirs législatifs, judiciaires ou des autorités administratives. Dans le domaine de la protection des données à caractère personnel, cette dimension revêt une importance considérable.

B. La garantie des droits

1. Dans le cadre de la Convention européenne des droits de l'homme, le mécanisme de contrôle est celui de la Cour européenne des droits de l'homme, une juridiction internationale par définition. Ce contrôle a sa logique propre et c'est précisément dans cette perspective qu'il importe de penser et d'articuler la complémentarité entre les mécanismes de protection.

Le contrôle de la Cour européenne des droits de l'homme est un *contrôle judiciaire*, un contrôle entièrement judiciaire depuis la réforme introduite par le Protocole n° 11 qui a fusionné la Commission européenne des droits de l'homme et l'ancienne Cour en une nouvelle Cour unique et permanente. Ce contrôle est fondé sur le *recours individuel*, lui aussi développé et

[1] P. De Hert et E. Schreuders, *The relevance of Convention* 108, pp. 9 et sv.

amélioré par le Protocole n° 11 qui permet désormais à chaque individu, chaque personne - huit cent millions aujourd'hui dans la grande Europe, la « maison commune » du Conseil de l'Europe- de saisir directement la Cour, sans autre filtre que celui des conditions de recevabilité de la requête parmi lesquelles, bien sûr, l'épuisement des voies de recours internes (art. 35). Le droit de recours individuel est la force et le caractère unique du contrôle de la Cour et il ne devrait jamais être abandonné.

Mais, ce caractère unique et spécifique du mécanisme de contrôle de la Cour entraîne des conséquences ou, plus exactement, contient certaines limites.

La Cour ne s'attache qu'à des *cas individuels* et ne peut donc atteindre des situations générales ni structurelles. De même, elle ne peut intervenir que si elle est *saisie*, par une personne, un groupe de personnes ou une organisation non gouvernementale (ONG) qui peuvent se prétendre « victime » d'une violation de la Convention (art. 34). Dans le domaine de la protection des données, une question sensible est celle des personnes morales. Je pense peut-être moins aux sociétés commerciales qu'aux associations, aux syndicats ou à différentes organisations : ainsi, par exemple, si leurs prises de position, notamment dans les médias ou pendant des manifestations, sont recueillies et conservées, peuvent-elles invoquer la garantie de l'article 8 ? La Cour ne s'est pas encore prononcée directement sur cette question mais elle pourrait sans doute être amenée à le faire, à la lumière notamment de l'arrêt Goodwin contre le Royaume-Uni du 27 mars 1996 où la Cour estime que le but légitime de nature à justifier des restrictions à la liberté d'expression est la protection du secret d'affaires d'une entreprise (§ 42) ou encore de l'arrêt Comingersoll S.A. contre Portugal du 6 avril 2000 (§ 35). La Cour ne peut, dans cette perspective, intervenir que *a posteriori*, et parfois dans un délai relativement long après les faits. Enfin, son action se meut sur le plan de la *sanction*, de la répression et non pas celui de la prévention ou de la conciliation.

2. Il est évident, en raison de cette spécificité de l'intervention de la Cour européenne des droits de l'homme, que son contrôle n'épuise pas le champ des contrôles possibles et qu'il doit s'articuler, de manière complémentaire, avec les autres mécanismes de protection. En l'espèce, il s'agit du mécanisme de contrôle mis en place par la Convention 108 et le Protocole additionnel à cette Convention qui renforce les autorités de contrôle, notamment dans la ligne de l'arrêt Gaskin contre Royaume-Uni du 7 juillet 1989. A cet égard, il serait sans doute utile de poursuivre la suggestion du professeur De Hert de se livrer à une analyse comparative plus poussée des deux régimes de protection.

Je pense cependant qu'il faudrait aller plus loin et souhaiter non seulement une complémentarité entre ces mécanismes de protection et de contrôle mais aussi une interaction, une synergie entre eux, en ce sens que l'un pourrait renvoyer à l'autre, l'un pourrait renforcer l'autre et participer ainsi à l'élaboration d'un véritable droit international des droits de l'homme dans le domaine de la protection des données à caractère personnel. *A contrario*, ce qu'il importe d'éviter c'est que la multiplication des mécanismes de contrôle n'entraîne, en raison d'une ignorance réciproque, une forme de « compartimentalisation » des droits.

Dans l'état actuel des choses, je constate que certains arrêts récents de la Cour évoquent la Convention 108 et y renvoient. Ainsi, l'arrêt Z. contre Finlande du 25 février 1997 se réfère directement à la Convention 108 pour fonder son affirmation selon laquelle le législateur interne doit offrir des garanties pour empêcher la divulgation d'informations qui seraient contraires au droit garanti par l'article 8 de la Convention. De même, dans l'arrêt Amann contre Suisse du 16 février 2000, la Cour adopte une conception extensive de la vie privée en précisant que celle-ci « concorde » avec la Convention 108 dont le but est de garantir à toute personne physique le respect de ses droits et libertés et notamment de son droit à la vie privée à l'égard du traitement automatisé des données à caractère personnel (§ 65). Il en va de même dans l'arrêt Rotaru contre Roumanie du 4 mai 2000 que nous examinerons plus en détails au point suivant (§§ 57-60).

II. Les avancées de la jurisprudence récente de la Cour européenne des droits de l'homme

J'évoquerai la jurisprudence récente de la Cour européenne des droits de l'homme à partir de l'arrêt le plus récent qu'elle a rendu en cette matière, l'arrêt Rotaru contre Roumanie du 4 mai 2000, qui soulève des griefs au regard des articles 8, 13 et 6 de la Convention. C'est un arrêt que je qualifierai volontiers de pédagogique et qui permet à la fois de montrer la manière dont la Cour exerce son contrôle et de prendre la mesure des évolutions qui se dessinent. Le commentaire de cette décision par O. De Schutter me servira, en partie tout au moins, de fil conducteur[2].

Rappelons brièvement les faits. Entre 1946 et 1948, le requérant avait exercé des actes de résistance au régime communiste qui se mettait en place et il avait été condamné pénalement. Après la chute du régime en 1989, sur base du décret n° 118 du 30 mars 1990 qui accordait certains droits aux personnes persécutées par le régime communiste et qui n'avaient pas eu d'activités fascistes, le requérant engage une procédure judiciaire devant les tribunaux roumains. Au cours de celle-ci, le ministère de l'Intérieur transmet au tribunal une lettre du 19 décembre 1990 du SRI (Service roumain de renseignements) indiquant, outre les activités de résistant menées par le requérant dans les années 1940, le fait que pendant ses études en 1937 (il avait alors seize ans), il avait été membre d'un mouvement de type « légionnaire », une organisation paramilitaire d'extrême droite, nationaliste et antisémite. Après différents recours, cette information fut déclarée fausse par la cour d'appel de Bucarest dans un arrêt du 25 novembre 1997. Néanmoins, il semble que cette lettre soit toujours consignée dans les fichiers du SRI et que l'arrêt de 1997 n'y est pas mentionné. Le requérant se plaint que le SRI détient et peut dès lors utiliser à tout moment des données sur sa vie privée, dont certaines sont fausses.

A. Je commencerai par le débat autour de l'article 8 de la Convention que la Cour a déjà eu l'occasion d'évoquer dans l'arrêt M. contre Suède du 27 août 1997 : « la protection des données à caractère personnel (...) revêt une importance fondamentale pour l'exercice du droit au respect de la vie familiale et privée » (§41).

En l'espèce, la Cour va examiner successivement l'applicabilité (1) et l'observation de l'article 8 de la Convention (2).

1. Le gouvernement contestait l'applicabilité de l'article 8 de la Convention en faisant valoir que les informations mentionnées dans la lettre du SRI ne relèvent pas de la vie privée du requérant mais de sa vie publique. « En effet, en décidant de mener des activités politiques entre1946 et 1948, l'intéressé a implicitement renoncé à l'anonymat inhérent à la vie privée » (§ 42). En outre, l'interrogatoire par la police et le casier judiciaire sont des informations par nature publiques.

En fait, sous cette forme, cette question était relativement nouvelle. En effet, la Commission européenne des droits de l'homme avait, dans certaines décisions, conclu qu'il n'y avait pas ingérence dans la vie privée soit lorsque les renseignements collectés, bien que constituant des données à caractère personnel, ne renfermaient pas de données relatives à la vie privée[3], soit encore lorsque la personne ne tenait pas à la confidentialité des données recueillies (ainsi par exemple une personne photographiée par une vidéosurveillance pendant qu'elle participait à une manifestation publique). Même l'arrêt Leander contre Suède du 26 mars 1987, estime O. De Schutter, laissait « subsister un certain doute » en dépit du principe énoncé selon lequel « la mémorisation dans un registre secret et la communication de données relatives à la vie privée entrent dans le champ d'application de l'article 8 » (§ 48)[4].

---

[2] O. De Schutter, « Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel », observations sous Rotaru c. Roumanie, 4 mai 2000, *Revue trimestrielle des droits de l'homme*, 2001, pp. 148 et s.

[3] *Ibid.*, p. 151 ; Comm. eur. dr. h., 9 septembre 1992, F. Reyntjens c. Belgique, D.R. 73, p. 136.

[4] *Ibid.*, p. 153.

Pour résoudre cette question, la Cour organise son raisonnement en deux temps. La Cour va, tout d'abord, prendre appui sur une conception large de la vie privée dont les arrêts Niemietz contre Allemagne du 16 décembre 1992 (§ 43) et Halford contre Royaume-Uni du 25 juin 1997 (§ 42) offrent des illustrations très nettes[5]. En fait, elle souligne à nouveau (comme dans l'arrêt Amann contre Suisse du 16 février 2000), la concordance entre cette interprétation extensive et celle de la Convention 108 dont le but est de garantir à toute personne le respect de son droit à la vie privée à l'égard des données à caractère personnel le concernant (art. 1), ces dernières étant définies comme « toute information concernant une personne physique identifiée ou identifiable » (art. 2). Dans cette perspective, et c'est le second temps, la Cour estime que « des données de nature publiques peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics » (§ 43).

Quel est l'effet de ce raisonnement ? Il en résulte que la distinction public / privé s'estompe dans une conception élargie, intégrée de la vie privée. La protection de l'article 8 de la Convention est identique qu'il s'agisse de la sphère privée ou de la sphère publique.

Pour O. De Schutter, dans la ligne des arrêts Amann contre Suisse du 16 février 2000 et Tsavachidis contre Grèce, du 21 janvier 1999 (règlement amiable) qui ont « préparé le terrain », « l'arrêt Rotaru peut être considéré comme le premier arrêt dans lequel l'applicabilité de l'article 8 de la Convention est déduite du fait que l'on se trouve en présence d'un traitement de données à caractère personnel, indépendamment de la question de savoir si ces données sont, en outre, relatives à la vie privée de l'individu, c'est-à-dire sans qu'il importe de déterminer si les renseignements concernent des activités de l'individu à la publicité desquels il a délibérément consenti ou non »[6].

En définitive, il s'opère ainsi un rapprochement dans le domaine d'applicabilité de l'article 8 de la Convention européenne des droits de l'homme et de la Convention 108 qui contiennent des garanties parallèles mais non pas identiques. Alors que la Convention 108 s'attache à la protection des données à caractère personnel à l'égard du traitement automatisé des données, l'article 8 de la Convention semble plus large puisqu'il est susceptible de concerner toute forme de traitement de données à caractère personnel, y compris les traitements manuels de fichiers contenant des données à caractère personnel (Z. contre Finlande, arrêt du 25 février 1997).

2. Pour déterminer si, quant au fond, il y a ou non violation de l'article 8 de la Convention, la Cour va adopter, au regard de l'article 8 § 2, sa démarche habituelle : existence d'une ingérence (a) et justification de l'ingérence (b).

a. En ce qui concerne l'existence d'une ingérence, cette démarche est contestée par O. De Schutter qui estime qu'elle aurait pu être évitée. En raison de l'extension de la notion de vie privée, la Cour aurait pu dire « que toute forme de traitement de données à caractère personnel constitue une ingérence dans le droit au respect de la vie privée dont la compatibilité est subordonnée au respect des conditions fixées à l'article 8 § 2, sans qu'il faille déterminer si ces données concernent des activités privées ou publiques puisque, dans les deux cas, on est toujours en présence d'une manifestation de la vie privée »[7].

La Cour n'a pas suivi cette démarche et elle rappelle que « tant la mémorisation par une autorité publique de données relatives à la vie privée d'un individu que leur utilisation et le refus d'accorder la faculté de les réfuter, constituent une ingérence dans le droit au respect de la vie

---

[5] Sur la notion de vie privée, voy. Fr. Sudre, « Les aléas de la notion de vie privée dans la jurisprudence de la Cour européenne des droits de l'homme », *Mélanges en hommage à L.-E. Pettiti*, Bruxelles, Bruylant, 1998, pp. 687 et s. ; O. De Schutter, « La vie privée entre droit de la personnalité et liberté », *Rev. trim.D.H.*, 1999, pp. 827 et s.

[6] O. De Schutter, « Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel », *op. cit.*, p. 165.

[7] *Ibid.*, p. 165.

privée garanti par l'article 8 § 1 de la Convention » (§ 46). Outre les décisions déjà citées, elle se réfère aussi à l'arrêt Kopp contre Suisse du 25 mars 1998 (§ 53).

b. Quant à la justification de l'ingérence, il s'agit de déterminer si l'ingérence ainsi constatée dans la vie privée du requérant peut se justifier au regard du paragraphe 2 de l'article 8 et, dans cette démarche, l'interprétation doit suivre une voie étroite. En fait, nous nous trouvons ici dans une situation qui peut être mise en parallèle avec le principe de loyauté et de licéité inscrit à l'article 5 de la Convention 108.

L'ingérence était-elle prévue par la loi ? La Cour va se focaliser sur un point, celui de la qualité de la loi, « en recherchant en particulier si le droit interne fixait avec une précision suffisante les conditions dans lesquelles le SRI pouvait mémoriser et utiliser des informations relatives à la vie privée du requérant » (§ 56). En l'espèce, elle constate « qu'aucune disposition du droit interne ne fixe les limites à respecter dans l'exercice de ces prérogatives » (§ 57). La Cour estime qu'elle doit aussi se convaincre de l'existence de garanties adéquates et suffisantes contre les abus car « un système de surveillance secret destiné à protéger la sécurité nationale risque de saper voire de détruire la démocratie au motif de la défendre » (§59). Il est significatif d'observer ici que la Cour fait référence à l'arrêt Klass et autres contre Allemagne du 6 septembre 1978 (§§ 49-50). En l'espèce, « la Cour relève que le système roumain de collecte et d'archivage des informations ne fournit pas de telles garanties, aucune procédure de contrôle n'étant prévue » (§ 60). Dans ces conditions, la Cour en conclut que « la détention et l'utilisation par le SRI d'informations sur la vie privée du requérant n'étaient pas prévus par la loi, ce qui suffit à constituer une méconnaissance de l'article 8. Au surplus, cette circonstance empêche la Cour de contrôler la légitimité du but recherché par les mesures ordonnées et si celle-ci était, à supposer le but légitime, nécessaire dans une société démocratique » (§ 62).

L'opinion concordante du juge Wildhaber, à laquelle sept juges ont déclaré se rallier, complète en quelque sorte cette analyse « inachevée » : « quand bien même un fondement légal prévisible aurait existé dans cette affaire, la Cour aurait néanmoins dû conclure à la violation de l'article 8, soit au motif qu'aucun but légitime ne justifiait de continuer à tenir un système abusif de fichiers secrets, soit parce que cette mesure n'était manifestement pas nécessaire dans une société démocratique » (page 29).

B. Le requérant se plaint que l'absence de tout recours devant une instance nationale pouvant statuer sur sa demande visant à faire détruire le fichier qui comportait des données à son sujet et à y faire modifier les données inexactes est contraire à l'article 13 de la Convention. Sous cette forme, ce grief reprend la question du droit d'accès aux informations récoltées qui constitue un aspect du droit à un recours effectif garanti par l'article 13 de la Convention.

La Cour conclut que le requérant a été victime d'une violation de l'article 13 dans la mesure où elle « n'a pas été informée d'aucune autre disposition en droit roumain permettant de contester la détention, par les services de renseignements, de données sur la vie privée du requérant ou de réfuter la véracité de ces informations » (§ 72).

Toutefois, cette conclusion ne remet pas en cause la possibilité pour les États de prévoir, en outre, un mécanisme de contrôle objectif, notamment lorsque le traitement en cause a lieu dans le cadre d'une surveillance secrète. Il s'agit de la doctrine inaugurée par l'arrêt Klass et autres du 6 septembre 1978 (§ 67) et qui est conforme aux exigences de la Convention 108 (§ 69).

C. Enfin, le requérant se plaint que le refus des tribunaux d'examiner sa demande visant à obtenir le remboursement des frais et un dédommagement a porté atteinte à son droit à un tribunal, en violation de l'article 6 de la Convention.

La Cour estime que l'omission de la cour d'appel d'examiner cet aspect de la demande a porté atteinte au droit du requérant à un procès équitable et qu'il y a donc eu violation de l'article 6 de la Convention (§§ 78 et 79).

Il m'est difficile de conclure sur une matière qui est en constante évolution et dont je me suis limitée à évoquer un moment. Entre effectivité et complémentarité. D'un côté, comme le constate O. De Schutter, à travers l'extension qu'opère l'arrêt Rotaru contre Roumanie, la Cour européenne des droits de l'homme a voulu se donner les moyens de participer à l'effectivité du contrôle de la protection des données à caractère personnel et de renforcer ainsi les droits fondamentaux de l'individu[8]. D'un autre côté, il importe aussi de soutenir et de développer les possibilités de protection complémentaire offertes par les différents instruments qui peuvent être mobilisés dans le champ qui nous occupe aujourd'hui.

[8] *Ibid*., p. 181.

The individual's means for protecting his/her personal data and asserting his/her rights in the context of globalisation: Paper submitted by Ms Sarah ANDREWS

THE INDIVIDUAL'S MEANS FOR PROTECTING HIS/HER PERSONAL DATA AND ASSERTING HIS/HER RIGHTS IN THE CONTEXT OF GLOBALISATION

Paper by

Sarah ANDREWS
Research Director
Electronic Privacy Information Center (EPIC)
United States of America

I would like to begin with some background on the Electronic Privacy Information Center (EPIC). EPIC is a public interest and advocacy group based in Washington DC. We were formed in 1994 to preserve privacy, anonymity, free speech and other key constitutional values on the Internet. We maintain a comprehensive website[1], provide a free bi-weekly electronic newsletter[2] and publish a number of books each year including the Privacy Law Sourcebook, the Consumer Law Sourcebook Privacy and Human Rights, Filters and Freedom and Cryptography and Liberty.[3] We are independently funded by charitable foundations and individuals and we do not receive money from private companies or the government.

As there is no official privacy agency in the United States[4], individuals are to a large extent responsible for protecting themselves against invasions of their privacy and misuse of their personal data. This is often a difficult task for individuals and is compounded by the fact that there is no comprehensive privacy law governing the collection and use of information by private parties. In the commercial sector, the U.S. approach to privacy protection relies on sectoral laws and self-regulation. Sectoral laws target only narrow areas of the marketplace at a time. They are issued from time to time in response to new technologies or when particular problems or bad practices appear ubiquitous across an entire industry.[5] Examples include, the Family Educational Rights and Privacy Act 1974; the Cable Communications Policy Act 1986; the Video Privacy Protection Act 1988; the Telephone Consumer Protection Act 1991; the Driver's Privacy Protection Act 1994; the Telecommunications Act 1996; the Children's Online Privacy Protection 1998; the Financial Services Modernization Act 1999 and the recently enacted

---

[1] See <http://www.epic.org>.

[2] Archives of 'the Alert', dating back to 1994, are available at <http://www.epic.org/alert/>.

[3] For more information on these and other publications visit the EPIC bookstore at www.epic.org/bookstore

[4] Although the Federal Trade Commission (FTC) has been operating as the "de facto" privacy agency, in truth it lacks the basic powers of oversight and enforcement and has not been effective in protecting the privacy of individuals. The agency has a broad, non-privacy specific, mandate to prohibit "unfair or deceptive acts or practices in or affecting commerce." This authority is not a sufficient substitute for a comprehensive privacy law and does not contain any articulation of fair practices for information processing. Furthermore, although individuals may submit complaints of a privacy violation to the agency, it is not under any obligation to review or respond to these complaints. For more information on the FTC visit <http://www.ftc.gov>.

[5] See generally "The Privacy Law Sourcebook 2000: United States Law, International Law, and Recent Developments", Marc Rotenberg (EPIC 2000).

medical regulations (HIPPA regulations).[6] While these privacy laws are useful to provide detailed protections for certain categories of information, the underlying flaw of a sectoral approach to privacy protection, is that the laws continually need to be updated as new technologies give rise to unanticipated practices. Without a backdrop of a comprehensive privacy law, U.S. individuals cannot be assured of privacy protection on an on-going basis.

Even less can be said of a self-regulatory regime for privacy protection. This has been the official approach of the U.S. government for Internet privacy since the early 1990s and is strongly backed by the corporate sector. Under such a scheme businesses voluntarily agree to abide by a set of good principles. The idea is to avoid "heavy-handed" regulation and allow competitive forces within the marketplace to respond to consumer demands. The fundamental flaw in this method is that there is no real oversight and enforcement. Even when companies sign on to a "seal" program of a third party body, bad practices most often go unpunished. In many cases, this is because the third party is funded by the very companies it is meant to oversee and therefore lacks any real independence.

EPIC believes that these are serious deficiencies in the US legal system. We strongly support the passage of comprehensive privacy legislation for the private sector and the establishment of an independent body to oversee implementation of such a law. However, we also recognize that there are other complimentary means for individuals to prevent or at least decrease the most egregious violations of their personal data.

The first and most obvious means is through the use of technology. Technology plays a critical role in safeguarding privacy. Since its creation EPIC has worked to encourage the development of technologies that allow Internet users to safeguard their data and protect their identity. Technologies aimed at eliminating or limiting the collection and processing of identifiable data are known as "Privacy Enhancing Technologies" (PETs). Examples of useful PETs include anonymous web browsers, remailers, proxy servers, encryption, cookie busters and html filters. In addition, systems are now being developed to allow users to conduct commercial transactions on an entirely anonymous basis. Companies such as the US-based iPrivacy allow consumers to shop, buy, and have goods delivered to them without revealing personal information to any of the data collectors on the Internet such as ISP's, advertisers, or even the merchants themselves.[7] During the summer of 2001, the German government launched a project known as Data Protection in Teleservices (DASIT) to develop similar software systems that will allow consumers make anonymous Internet purchases and payments. We maintain a list of these products and developments on our Practical Privacy Tools page and it has proved to be one of the most popular features on our web site.[8]

It is important to distinguish, however, between genuine PETS and other products offered by industry as privacy protective but in reality operate merely to warn consumers how their personal data will be disclosed to others rather than to limit disclosure of personal information. An example of such a product is the World Wide Web Consortium's (W3C) Platform for Privacy Preferences (P3P). In June 2000, EPIC and Junkbusters.com (a privacy advocacy firm based in New Jersey, USA) issued an assessment report of P3P. The report concluded that "P3P fails to comply with baseline standards for privacy protection. It is a complex and confusing protocol that will make it more difficult for Internet users to protect their privacy." [9]

Another less reliable means to improve companies' privacy practices is through the use of public pressure and boycotts. EPIC and other consumer and privacy organizations have taken

---

[6] The *Standards for Privacy of Individually Identifiable Health Information; Final Rule* was issued by the Department of Health and Human Services (DHHS) on December 28, 2000 pursuant to the Health Insurance Portability and Accountability Act 1996 (Public Law 104-191). The rules became effective on April 14, 2001

[7] See <http://www.iprivacy.com>.

[8] See <http://www.epic.org/privacy/tools.html>.

[9] EPIC and Junkbusters, "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy" (June 2000) <http://www.epic.org/reports/prettypoorprivacy.html>.

this approach and lead campaigns on behalf of individuals on a number of occasions. The first such campaign was in 1999 in response to an announcement by Intel that it planned to include a unique ID number in each of its new Pentium III chips. The number, called a Processor Serial Number (PSN), was to be accessible via software and was designed for use by software programs and web-based services to identify users. EPIC, Junkbusters and Privacy International called for a boycott of Intel products until the company disabled the PSN and recalled existing chips. [10] The boycott was a public relations disaster for the company and soon thereafter Intel promised to offer a software patch to disable the PSN.[11] In April 2000, Intel announced that it would not include the serial number in future chips.[12]

The next major campaign was against Doubleclick, the Internet advertising giant that tracks Internet user behavior in order to better target banner ads. In November 1999, DoubleClick announced that it was buying Abacus, owner of the largest direct marketing lists in the country, with information on the purchasing habits of 90 percent of all U.S. households. DoubleClick planned to merge this information from the purchasing databases with its own profiles on Internet users and their browsing habits. In response, EPIC filed a complaint with the Federal Trade Commission calling for an immediate investigation of the company for engaging in “unfair and deceptive practices.” Again, public outcry and extensive media coverage embarrassed the company into submission. In March 2000 DoubleClick announced that it was suspending its plan to merge the databases stating that it had made a "mistake by planning to merge names with anonymous user activity across Web sites.” [13]

The most recent campaign being led by EPIC is against Microsoft for the anti-privacy features in its new operating system, Windows XP, and associated services. In July 2001, EPIC and thirteen other public interest groups filed a formal complaint with the Federal Trade Commission alleging that Windows XP and associated services such as Hailstorm, Passport, and E-Wallet, are intended to profile, track, and monitor millions of Internet users. The central argument against these services is that they collect and disclose detailed personal information about users without sufficient guarantees of privacy or security, and often without any real knowledge or consent. For example, Passport account information is shared among third party Web-sites; Windows XP users are forced to create a Passport account to use Internet communications features (such as instant messaging); Hailstorm essentially strips users of their right to control their personal information; and Hotmail users are automatically signed up for a Passport account without notice or even an opt-out facility. Coupled with the extraordinary market dominance of Microsoft, the far-reaching and inter-connected nature of these Internet business activities constitutes a unique threat to the privacy of computer users. The issue is now the subject of considerable public debate and it is hoped that the Federal Trade Commission will soon begin an investigation into the exact information collection capabilities of these services.

These examples of technologies and effective public campaigns illustrate how individuals can assert more control over their personal information and influence business practices. However, it is important to remember that although they may be a useful compliment to a legal framework they cannot replace it and should not be used as a justification for not adopting privacy laws.

---

[10] For more information on the boycott visit <http://www.bigbrotherinside.com/>.

[11] See “Intel on Privacy: 'Whoops!,” by Polly Sprenger, Wired News, Jan. 25, 1999. <http://www.wired.com/news/politics/0,1283,17513,00.html>.

[12] “ Intel Nixes Chip-Tracking ID,” by Declan McCullagh, Wired News, April 27, 2000. <http://www.wired.com/news/politics/0,1283,35950,00.html>.

[13] For more background information on this deal see http://www.epic.org/privacy/doubletrouble/.

OTHER CONTRIBUTIONS

DOCUMENTING NATIONAL DATA PROTECTION LAWS

Paper by

Mr Frits HONDIUS
Representative of "I-Ways Digest"
United States of America

Introduction

On 18 September 1980, the Committee of Ministers of the Council of Europe adopted Recommendation No R (80) 13 on exchange of legal information relating to data protection regulation. This Recommendation took into account that States should have ready access to information relating to constitutional, legislative or administrative texts, and judicial decisions and official documents on data protection from member States as well as non-member States.

Making such information available through the intermediary of the Council's Secretariat and where possible translated into one of the Council's official languages serves a two-pronged goal. First of all, national legislators can take inspiration from each other's regulatory processes, taking duly into account of course differences between legal systems (federal or unitary, civil law or common law, etc.) Secondly, transborder data flows are a reality in global society. Regulators, data users and data subjects need to know and are entitled to know the legal regimes governing specific data transactions across the borders.

It was not sufficient to include an obligation for information exchanges in Convention 108, because this instrument only binds the States parties, not all States having data protection regulations. The Convention is particularly watchful with regard to third countries, in particular those which are not, for political or geographical reasons, members of the Council of Europe.

For this reason, ever since its establishment 30 years ago, the Committee of experts, later renamed Project Group, on data protection (CJ-PD), has been devoting an important part of its work to the collection and presentation of the latest information on data protection laws in member and observer States. As long as these States were relatively limited in number it was possible for the Committee to listen to oral statements and engage in questions-and-answers. This procedure was no longer possible however when participating States grew in number (from 19 in 1971 to 43 today) and in the face of a veritable proliferation of data protection laws. For this reason the CJ-PD now relies on the circulation of written information. This information includes not only laws in existence, but also draft laws. It is a valuable source of information, especially for parliaments and governments. The countries of Central and Eastern Europe, where data protection belongs to the body of new law on human rights, can also receive the relevant information through the intermediary of the Council's network of Information and Documentation Centres. Moreover, the general public can now access the Council's public documents via website http://www.coe.int.

Information journals and sourcebooks

It is vitally important for data protection information to be widely and publicly available. Since the beginning of the data protection programme in the Council of Europe, many books and journal articles have appeared on the subject. New university departments and research centres have been created to deal with the subject in a diverse range of fields of activity such as human rights, information technology, administrative science, etc.

Of particular importance are those publications which aim at providing the readers with regular updates, data protection being a very dynamic discipline. Moreover, there is a great need for making information available in languages other than those of the Council of Europe.

The most useful format is that of *loose-leaf sourcebooks.*. Mention should be made in this respect of the publication in three languages "*Datenschutz in der Europäischen Union*/Data Protection in the European Union/*Traitement des données personnelles dans l'Union Européenne*" -authors Simitis, Dammann and Körner, editor Anne Arendt of Frankfort University (published by Nomos, Baden-Baden) which contains the complete texts of data protection laws in the European Union.

Another type of sourcebook is that for national consumption such as the Dutch language publication "*Voorschriften Privacybescherming*" published by Elsevier Bedrijfsinformatie, The Hague, which was launched in 1980 and now comprises four thick volumes documenting the law, subsidiary regulation and case-law, self- regulation in major sectors of government and the economy. Volume 4 (contributed by the author of the present Note) documents international and foreign legislation.

Finally, a very useful type of documentation source is the various national and international *journals* dedicated to data processing and data protection. Mention can be made here of the journal "I-Ways Digest" published at Fairfax, VA, USA, which is a continuation of the former journal "Transnational Data Report".

A call for contributors

On behalf of the editorial boards and publishers of the three sourcebooks and journals mentioned above, we wish to express our gratitude to all those in national and international administrations, libraries and research centres who have contributed in the past to our documentation work. It is often tedious, time consuming and requires a great deal of attention to minute details (date, name and serial number of official gazettes, Internet Website information, providing and checking translations etc.). We encourage them to continue their effort and we will also welcome offers of new contributors. The Council of Europe's Warsaw Conference on Data Protection seems an excellent opportunity for strengthening the information and documentation effort, an essential element of the Council's monumental work on data protection.

Our email address: hondius@wanadoo.fr

SUMMARY AND CONCLUSIONS BY THE GENERAL RAPPORTEUR OF THE CONFERENCE

presented by

Ms Waltraut KOTSCHY
Data Protection Commissioner of the Council of Europe,
Executive Member of the Austrian Data Protection Commission and
Head of the Data Protection Section in the Austrian Prime Minister's Office

On the 20th anniversary of Convention 108, the most generally acknowledged legal instrument on data protection in Europe, it seems more than justified to take a short break in our daily endeavours to deal with numerous greater or smaller data protection problems and gather in this Conference in order to contemplate

- the overall situation of data protection, especially in Europe,
- the impact which Convention 108 is still able to exercise and
- conclusions - whether there is a need for future action within the framework of Council of Europe regulations dealing with the topic of data protection.

The programme of the present Conference was drawn up in accordance with these intentions:

The first morning was reserved for general reflection on the challenges of the information society in relation to data protection, enriched by reports on the latest developments and experience in Poland, the Czech Republic, Slovakia and Lithuania.

The social and legal background was thus defined for an examination of the present and future significance of Convention 108 in a world which has undergone considerable changes since the late 1970s when the text of the convention was elaborated. This examination concentrated on the relevance of Convention 108 as such – including questions on the significance of the new Additional Protocol to the convention - and on the relevance of the fundamental data protection principles as set out in the convention. The topics were analysed by two reports and highlighted by two Round Tables where participants were invited to comment especially on whether new principles ought to be introduced into European data protection and – in the second Round Table – on the suitability and efficiency of transborder data flow regulations for the protection of the rights of citizens of Member States party to Convention 108.

The second day was reserved for the discussion of instruments - existing or future – for the implementation of data protection, covering also the topic of implementation in a global society which results in a growing need for co-operation. As the role of supervisory authorities is one of the principle means of effective implementation of data protection this subject was examined in one report and two round tables.

A further topic of this conference, which was dealt with in the afternoon session of the second day, was the individual's means for asserting and protecting his/her rights to data protection.

In the following remarks I will try to summarise the arguments brought forward and the conclusions which would have to be drawn.

A. SUMMARY

On information society and the need for data protection

In the first report of this conference, today's information society, as the background to the need for data protection, has been aptly described by Professor Safjan as a battle field of contradicting – though justified – interests, which requires special legislative skill in order to establish a satisfactory balance. The fact that in many European countries a fundamental (constitutional) right to data protection exists side by side with a fundamental (constitutional) right to access to public information clearly shows the dichotomy or "Janus aspect", as it was called by Professor Safjan, of legitimate interests in a free and democratic society.

How new both of these contradicting interests are for the citizens of the former eastern European countries, was pointed out during the Round Table on data protection legislation in the countries of Central and Eastern Europe: Transparency of public life (access to information held by the state) as well as protection of a personal sphere from intrusion (data protection) were both non-existent in the totalitarian regimes. It will take time to firmly establish awareness of these rights in citizens' minds. The guarantee of the individual's privacy is however "essential for a person to feel free and safe", as the Data Protection Inspector of Lithuania pointed out.

As for the harmonisation of the above-mentioned contradicting social interests, the rapporteur, Professor Safjan, diagnosed a certain lack of precision and completeness where the existing legal instruments try to define the lawful derogations from either of these fundamental rights in the interest of the other fundamental right. Considering the importance of a workable solution for the question of which exemptions from the (fundamental) right to data protection should be considered lawful, this diagnosis - which is also backed up by the experience of the rapporteur as president of a constitutional court - might lead to the conclusion that there is need for further action.

The mere existence of ever increasing amounts of personal data and their technically easy accessibility by more and more effective means of information technology result in a growing demand for these data for different kinds of exploitation: Data as valuable goods on the market are a necessary aspect of the information society. Whose must shoulder the burden of protection of personal data in these circumstances? Is it the individual who has to take care of his own interests as a consequence of his/her information autonomy? Or is it society which ought to take the main responsibility? Professor Safjan opted for the main responsibility resting with society, as the individual would in his opinion not be in a position to be effectively able to defend his personal sphere: "It is no longer the individual alone that decides on the scope of his own information-related autonomy, but the decisions concerning the areas in which it can still remain free from external interference are being taken on his behalf by the law and by public institutions."

Agreeing or disagreeing with this evaluation is not an academic dispute but a question of vital importance for the future of data protection:

- Should the enforcement of data protection rules be reserved for civil law actions to be brought by the data subject, or should society provide for special public law tools which aim at the protection of personal data as a public interest (as is the case for the protection of other fundamental rights)? Should the state provide for preventive means aiming at avoiding data protection infringements, or is it enough to enable the data subject to claim compensation if infringements occur?

- Should data subjects throughout their lives be confronted by an endless stream of situations where they asked to opt into (or opt out of) the permission to use their data? Or should there be a widely acknowledged set of general legal rules taking care of the question of which data may be used lawfully in which situation for which purposes, thus creating an environment for the use of information which can function lawfully even without the active participation of the data subject?

These questions will be taken up when commenting on the observations of the rapporteurs and the panellists discussing the data protection rules of Convention 108.

On the principles set out in Convention 108

What are these essential rules, set out in Convention 108?

As this question is the topic of a report by Mrs Estadella Yuste, what the rapporteur defines as "principles" of the convention needs looking into: enumerated as "fundamental principles of the Convention" were the provisions of Article 5 ("quality of data"), of Article 7 ("data security") and of Article 8 ("additional safeguards for the data subject"); as additional principles the rapporteur defined the "accountability of the controller of the file", "free flow of data between Member States" and "co-operation and mutual assistance", which were deduced by the rapporteur from various provisions of Convention 108.

This enumeration already shows how difficult it is to decide which of the provisions of Convention 108 should be called a "principle" to be set apart form "normal provisions". I personally do not think that there is much added value in a discussion about the qualification of provisions as principles as all provisions of the convention must be implemented in national law, whether they are called principles or not. What we have to look at and evaluate are the main features of Convention 108. Their appropriateness (relevance) could be analysed under different aspects:

On the relevance of the content of the provisions of the Convention

Concentrating first on the provisions of Chapter II of Convention 108 - mainly Articles 5, 7 and 8 - we will try to recall what has been said concerning their relevance in today's world:

The rapporteur pointed out that they represent a set of data protection rules which are widely agreed upon not only in Europe but throughout the world. There does not seem to be any need for alteration of these articles of the convention. The question would rather have to be: Are these rules complete seen from today's perspective?

Before we can proceed to analyse this question we should, however, deal with a very interesting topic raised in the Round Table on the relevance of the principles of the Convention:

Is it still justified to apply all of the data protection principles of the Convention in the same way to all kinds of data processing, especially also to the processing of unstructured texts?

This question stands for a rather fundamental problem in data protection:

Which are the factors that constitute the specific dangers of electronic data processing. Are these dangers significantly less acute if non-structured information is stored electronically, or is the danger just the same considering the possibilities of full text retrieval?

Answers to this question might have to be found in the context of the definition of "processing". Although the tendency in the 1990s was towards including all kinds of electronic data processing into the current data protection regime, reconsideration of this position should not be excluded in a world where more or less all information handling has become electronic: Is it justified to apply rules which have been developed vis-à-vis the threat of huge electronic registers – that is: structured and condensed information – to everyday use of information, where the computer to a large extent only substitutes the typewriter and the archives for letters and other files?

Further discussion is needed on this topic. It might be possible to tackle this problem reasonably not only with regard to the definition, but rather from the perspective of the principles of Article 5, especially by considering the implications of the "fair processing" principle: It is widely

acknowledged today that this principle deals mainly with the possibilities of access to information, which must be offered to data subjects concerning the use of their data. This principle would perhaps allow for a more differentiated interpretation of a controller's duties in today's information society compared with the situation of 20 years ago, and may probably result in a different transparency regime for different kinds of data processing.

On the completeness of the principles of Convention 108

Coming back to the question of whether the rules contained in Convention 108 are "complete", seen from today's perspective, it has to be remembered that in the Round Table discussion on the relevance of the principles of the Convention there was a definite proposal for the adoption of at least one further principle which would have to be added to the existing ones:

Should a new principle of data avoidance (data austerity) be adopted?

This question concerns the new logical and technological possibilities for processing personal data without making identifiers available to the user. Considering the evident importance of this question, it would certainly be worth analysing how far this principle is already contained in Article 5 (c) of the Convention or if – and how – Article 5 would need interpretation, clarification or express extension on this point.

Whether the Convention contained regulation of all points which are at present considered essential for effective data protection was checked within the Council of Europe's Consultative Committee for Convention 108 in 1998 before embarking on the task of elaborating an Additional Protocol to the Convention. The outcome of this evaluation was the addition of the two principles (rules on data transfer to third countries and the independent data protection control authority) to be outlined in greater detail below. Apart from these additions the Consultative Committee considered Convention 108 to be "complete" according to today's standards of data protection.

On the explicitness of the provisions of the Convention

Compared with newer instruments on data protection – such as, for example, the EU Directive 95/46 - the provisions of the Convention could certainly be described as very general. Is the relevance of these provisions lessened by the fact that they do not give precise recipes for how to cope with the manifold situations in a world of growing complexity? How can these 20-year-old provisions contribute to solving problems which arise in a completely changed technological environment?

So far, the only remedy against laws constantly being outdated by technological development was and is: to keep legal provisions fairly general and "technology neutral". Successful examples show that this is a realistic option. As a negative consequence, however, such legislative style calls for considerable skills in interpretation when implementing the general rules in concrete situations. One way out of this dilemma is the creation of special laws for areas where finding balanced solutions by mere interpretation of general rules would lead to very uncertain results. Most countries have chosen this mixed solution: A fairly general law on data protection which attempts to be as "technology neutral" as possible goes together with several area-specific laws.

The Council of Europe traditionally pursues a similar policy in data protection matters: Convention 108 (now supplemented by the Additional Protocol) sets out the general principles, whereas the Council of Europe Recommendations take care of defining standards for specific areas of data processing, which can easily be adapted to the relevant technological, economic or other changes in society.

This system has so far proved to be most valuable. It is essential, especially in times of rapid change, to have some points of reference which do not change. Just as the ECHR has now for 50 years been a constant benchmark for the legitimacy of infringements of fundamental rights of

the citizens, the principles of Convention 108 should be kept as the essence of data protection which cannot be changed according to everyday political whims. In my opinion, it is the very general nature of the provisions of Convention 108 which have prevented the text from becoming outdated.

On the effectiveness of the provisions of the Convention

The effectiveness of legal rules depends to a large extent on the effectiveness of the means for their enforcement. As was already pointed out in the introductory report given by Professor Safjan, the effectiveness of such enforcement would be greatly influenced by the decision whether society leaves individuals alone in their struggle to enforce their rights or whether society takes an active interest in the possibilities of enforcing certain rights and therefore establishes special enforcement procedures under public law.

These questions are dealt with in the Convention under Article 8 ("additional safeguards for the data subject") and Article 10 ("sanctions and remedies"). A special report was given by Mrs Mallet-Poujol on "The individual's position in a globalised information world: Rights and obligations".

Article 8 of the Convention introduced the idea that data subjects must be enabled to have adequate knowledge about the use of their data and that they have the right to have incorrect data rectified and unlawfully used data deleted.

Since the creation of these principles in Article 8 in the late 1970s a comprehensive set of instruments for the realisation of this concept has been elaborated, such as notification of registration, a special right to access, a right to rectification, and so forth. Among the more recent achievements in this area, the controller's obligation to give adequate information to data subjects and the right of data subjects to object to use of their data must be mentioned. These conditions for lawful data processing have all been developed on the basis of Article 8 of Convention 108.

It might be interesting to point out, as Mrs Mallet-Poujol did in her report, that the importance of the instruments mentioned above may vary according to the technology used for the processing of data:

In the Internet world the obligation to inform and the right to be informed about the use of one's data is of the utmost importance for the protection of the data subject's rights, especially when combined with a request for the data subject's consent (be it opt-in or opt-out) as the legal basis for the use of data.

For a situation of intensified global data transfer and exchange, the right to object may become very useful in the form of the possibility to opt out after having been informed about intended transfers.

On the whole, it seems that the information society calls for alert and active data subjects, making use in their turn of the possibilities of modern technology - like the Internet - in order to exercise their rights for the protection of their data.

On the Additional Protocol

With regard to the position of the individual in a world of global exchange of information, the newly formulated principles of the Additional Protocol to Convention 108 also need to be considered. The Additional Protocol contains two new requirements for appropriate data protection, which are:
the existence of national legal provisions on the special protection of data which are to be transferred to countries which are not parties to Convention 108; and
the existence of an independent national data protection supervisory authority.

On Transborder Data Flows

A special Round Table on transborder data flows was entrusted with the task of outlining the most recent achievements concerning instruments for securing the necessary special protection of personal data used outside the territory of the parties to Convention 108.

The new “Standard Contractual Clauses for the transfer of personal data to third countries” and “Standard Contractual Clauses for the transfer of personal data to processors established in third countries”, launched by the European Commission, were presented to the audience, followed by an evaluation of the situation from the point of view of industry, represented by the International Chamber of Commerce.

To ensure satisfactory protection of personal data in a foreign country which does not have an adequate level of data protection, by means of a contract between the data importer and the data exporter, is a well-established procedure in international data protection law. Considering the important role of multinational companies on the global scene of data transfer, consideration of another means of guaranteeing data protection should however not neglected: using the model contract between the different entities within multinational companies is usually an unnecessarily complicated process. Keeping in mind that the control of data transfers within such company structures can be quite well controlled as there is a common head of companies with the power to order all affiliates to behave in a certain way, a solution of the following nature could also be envisaged: the multinational company headquarters could establish a code of conduct mandatory for all affiliates and company institutions. By unilateral - legally binding - commitment of headquarters vis-à-vis the relevant national data protection supervisory authority:

- to follow this code of conduct;
- to submit to the findings of the Control Authority in case of claim settlement; and
- to enforce compliance with such findings by the affiliates,

guarantees for the effectiveness of the code of conduct could be achieved which are at least as reliable as contracts between the different entities within multinational companies. An additional advantage could be a certain trend-setting function of such multinational companies in data protection matters, especially as they would have to stipulate adherence to their code of conduct by all companies which wish to act as service providers for such multinational companies.

There are naturally limits to the protection effect of such legal instruments - regardless of whether they are contracts or unilateral commitments - if state authorities in the recipient country enforce access to transferred data. The decisions of the European Commission on the aforementioned standard contractual clauses try to take care of this problem by allowing for a certain margin of discretion by the national supervisory authorities, where dangerous interference of the state in the recipient country is likely, in which case the supervisory authority could exceptionally forbid transborder data flows even though there was a contract following the standards.

Important as the free flow of data over national borders would be for globalisation of the information society, an adequate protection of citizens’ rights forces those countries which have data protection rules in place to establish certain checks in order to balance the specific dangers of data transfer to countries without data protection. The participants in the Round Table also discussed models for establishing adequate data protection for a country – not only for one controller - by self-regulation without – or with a minimum of - state interference. The first example of this kind, acknowledged at least by the European Union as adequate, are the so-called “safe harbour principles”, containing a set of rules to be followed by those private companies which openly declare their adhesion to the safe harbour principles. The weak point about self regulation, which is enforcement of the rules in case of infringements, is counteracted in the safe harbour system by the involvement of the United States Federal Trade Commission. Whether mere self-regulation without such enforcement guarantees would meet with the

requirements of a level of data protection which could be called satisfactory in the light of Convention 108 remains to be seen. However, in cases of lack of state regulation, encouragement of the creation of self-regulation systems should not be denied as long as it is understood that self-regulation will most likely only be a step on the way to a satisfactory data protection regulatory system for a whole country.

On independent control authorities

The necessary existence of an independent national data protection supervisory authority is the second requirement introduced by the Additional Protocol.

Convention 108 provides in Article 10 for appropriate remedies for data protection violations giving effect to the basic principles set out in Articles 4 to 11of the Convention. It does however not expressly demand the possibility of bringing a claim before a special independent supervisory authority.

The reason why such special remedies seem to have become so important in the present context may be found the high degree of complexity of today's society, which leaves data subjects with a dangerous disadvantage compared with those governing the information society, if there is no expert help available easily and without the risk of exorbitant cost. The data protection control authorities should grant this expert help.

A Round Table on the position of supervisory authorities illustrated the different tasks which are entrusted to the supervisory authorities of member States: There is a wide range of different solutions with very different combinations of competences and different priorities: some authorities have more ombudsman-type functions, some concentrate on auditing functions, some are similar to courts – most are endowed with a mixture of all of these types of competences. One thing they must have in common, however, is independence, at least in function if not in organisation.

A Round Table on individuals' means for protecting their personal data and asserting their rights in the context of globalisation gave additional information on remedies in data protection matters besides appealing to a supervisory authority. Mrs Tulkens, judge at the European Court of Human Rights, gave an introduction to the functioning of remedies under the ECHR; on behalf of the Polish Ombudsman for Human Rights his legal possibilities for involving in data protection matters were discussed; and finally a representative of the United States non-governmental organisation EPIC illustrated how NGOs can effectively contribute to the implementation of data protection.

The fact that a global information society tends to create problems which surpass national boundaries is evident; just as evident as the fact that the solution of such problems calls for co-operation of the state bodies, especially the supervisory authorities, entrusted with the implementation of data protection in member States.

What has been achieved in this area and what could be envisaged for the future was pointed out in the report by Mrs Alonso Blas on "Mechanisms for implementation and international co-operation in the context of data protection".

The panellists of a Round Table representing the Spanish, the French, the Irish and the Italian Data Protection Supervisory Authorities made a special contribution on this subject.

On the relevance of the Convention 108 in the light of other legal instruments on data protection in Europe

When evaluating the legal relevance of Convention 108 at present in a European context the points of reference would doubtless have to be the European Convention on Human Rights and Fundamental Freedoms, the EU Charter on Human Rights and the EU Data Protection Directive.

1. The relevance of Convention 108 in the light of the ECHR was profoundly analysed in the report of Drs de Hert and Schreuders. The report recalls why a special convention on data protection had to be created in spite of the existence of the ECHR and points out the differences in scope between these two legal instruments.

In this context it is only natural to raise the question of whether there should not be a fundamental right to data protection under the ECHR. It is true that many of the States parties to Convention 108 guarantee the right to data protection at the level of their constitution. It is further true that the new European Charter on Human Rights, although only "soft law", explicitly contains a fundamental right to data protection. It is however also true that as the legal nature of fundamental rights under the ECHR is that of rights against the state, this would not cover the whole range of necessary protection: The private sector, as the addressee of data protection obligations, would not fit easily into the structure of the ECHR and the instruments for its enforcement.

The fact that most States parties to Convention 108 have special authorities in place dealing with remedies for infringement of data protection by the state as well as by private controllers is most likely one of the reasons why it has so far not been found to be an intolerable disadvantage that there is no fundamental right to data protection under the ECHR which is also effective against private controllers. (This is also justification for the fact that the Additional Protocol contains an obligation for Member States to establish an independent supervisory authority).

There is however another effect inherent in the ECHR which would be most valuable for data protection matters according to everyday experience: within the scope of the ECHR – and its jurisprudence – it also acts as a benchmark (and borderline) for national legislation. This function could and ought to be fulfilled by Convention 108 in data protection matters, as it would bind national legislators to follow their obligations under international law. Article 9 of Convention 108 was evidently intended to play this role with regard to the quasi-fundamental right to data protection. [1]

There is however an important structural difference between Article 8 of the ECHR on the one hand, and Article 5 together with Article 9(2) of Convention 108 on the other hand, which results in a situation where it is not really clear from which principles exemptions are possible under Article 9. Whereas it seems clear that under the conditions of Article 8(2) ECHR exemptions from the whole of Article 8(1) ECHR would be admissible, it is certainly not possible to imagine an exemption from all of the principles of Article 5 of Convention 108 under the conditions of Article 9 of the Convention: there can be no exemptions from the principle that personal data should be obtained and processed lawfully; or that only data relevant for the purpose of the processing may be collected. Other examples could easily be found.

This leads to the conclusion, that it would most likely be valuable to find a legal form for commenting on the exact relationship between Article 9 on the one hand and Articles 5, 6 and 8 on the other hand in order to avoid misunderstandings.

When analysing the full meaning of these articles, the significance of the consent of the data subject in the logical system of Convention 108 should also be clarified. Is it part of the fairness principle of Article 5, that all data could be used if consent is given by the data subject? Or is it

[1] The fact that its formulation differs from Article 8(2) of the ECHR is regrettable, all the more since this results in different standards for legislation on infringement of the right to privacy and of the right to data protection, even if both aspects should cover the same case. The same is true, by the way, with regard to Article 13 of the EU Directive 95/46 and Article 15 of EU Directive 97/66, which all have a similar function to Article 8(2) of the ECHR: All of these rules for lawful exemptions from the right to data protection – which is partly also the right to privacy - are formulated differently, a fact which could cause problems one day.

one of the not expressly mentioned – but evidently premeditated – cases of data being "obtained and processed lawfully"? Or is it one of the lawful exemptions from the principle of data protection under Article 9, that data may be used with the consent of the data subject? Clarification by interpretation would certainly be useful.

2. If the EU Directive 95/46 is taken as a point of reference for the evaluation of Convention 108, the much broader scope of the Convention establishes its great importance in the EU context as well. In all matters of the so-called Third Pillar, it is Convention 108 which is expressly mentioned as the benchmark for relevant data protection provisions contained in the legal instruments of the Third Pillar. It is thus Convention 108 that rules data protection in these most sensitive areas for citizens' rights: state security, national defence and crime prevention.

3. If the political and legal situation in all Europe is taken as a point of reference for evaluation of the relevance of Convention 108, its importance becomes even more visible: Presuming that the free flow of information throughout the whole of Europe will be an important factor for the future growing together of all countries in Europe, the existence of Convention 108 as extended by the Additional Protocol is a legal *conditio sine qua non*: Ratification of these instruments will be the means of abolishing barriers to the free flow of information which would otherwise have to be upheld in the interest of the protection of citizens' rights.

4. If, finally, the global situation is taken as a point of reference for the relevance of the Convention, the outstanding importance of the Convention is more than evident. Even if political reasons were probably to hinder one or another country from formally adhering to the Convention, constant propagation of its principles could secure a degree of acknowledgement comparable to that of the ECHR. A global information society needs globally acknowledged principles for handling information. So far no other set of rules for data protection has been elaborated which possesses an easier and broader applicability than Convention 108 in view of its concise and flexible formulation.

B. CONCLUSIONS

Having pointed out the wide range of areas for which only Convention 108 contains applicable rules on data protection, it seems imperative to facilitate its understanding and implementation as much as possible. To this end it might be necessary to reconsider from time to time how the principles of the Convention would have to be interpreted including phenomena newly created by the development of the information society.

The legal form of such an enterprise would have to be looked into carefully; this would however be a task worthy of the attention of the Consultative Committee for the Convention.

Thus the advantage of having consistent and widely recognised principles for data protection, set out in Convention 108, could be combined with the possibility of better understanding their meaning in a constantly changing world which would be a sure requirement for their global acknowledgement.

PROPOSALS FOR FOLLOW-UP ACTION BY THE COUNCIL OF EUROPE

By

Mr Alexey KOJEMIAKOV,
Head of the Public Law Department
Directorate General of Legal Affairs
Council of Europe

Mrs Chair of the Conference,
Ladies and gentlemen;

We have just listened to the excellent summary and conclusions of this European Conference on Data Protection by our General Rapporteur, Mrs Waltraut KOTSCHY, on the present and future of our Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data on the occasion of its 20th anniversary. Therefore, I do not intend to summarise the main conclusions of this Conference again.

Instead I would like to take this opportunity to explain, as far as possible on the basis of our General Rapporteur's conclusions, our proposals for follow-up action by the Council of Europe.

In our opinion, this European Conference on Data Protection has shown something in which the Council of Europe firmly believes: that the principles set out in Convention 108 are still relevant today and continue to provide a strong basis for the elaboration of data protection laws and to serve as the main point of reference for any activities in this field. However, this does not exclude the possibility that it might be necessary to modernise data protection law to a certain extent in order to meet the challenges of globalisation and in order to use the various technologies to protect personal data and make the principles of Convention 108 more effective.

During this Conference, the relationship between Convention 108 and Article 8 of the European Convention on Human Rights (ECHR) has been examined. The relationship between these two international instruments is obviously very close: in fact Convention 108 originated from Article 8 of the ECHR. The Council of Europe's data protection convention was prepared when it became apparent that effective legal protection of personal data would require more specific and systematic development of the general reference to respect for private life in Article 8 of the ECHR. This close relationship, as has been mentioned during this conference, continues through the case law of the European Court of Human Rights which has contributed to the consolidation and expansion of the European standards on protection of personal data. This aspect was clearly stated in the case of M.S. v. Sweden of 27 August 1997 in which the European Court of Human Rights, "*reiterates that the protection of personal data (...) is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention".*

As I said before, we consider that the general principles of Convention 108 are still valid and the fact that the member states of the Council of Europe continue to ratify Convention 108 and adopt its principles into their national legislation serves as proof of its continuing relevance However, this does not mean that this Convention cannot be completed and enriched with the preparation of further additional protocols and with further recommendations to provide legal

answers to the challenges presented by the rapid developments in the field of information technology. A further option for the enrichment of the European acquis on data protection would be the preparation of guiding principles or handbooks which provide a useful solution for subjects on which it has been difficult to reach a general consensus for the preparation of an international legal instrument but where it is still necessary to offer member states guidance for the elaboration or revision of their national law on these subjects.

Coming back to the European Convention on Human Rights, it is useful to draw parallels between the "life cycles" of this Convention and Convention 108. Both these legal instruments establish rights and contain general principles which continue to be relevant and valid but occasionally it might be necessary to establish new rights and principles through the addition of protocols in order to respond to the new legal and technological challenges of our society.

For example, in the field of data protection, the Additional Protocol on Supervisory Authorities and Transborder Data Flows was prepared in response to the increase in exchanges of personal data across national borders and the need to safeguard the right to privacy in relation to these exchanges and requires states to set up supervisory authorities to ensure the proper implementation of personal data protection legislation.

Future international instruments will draw on Convention 108 without touching the key data protection principles contained therein, but will instead complement and enrich these essential principles by the addition of any new or supplementary principles which may be required by the information society in the future in order to prevent unlawful infringements of use of personal data.

As the Deputy Secretary General of the Council of Europe pointed out in his opening speech, international instruments already exist in this field; not only those of our Organisation but also those of other international organisations, in particular those of the European Union. These international legal instruments also constitute the European acquis which serves to consolidate and expand the European standards on data protection.

The future legal instruments of the Council of Europe I have referred to previously, whether further protocols to Convention 108 or new recommendations, will enrich this European acquis.

An important part of this "acquis" is also configured by the work carried out by the Council of Europe's data protection committees. Apart from preparing the international legal instruments, reports, guidelines and opinions on different data protection issues they also provide an essential and operational forum for the consideration of topical data protection issues and for giving rapid responses to the challenges of the information society.

For instance, in accordance with Article 19 of Convention 108, the Conventional Committee (T-PD) formulates opinions concerning the application of this Convention.

The Project Group on Data Protection (CJ-PD) is also requested by other bodies of the Council of Europe to prepare opinions on issues related to data protection in many other fields of activity. For example, at the request of the Committee of Ministers, the CJ-PD is currently preparing the third evaluation of Recommendation No R (87) 15 on the use of personal data in the police sector. The composition of this forum constituted by the Council of Europe's data protection committees is very specific to our Organisation because they involve the participation not only of national representatives of the different ministries responsible for the application of data protection legislation but also data protection commissioners, independent experts and representatives of other international organisations, both governmental and non-governmental.

And taking into account that we have been here for the past two days celebrating the 20th anniversary of a convention which is most definitely alive, Convention 108, in order to face the new technological and legal challenges in the field of data protection the Council of Europe is currently at the beginning of the process of reorganising its committees in this field to reinforce

and renew the role of the conventional committee set up by this Convention, the "Consultative Committee".

This Consultative Committee was created with a view to facilitating and improving the application of the Convention. As has been pointed out by the Council of Europe data protection committees, a teleological interpretation of the Consultative Committees mandate contained in Convention 108 could allow the Council of Europe to carry out all its activities in the field of data protection – those which it is examining at present and those it will examine in future. The basic idea of this reorganisation is the setting up of a single renewed data protection committee which would be composed by the members of the Project Group on Data Protection (CJ-PD) and the Consultative committee (T-PD) and would form a renewed Consultative committee.

This renewed Consultative committee will therefore be composed not only of Parties to Convention 108 but also of the other member states of the Council of Europe, which are at present represented in the CJ-PD, and the observer states. It will therefore lead to greater efficiency by making better use of the available resources and will make it possible to provide rapid responses to the legal and technological challenges in the context of the global decision-making process.

So far, we have spoken about the current validity of our main legal instrument, Convention 108, and about the future structure of our committees which have been renewed to enable us to carry out our priorities in the field of data protection. The next step is, then, to determine what the priorities of the Council of Europe are and which subjects are to be examined in the near future and in the longer term.

- Firstly, I would like to remind you that the data protection committees of the Council of Europe are currently working on a number of subjects including video surveillance, smart cards, contractual clauses in transborder data flows, and the impact of data protection principles in the police sector and in judicial co-operation in criminal matters, and our committees will devote their attention to these subjects in the near future.

- Secondly, we would like to point out that some of these subjects will need to be examined from new perspectives. For instance, the enormous increase in transborder data flows calls for further examination of the different aspects of this subject, such as which criteria should be fulfilled in order for an importing country to be considered as having an adequate level of data protection or the issue of the application of the data protection principles to judicial data or new ways of co-operation between data protection authorities.

- Thirdly, we must be ready to examine the data protection aspects of new technological developments as they arise and examine how technology can play a role in preventing new challenges to data protection as well as, wherever necessary, prepare appropriate international legal instruments to ensure that progress in the world of information technology does not lead to infringements of the individual's privacy. Developments in such fields as biometry and genetics, for example, raise important questions from a data protection point of view which require close examination.

- Fourthly, as the Deputy Secretary General mentioned in his opening speech, the work of the Council of Europe data protection committees sometimes goes beyond the greater Europe with the participation of the States with observer status in the Council of Europe (such as Canada, Japan and the United States). In this respect, the Council of Europe might wish to examine the universality of the scope of application of principles contained in Convention 108 but first of all it should be advisable to discuss with member states the reasons why they have not yet ratified Convention 108 and to provide any assistance necessary. The Council of Europe would also like to reinforce its existing co-operation with other international organisations dealing with data protection issues. An important example of this new type of co-operation is the joint activities which the Council of Europe and the European Commission are carrying out together in relation to those member States of our

Organisation which are candidates for accession to the European Union. In these activities representatives of both organisations examine national legislation from the perspective of Convention 108 and Directive 95/46/EC while at the same time taking into account the closely connected content of both international legal instruments.

- Finally, we have made many references during this conference to the rapid technological progress. Therefore, we must leave enough room for dealing with new subjects which could appear during the years to come. We must also take into consideration the fact that other changes may take place in society in general which will have considerable influence on how we expect to protect personal data and what categories of data. As the Deputy Secretary General of the Council of Europe reminded us in his opening speech, the terrorist attacks of 11 September will undoubtedly lead to a significant increase in the circulation of personal data between the different security services all over the world. He also underlined that in spite of these challenges to democracy, the fight against terrorism should not tempt us to unlawfully infringe on human rights and individual privacy. In this respect, we must be ready to deal with new social and political situations created by this sort of phenomenon. In this respect, I would like to inform you that last week the Committee of Ministers of the Council of Europe approved the setting up of a new Multidisciplinary Group against Terrorism (GMT). The activity of this multidisciplinary group is expected to take into account, among other issues, those concerning data protection.

It goes without saying that these proposals, based on the outcome of this Conference, could be formulated and examined firstly by the Council of Europe data protection committees and wherever appropriate extended or revised and submitted to the appropriate bodies of the Council of Europe for approval.

Data protection is part of our fundamental rights and liberties and is a requirement of democratic society. It has become an essential element in the computerisation process. It should also be an essential guarantee of the balance between individual freedoms and security requirements, between privacy and the need for exchanges of information.
I would like to finish by saying that, as always, the Council of Europe is open to any suggestions that you may have with regard to ways of enriching the European acquis in the field of data protection or with regard to new subjects which may require examination.

Thank you very much for your attention.

CLOSING SPEECHES

CLOSING SPEECH

by

Mr Alexey KOJEMIAKOV
Head of the Public Law Department
Council of Europe

Mrs Inspector General of Poland for personal data protection,
Ladies and Gentlemen,

We have reached the end of two days of intensive debates and exchanges of views on the past, present and future of our *Convention for the protection of individuals with regard to automatic processing of personal data* on the occasion of its 20th anniversary. I would like to thank you all very much for coming here and for your contributions to these debates.

And, on behalf of the Council of Europe, I would like to express our gratitude to the authorities of the Republic of Poland for offering to host this Conference in this magnificent location and, in particular, I would like once again to warmly thank the President of the Republic of Poland, for his patronage of this Conference.

Furthermore, I would like to thank Mrs Kulesza, Monsieur Walter, Mrs Souhrada-Kirchmayer and Madame Pitrat for chairing each of the sessions and the rapporteurs and Mrs Kotschy, our General Rapporteur, as well as the panellists for their contributions to the round tables.

There have been three key elements in this European Conference on Data Protection: the first has been a review of the achievements of Convention 108, the second an examination of this Convention and how it influences us in today's world, while the third looks toward the future of the Council of Europe Convention on data protection.

The presentations and discussions over the last two days confirm that Convention 108 and its legacy are very impressive: it was, as we have heard, the first binding international legal instrument in the field of data protection and is still the only binding international instrument in its field with a worldwide scope of application; it has provided the legal base for the elaboration of 12 sectorial recommendations and an Additional Protocol; and it has been a source of inspiration not only for the majority of the national laws on data protection in our member States but also for the development of further legal instruments by other international organisations, such as the European Communities' Directive 95/46/EC and so on. I may have referred to the legacy of the Council of Europe's data protection Convention, but this is not to say that we are talking about a 'dead' instrument. On the contrary, as this Conference has confirmed, this Convention continues to provide the hard core of legislation in the field of the protection of personal data and is the point of reference for any normative or research activity in this field. There can be no doubt that the general principles established in this Convention for the protection of personal data are still valid in today's world and the fact that the member states of the Council of Europe continue to ratify Convention 108 and adopt its principles into their national legislation serves as proof of its continuing relevance.

However, this does not mean that this Convention cannot be complemented and enriched by the preparation of further additional protocols or new recommendations, as I said in my previous

intervention. The rapid developments of new technologies and the worldwide information society need flexible and new legal responses as a counterbalance. These can be provided by supplementary international legal instruments, which will be drafted to meet the new challenges of tomorrow's information society as they arise, drawing on the principles and provisions of Convention 108. These supplementary texts will reinforce the role that the Council of Europe has always had as a pioneer in the field of the protection of personal data.

This Conference has offered us an invaluable analysis of the current relevance of principles set out in Convention 108 and has provided useful suggestions based on the valuable experience of member states and beyond as to how we can proceed in the future to ensure that this Convention maintains its role and its position at the forefront of the international legal instruments in this field. Thus, this Conference has fulfilled the expectations we had when we initially envisaged holding it, and has served as a first step towards the future of the data protection activities of the Council of Europe.

The Deputy Secretary General of the Council of Europe mentioned in his opening speech that four member states have ratified the Council of Europe's data protection Convention this year, bringing the total number of ratifications to 25, and some of the seven signatory states, including our host state, have announced its imminent ratification. He also mentioned that one State has already ratified and fifteen states signed the Additional Protocol regarding supervisory authorities and transborder data flows. I would also like to mention that sixteen Parties to the Convention have already accepted the Amendments allowing the European Communities to accede to Convention 108. The European Communities' application to accede to the Council of Europe's data protection Convention reflects its wish to strengthen and develop the excellent co-operation which already exists between these two international organisations and is a further step towards our common goal of creating a stronger international forum for the discussion of data protection issues and for the examination and preparation of responses to the needs of the information society.

It goes without saying that the more states ratify the Convention and its Additional Protocol, the stronger and more complete this international forum will be and therefore I would like to take this opportunity to invite those States who have not yet done so to ratify Convention 108 and its Additional Protocol and to ensure that the principles set out in these instruments are transposed into their national legislation. I would also like to invite all States which are Parties to Convention 108 to accept the Amendments to this Convention allowing the European Communities to accede.

Looking to the future, I believe that the current relevance and importance of Convention 108 will be maintained in the years to come, but this, of course, will depend on our efforts to reinforce and improve the protection of personal data at national and international level.

It only remains for me to thank you all once again for your participation and contributions. I would like to inform you that, as is the custom of the Council of Europe with all its conferences, we intend to publish the proceedings of this conference at the beginning of next year.

Finally, I think you will all want to join me when I offer my wholehearted thanks to Mrs Kulesza, not only for Chairing the Conference over the past two days, but also for all her hard work over the past months organising this Conference. And let us not forget to thank all the staff of her Bureau, all those who have worked so hard to organise this conference and to take care of us body and soul.

I wish you all a safe journey home and look forward to working and exchanging views with you on future occasions.

CLOSING SPEECH

by

Ms Ewa KULESZA
Inspector General for the Protection of Personal Data
Poland

Ladies and Gentlemen,

For last two days we have been discussing very important issues regarding Convention 108, the first and fundamental international legal instrument which regulates data protection questions, which defines the very notion of personal data, data subjects' rights which shall be guaranteed by the Parties of the Convention, the member States' obligations.

The summary of the Conference presented by Mrs Waltraut Kotschy was excellent and I do not intend to do it once again. However I would like to refer just for a moment to the issue discussed during the Conference regarding co-operation between data protection authorities.

Except for the reports including experiences acquired in the field of international co-operation, some proposals regarding the enhancement of forms of co-operation were very inspirational, like for example the proposal concerning the creation of a joint international magazine which would be prepared and distributed in different languages. These proposals are especially important for us, the representatives of the countries which have recently introduced data protection regulations into their legislation. I say "we", because I think that I can speak in the name of my colleagues who have recently become data protection commissioners. We have to learn data protection philosophy and derive from others' experiences to be able to perform our duties. In this we take advantage of our foreign colleagues from the countries which have had data protection regulations for a long time. At this moment I would like to thank them very much for their warm-hearted acceptance of us in the group of those who are engaged in data protection issues, and for their kind and versatile help.

Regarding international co-operation, I would also like to stress that we - data protection commissioners from the countries of Central and Eastern Europe - are not only waiting for help but we are also undertaking various actions ourselves. During this Conference it has been emphasised that we have different experiences and problems as data protection commissioners acting only in these countries. These problems result from different historical experiences, different legal systems, lack of social awareness of differences in activity in the public and private sectors typical of western Europe. In this respect, just to exchange our experiences and discuss attitudes, I made a proposal to my colleagues, who took up my initiative to organise a meeting in Warsaw on 17 December this year. During this meeting we should not only undertake substantial discussion but also determine the rules of permanent, broad co-operation.

Ladies and Gentlemen,
As a co-organiser of the Conference I would like to thank the Council of Europe for taking up our proposal regarding the organisation of the Conference in Warsaw. It was an opportunity for a wider group of Polish participants interested in data protection issues to hear the reports. May I remind you that among them are judges of the Supreme Administrative Court, representatives of the scientific world, practitioners from the private sector. For me, as the Inspector General for

Personal Data Protection, it was a chance for wide promotion of the idea of data protection in Poland.

I would like to thank all participants in the Conference, especially the authors of reports and panellists. Their interventions were really very interesting and inspiring and they have enriched our knowledge. In this regard all interventions should be published by the Council of Europe in the languages of the Conference in order to reach the widest possible circle of recipients.

I would also like to thank those persons who, as representatives of the Council of Europe, directly took part in the preparations for the Conference in Warsaw, Mr Alexey Kojemiakov, Ms Marta Requena and Ms Saskia Daniell. I would like to thank my employees for their work and help during the preparations, as well as all the interpreters on whom fell the pains of interpretation of very difficult and often very technical speeches.

Ladies and Gentlemen,
I hope you found the Conference interesting. I also hope that you will carry good memories away from Warsaw, which will lead you to future visits to Poland, to which I cordially invite you.

Herewith I am closing the Conference.

LIST OF PARTICIPANTS/LISTE DES PARTICIPANTS

I- MEMBER STATES OF THE COUNCIL OF EUROPE
ETATS MEMBRES DU CONSEIL DE L'EUROPE

ALBANIA/ALBANIE: Excused/excusé

ANDORRA/ANDORRE: Excused/excusé

ARMENIA/ARMÉNIE: Excused/excusé

AUSTRIA/AUTRICHE: Mrs Eva SOUHRADA-KIRCHMAYER, Deputy Executive member of the Austrian Data Protection Commission and Deputy Head of the Data Protection Section in the Austrian Prime Minister's Office, Federal Chancellery, VIENNA [Chair of the sitting]

AZERBAIJAN/AZERBAÏDJAN: Excused/excusé

BELGIUM/BELGIQUE: M. Claude DEBRULLE, Directeur Général, Ministère de la Justice, BRUXELLES

M. Bart DE SCHUTTER, Président de l'Autorité commune de contrôle Schengen et membre de la Commission sur la Vie Privée belge, Professeur, Vrije Universiteit Brussel, BRUXELLES [Panellist]

BULGARIA/BULGARIE: Mr Vassil STOYKOV, Advisor, Ministry of Interior, SOFIA

CROATIA/CROATIE: Ms Leda LEPRI, Ministry for European Integration, ZAGREB

Mr Edmond MILETIĆ, Assistant to the Minister, Director of Department, Ministry of Justice, Administration and Local Self-Government, ZAGREB

CYPRUS/CHYPRE: Ms Goulla FRANGOU, Attorney of the Republic, Law Office of the Republic, NICOSIA

CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE: Mr Karel NEUWIRT, President of the Office for Personal Data Protection, PRAGUE 3 [Panellist]

Mr František NOVÁK, Vice-President, The Office for Personal Data Protection, PRAGUE

Ms Hana ŠTĚPÁNKOVÁ, Spokeswoman, Head of the Public Relations Department, The Office for Personal Data Protection, PRAGUE

DENMARK/DANEMARK: Ms Lene Engedal KRAGELUND, Legal Adviser, Datatilsynet, Danish Data Protection Agency, COPENHAGEN

ESTONIA/ESTONIE: Mr Hillar AARELAID ; Acting Director General, Estonian Data Protection Inspectorate, TALLINN

FINLAND/FINLANDE: Mr Pekka NURMI, Director General, Ministry of Justice, HELSINKI

Ms Leena VETTENRANTA, Counsel of Legislation, Ministry of Justice, HELSINKI

FRANCE: Mme Marie GEORGES, Chef de la Division des Affaires Européennes, Internationales et de la Prospective, Commission Nationale de l'Informatique et des Libertés, PARIS [Panéliste]

Mme Charlotte M. PITRAT, Commissaire du Gouvernement auprès de la CNIL, Services du Premier Ministre, PARIS [Présidente de séance]

GEORGIA/GÉORGIE: Mr Vasil KHACHIDZE, Director of the System Analyses Board, Georgian State Department of Information Technology, TBILISI

GERMANY/ALLEMAGNE: Mr Ulrich DAMMANN, Head of International Relations, Office of the German Federal Data Protection Commissioner, BONN [Panellist]

Ms Anja-Maria GARDAIN, Legal Adviser, BERLIN

Mr Hansjürgen GARSTKA, Data protection and Information Access Commissioner of the State of Berlin, BERLIN, [Panellist]

Mr Jürgen WEIDEMANN, Legal Advisor, BERLIN

GREECE/GRÈCE: M. Panagiotis GIANNAKOPOULOS, Adviser on Public Law, Ministry of Justice, ATHENS

HUNGARY/HONGRIE: Ms Kinga SZURDAY, Senior Legal Counsellor, Ministry of Justice, BUDAPEST

ICELAND/ISLANDE: Ms Sigrún JÓHANNESDÓTTIR, Privacy Commissioner of Iceland, Data Protection Authority, REYKJAVIK

IRELAND/IRLANDE: Mr Séamus CARROLL, Principal Officer, Civil Law Reform Division, Department of Justice, Equality and Law Reform, DUBLIN 4

Mr Joe MEADE, Data Protection Commissioner, DUBLIN [Panellist]

ITALY/ITALIE: Mr Giovanni BUTTARELLI, Secretary General, Garante per la Protezione dei Dati Personali, ROME [Panellist]

Ms Vanna PALUMBO, Head of International Relations Service, Garante per la Protezione dei Dati Personali, ROME

LATVIA/LETTONIE: Mr Rihards KANCÉVIČS, Legal Advisor of Data State Inspection, RIGA

Ms Signe PLUMINA, Director of Data State Inspection, RIGA

LIECHTENSTEIN: Excused/excusé

LITHUANIA/LITUANIE: Ms Vaida LINARTAITĖ, Chief Inspector, State Data Protection Inspectorate, VILNIUS [Panellist]

LUXEMBOURG: Excused/excusé

MALTA/MALTE: Mr Saviour CACHIA, Information Resource Manager, Malta Information Technology and Training Services Ltd, HAMRUN

MOLDOVA: Mr Victor BURLEA, Head of Section, Department of Information Technologies, CHISINAU

NETHERLANDS/PAYS-BAS: Mr Alfred ROOS, Senior Legal Advisor, Ministry of Justice, THE HAGUE

NORWAY/NORVÈGE: Mr Georg APENES, Privacy Commissioner of Norway, Datatilsynet, OSLO

Mr Thomas KEISERUD, Higher Executive Officer, Ministry of Justice, OSLO

POLAND/POLOGNE: Ms Jolanta SZYMANEK-DERESZ, Head of the Chancellery of the President of the Republic of Poland, WARSAW [Special guest at the opening of the Conference]

Mrs Ewa KULESZA, Inspector General on Data Protection in Poland, Bureau of the Inspector General of Poland for Personal Data Protection, WARSAW [Chair of the Conference]

Mr Andrzej MALANOWSKI, Director of Unit I for Fundamental Rights and Citizens' Freedoms, Bureau of the Ombudsman for Human Rights, WARSAW [Panellist]

Ms Anna WYROZUMSKA, Acting Director, Department of Legal and Consular Affairs, LODZ [Panellist]

Mr Miroslaw WYRZYKOWSKI, Dean of the Faculty of Law and Administration, Warsaw University, WARSAW [Panellist]

PORTUGAL: Mr João Pedro CABRAL, Legal Adviser, GRIEC, Ministry of Justice, LISBON

ROMANIA/ROUMANIE: Ms Iulia Cristina TARCEA, Head of the Government Agent's Unit, Ministry of Justice, BUCHAREST

RUSSIAN FEDERATION/FÉDÉRATION DE RUSSIE: Excused/excusé

SAN MARINO/SAINT-MARIN: Excused/excusé

SLOVAK REPUBLIC/RÉPUBLIQUE SLOVAQUE: Ms Natália KRAJČOVIČOVÁ, Head of the Commissioner's Secretariat, Inspection Unit for the Protection of Personal Data of the Slovak Republic, BRATISLAVA

Mr Peter LIESKOVSKÝ, IT Expert of the Inspection Unit for the Protection of Personal Data, Office of the Government of the Slovak Republic, Namestie slobody 1, 813 70 BRATISLAVA [Panellist]

SLOVENIA/SLOVÉNIE: Mr Jožef ŠANTAVEC, Counsellor to the Government, Permanent Data Protection Inspector, LJUBLJANA

SPAIN/ESPAGNE: Mr Emilio ACED FÉLEZ, Data Inspector – International Relations, Agencia de Protección de Datos, MADRID

Mr Juan Manuel FERNÁNDEZ LÓPEZ, Director, Agencia de Protección de Datos, MADRID [Panellist]

Mr Rafael Andrés LEÓN CAVERO, State Attorney, Abogacia General del Estado, Ministerio de Justicia, MADRID [Panellist]

SWEDEN/SUÈDE: Mr Sören ÖMAN, Senior Legal Adviser, Division for Constitutional Law, Ministry of Justice, STOCKHOLM [Panellist]

SWITZERLAND/SUISSE: M. Jean-Philippe WALTER, Préposé fédéral suppléant à la protection des données, BERNE [Président de séance]

"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"/"L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACEDOINE": Excused/excusé

TURKEY/TURQUIE: Mr Aykut KILIÇ, Judge, Deputy Director General, Ministry of Justice, ANKARA

UKRAINE: Excused/excusé

UNITED KINGDOM/ROYAUME UNI: Mr David SMITH, Assistant Commissioner, Executive Department, Office of the Information Commissioner, WILMSLOW [Panellist]

Mr Graham SUTTON, Policy Adviser, Freedom of Information and Data Protection Division, Lord Chancellor's Department, LONDON [Panellist]

II- PARTICIPANTS INVITED BY THE HOST COUNTRY
PARTICIPANTS INVITÉS PAR LE PAYS HÔTE

Mr Andrzej BAŁABAN, University of Szczecin, Szczecin

Ms Elżbieta BERNABIUK, Director of the Organisational-Administration Department, the Bureau of the Inspector General for Personal Data Protection

Mr Jerzy BUCHNER, Ministry of Internal Affairs and Administration, ul. Stefana Batorego 5, 02-591 Warsaw

Mr Andrzej DORSZ, Director of Law and System Office, Chancellery of the President of the Republic of Poland, Warsaw

Mr Jerzy FLAKOWSKI, Polska Telefonia Cyfrowa Sp. z o. o., Warsaw

Mr Detlef GAŁDYN, Polish Chamber of Insurance, Warsaw

Ms Małgorzata GERSDORF, Bureau of Judical Decision, Supreme Court, Warsaw

Ms Teresa GÓRZYŃSKA, Polish Academy of Sciences, Law Sciences Institute, Warsaw

Mr Roman HAUSER, President of the Supreme Administrative Court, Warsaw

Mr Wacław ISZKOWSKI, Polish Chamber of Informatics and Telecommunications

Mr Jerzy JASKIERNIA, President of the Foreign Affairs Committee, Sejm of the Republic of Poland, Warsaw

Mr Andrzej KACZMAREK, Director of the Computer Department, the Bureau of the Inspector General for Personal Data Protection

Mr Ryszard KALISZ, President of the Legislative Committee, Sejm of the Republic of Poland, Warsaw

Ms Małgorzata KAŁUŻYŃSKA-JASAK, Press Body, the Bureau of the Inspector General for Personal Data Protection

Mr Igor KOWALEWSKI, International Relations Manager, the Bureau of the Inspector General for Personal Data Protection

Mr Marek KUROWSKI, Polska Izba Ubezpielzeń (Polish Chamber of Insurance), Warsaw

Mr Jan MALINOWSKI, TP S. A.[Telecommunications Company]

Ms Ewa MATUSZEWSKA, Senior Specialist Lawyer, Polish Commissioner for Civic Rights Protection, Warsaw

Mr Thomas NESINGER, Advisor, German Embassy

Ms Teresa PETELCZYC, Deputy Unit Director, Bureau of the Ombudsman for Human Rights, Warsaw

Ms Jolanta RAJEWSKA, President of Unit II, Supreme Administrative Court, Warsaw

Mr Rafał ROJEWSKI, Legal Department, Polkomtel S. A., Warsaw

Mr Maciej RYBICKI, Ministry of Foreign Affairs

Mr Włodzimierz RYMS, Vice-President of the Supreme Administrative Court, Warsaw

Ms Jolanta SALA, Director, Informatics Center, Local Data Bank in Regional Office, Gdańsk

Mr Krzysztof SILICKI, Director for Technical Matters, Scientific and Academic Computer Network –NASK, Warsaw

Ms Alina SZYMCZAK, Director of the Bureau of the Inspector General for Personal Data Protection

Ms Patrycja TRZASKA, Uniwersytet Jagielloński, Kraków

Ryszard WALENDZIK, Supreme Chamber of Inspection, Warsaw

Mr Aleksander WITTLIN, Physics Institure, Polish Academy of Sciences, Warsaw

Mr Janusz WOJCIECHOWSKI, Deputy Speaker of the Sejm, Sejm of the Republic of Poland, Warsaw

Ms Halina WOJTACHNIO, President of Unit V, Supreme Administrative Court, Warszawa

Mr Jerzy WYSOCKI, President of the Polish Chamber of Insurance, Warsaw

Mr Jerzy ZALEWAŃSKI, Bureau of the Ombudsman for Human Rights, Warsaw

Mr Tadeusz ZAJM, Ministry of Finance

Ms Maria ZIÓŁKOWSKA, Scientific and Academic Computer Network –NASK, Warsaw

III RAPPORTEURS

Ms Diana ALONSO BLAS, Senior International Officer, College Bescherming Persoonsgegevens (Data Protection Authority), THE HAGUE

Ms Olga ESTADELLA YUSTE, Associate Professor in the Department Public International Law and International Relations, Faculty of Law, Autonomous University of Barcelona, Bellaterra (BARCELONA)

Mrs Waltraut KOTSCHY, Executive Member of the Austrian Data Protection Commission and Head of the Data Protection Section, Prime Minister's Office, VIENNA [General Rapporteur]

Mme Nathalie MALLET-POUJOL, Chargée de Recherche au CNRS, ERCIM, Faculté de Droit, Université de Montpellier I, MONTPELLIER

Mr Marek SAFJAN, President of the Constitutional Court, WARSAWI

Mr Paul DE HERT, Post Doctoral Researcher, Centre for Law, Public Administration and Computerization, Tilburg University, TILBURG

IV NON-MEMBER STATES WHOSE PARLIAMENTS HAVE GUEST STATUS WITH THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE
ETATS NON-MEMBRES DONT LES PARLEMENTS ONT LE STATUT D'INVITÉ SPÉCIAL AUPRÈS DE L'ASSEMBLÉE PARLEMENTAIRE DU CONSEIL DE L'EUROPE

BOSNIA AND HERZEGOVINA/BOSNIE-HERZÉGOVINE: Excused/excusé

FEDERAL REPUBLIC OF YUGOSLAVIA / RÉPUBLIQUE FÉDÉRALE DE YOUGOSLAVIE: Ms Gordana MOHOROVIĆ, Senior Advisor, Federal Ministry of Justice of the Federal Republic of Yugoslavia, BELGRADE

V- NON-MEMBER STATES HAVING OBSERVER STATUS WITH THE COUNCIL OF EUROPE
ETATS NON-MEMBRES AYANT LE STATUT D'OBSERVATEUR AUPRÈS DU CONSEIL DE L'EUROPE

HOLY SEE/SAINT-SIÈGE: Mr Giorgio FILIBECK, Membre du Secrétariat du Conseil Pontifical "Justice et Paix", CITTÀ DEL VATICANO

UNITED STATES OF AMERICA/ÉTATS-UNIS D'AMÉRIQUE: Ms Sarah ANDREWS, Research Director, Electronic Privacy Information Center (EPIC), WASHINGTON [Panellist]

CANADA: Mr Denis C. KRATCHANOV, Senior Counsel, Director of Information Law and Privacy Section, Ministère de la Justice du Canada, OTTAWA

JAPAN/JAPON: Excused/excusé

MEXICO/MÉXIQUE: Excused/excusé

VI- COMMISSION OF THE EUROPEAN COMMUNITIES
COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Mr Ulf BRÜHANN, Internal Market, Directorate General, Commission of the European Communities, BRUSSELS, [Panellist]

VII- OTHER OBSERVERS
AUTRES OBSERVATEURS

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)/ ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES (OCDE): Mme Anne CARBLANC, Administrateur Principal, OCDE, Division Information, Informatique et Communications, PARIS [Panellist]

INTERNATIONAL CHAMBER OF COMMERCE (ICC)/CHAMBRE DE COMMERCE INTERNATIONAL (CCI) : Mr Christopher KUNER, ICC Special Advisor on Data Protection, Privacy and E-business Issues, BRUSSELS [Panellist]

VIII- OTHER PARTICIPANTS
AUTRES PARTICIPANTS

Mr Frits HONDIUS, Representative of I-Ways Digest, Publisher of Transnational Data Reporting Service (USA), GRIESHEIM SUR SOUFFEL

Mr Pál KÖNYVES-TÓTH, Principal Adviser, Ministry for Environment, BUDAPEST

M. Morvan LE BERRE, Avocat, BRUXELLES

Ms Alessandra PIERUCCI, Researcher at European University Institute (IUE), FLORENCE

IX- COUNCIL OF EUROPE / CONSEIL DE L'EUROPE

Mr Hans Christian KRÜGER, Deputy Secretary General, Council of Europe [Special guest at the opening of the Conference]

Mme Françoise TULKENS, Juge à la Cour européenne des droits de l'homme, Palais des droits de l'homme [Panéliste]

Mr Alexey KOJEMIAKOV, Head of the Public Law Department, Directorate General of Legal Affairs, Council of Europe

Ms Marta REQUENA, Head of the Data Protection Unit, Public Law Department, Directorate General of Legal Affairs, Council of Europe

Ms Saskia DANIELL, Secretariat, Data Protection Unit, Directorate General of Legal Affairs, Council of Europe

Ms Hanna MACHIŃSKA, Deputy Director, Council of Europe Information Centre, University of Warsaw, Warsaw

X- INTERPRETERS/INTERPRETES

Mr Vladimir OLEXA, PRAGUE-RICANY

Mr Jan KROTKI, PARIS