The introduction and use of personal identification numbers: the data protection issues (1991)

Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1991

The growing use of computers in society has led administrations to have more and more recourse to identifiers. The PIN (personal identification number), when used in computers, is liable to encroach upon privacy, especially because of the risks linked to interconnection of flies. This study passes in review the advantages of the use of PINs, the risks for the data subjects as well as the safeguards for their use.

INTRODUCTION

The contribution of the Committee of Experts on Data Protection (CJ-PD) to the creation and sustaining of an enlightened international data protection policy is not confined exclusively to the elaboration of legal instruments. True, the opening to signature on 28 January 1981 of the world's only binding legal instrument on data protection - the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("the data protection convention") - is still regarded as the greatest achievement of the committees. However, no less negligible are the successful endeavours of the committee of experts to provide policy guidelines for specific data processing contexts. The six recommendations adopted by the Committee of Ministers of the Council of Europe covering various fields of data processing activity testify to the enlightened diligence with which the committee of experts has pursued a sectoral approach to data protection issues (Recommendations No. R (81) 1, automated medical data banks; No. R (83) 10, scientific research and statistics; No. R (85) 20, the direct marketing sector; No. R (86) 1, the social security sector; No. R (87) 15, the police sector; No. R (89) 2, the employment sector; and No. R (90) 19, payment and other related operations).

However, the work of the committee of experts has ranged beyond the drafting of legal texts. Its contribution to the data protection debate must also be evaluated in terms of the informed exchange of views on various privacy issues of a topical, sometimes urgent, nature which characterise its biannual plenary session. The exchange of information on such subjects as Aids, the media, genetics, the role of self-regulation in the scheme of

data protection, etc., serves to sensitise the representatives of all member governments (and, for the sake of completeness, reference should also be made to the observers from other international organisations as well as from non-Council of Europe countries) to the data protection problems surrounding these types of issues. It exposes them to comparative experience and suggests to them comparative ways of looking at and solving the issues.

Sometimes this exchange of views has shown the need to look more closely at a particular issue, for example in the context of a working party mandated to explore the problem and report back on possible solutions. Such an approach was followed for the data protection issues posed by new technologies. Rather than drafting away in precise legal language the problems which new technologies create for data protection, the committee of experts opted for the publication of its working party's findings and conclusions (see the study entitled "New technologies - A challenge to privacy protection?").

And so it is with the issues raised by the introduction and use of personal identification numbers (or PINs) and the problems which they create for data protection. In the course of an exchange of views on PINs, the committee noted that they were by no means a neutral issue. Varying degrees of concern were being expressed in member states with regard to their planned introduction and/or use. This attitude was reflected in the replies which the committee had received pursuant to a preliminary request for information which it had addressed to the governments of member states of the Council of Europe. This questionnaire was intended to elicit information in regard to the following factors:

a. national legislation, if any, governing the introduction and use of PINs;

b. the reasons why certain countries have decided not to introduce a system of PINs;

c. the data protection problems which have arisen in various countries as a result of the introduction and use of PINs.

The committee believed that the richness of the information which it received in response to its questionnaire as well as its tentative findings on the delicacy of the PINs issue, at least as far as an appreciable number of countries is concerned, merited further analysis. It is for this reason that the committee constituted a small study group composed of experts from the Federal Republic of Germany, the Netherlands and Sweden to explore in depth the whole range of issues which the introduction and use of PINs may create for data protection policy. This study group, which met from 12 to 13 June 1989, fulfilled the ad hoc terms of reference entrusted to it by the plenary committee by drawing up a report, in collaboration with the Secretariat, on these issues. It borrowed, in particular, on the information supplied by the member states as well as on the experience of its own members.

It should be noted that the group was intentionally so composed by the committee of experts so as to reflect the national experience of one country where PINs of a general multi-purpose nature were regarded as being an anathema to self-dignity (Federal Republic of Germany), of one country where PINs of this nature had been tolerated for a long period

but which was now moving towards a restriction on their use (Sweden) and of one country where context-specific PINs were in use and where new legislative proposals were in the offing so as to regulate further their spread and use (Netherlands). It goes without saying that the deliberations of the study group ranged far beyond the experiences of the three jurisdictions. Similarly, the conclusions put forward at the end of this report are intended for consumption by all governments and all national data protection policy makers and enforcers. No legal instrument is offered. Rather, it is hoped that those governments and bodies will benefit from an identification of the issues and from a distillation of ways of dealing with those issues on the basis of comparative experience. The Committee of Experts on Data Protection believes that in following this approach it will once again make a meaningful contribution to the data protection debate in Europe.

CHAPTER 1
PINs - A working definition; the sectors in which they may be used; the ways in which they may be composed; the current trends

The drafters of this report conceived of PINs in terms of a unique means of identifying an individual in an administrative file. This is not to suggest that PINs do not have applications beyond the exercise of functions by public powers. PINs may be the means of access to a whole range of services in the private sector - for example, a bank account number, a club membership number, a library membership number or a control number allocated to an individual to allow him authorised access to a data processing system in a private enterprise. The report is not primarily concerned with context-specific or one activity/one number situations in the private sector. Rather, the focus is on the PINs allocated by public authorities for administrative purposes and which also happen to be used, whether in an authorised manner or in a manner not originally contemplated, in the private sector.

PINs may in certain countries constitute universal/multi-purpose identifiers. That is to say, a PIN may be used for administrative purposes as well as for private sector purposes. The same number may be a tax number, a social security number, a passport number, a driving licence number and at the same time constitute the key to accessing goods and services provided by the private sector. Such a PIN is based on a monolithic view of administration. On the other hand, a PIN may have limited application. It may only come into being for one particular administrative purpose - managing tax files, or determining social security entitlement, or identifying the holder of a passport or identity document. In this scheme of things, an individual will be allocated a variety of identifiers for different administrative purposes. Confinement of the PIN's use to a specific administrative context reflects the principle of functional separation.

Finally, a PIN may be used to identify an individual in a population register or in a civil status register and its use may not be envisaged beyond these particular purposes.

Drawing on the situation in certain of the member states of the Council of Europe, it is possible to describe the ways in which PINs may be composed and the uses which are made of them, as well as present trends in regard to their introduction and use.

Austria

There is no universal identifier in Austria, despite internal administrative proposals to this effect. There are only context-specific PINs. Since 1988, however, the social insurance number can now be used for certain fiscal purposes.

Belgium

For the purpose of administering the population register, everyone in Belgium, whether a national or an alien, is accorded an identifier. This identification number, originally conceived to fulfil the aims of the 1983 National Register Act, has tended to become an acceptable identifier for a host of other administrative needs, leading to the abandonment of context-specific numbers such as social security and fiscal PINs. This trend towards the universalisation of the population register number is taking place despite the fact that the 1983 Act subjects the use of the PIN to the adoption of a royal decree after consultation with the Advisory Committee on the Protection of Privacy. These built-in safeguards have not confined the use of the PIN to its original purposes and authorised users.

Cyprus

The main specific PINs which are used by the public administration are:

a. social security number;

b. identity card number;

c. driving licence number.

The identity card number is also used for purposes of income tax.

Identifiers are also extensively used in the private sector, mainly by banks, both for purposes of administering bank accounts and credit cards.

Denmark

A law of 1968 introduced a ten-digit number made up of date of birth, a serial number and a conrol digit. Inhabitants of Denmark appear in the Central Population Register and may be identified in this register by means of the PIN. The register stores common personal data on all inhabitants with a view to their being used by appropriate administrative or private bodies in defined circumstances. Its application in the public sector is quite extensive. In the private sector, the use is restricted in accordance with the provisions of the Private Registers Act - the data protection law for Denmark in the private sector.

Finland

In Finland, personal identity numbers were introduced during the 1960s. The identity numbers were originally planned for social security purposes. An identity number consists of ten digits and a dash. The first six digits indicate the time of the data subject's birth, the following three numbers constitute a serial number for distinguishing between persons born on the same day. The odd serial numbers are reserved for males and the even numbers for females. The last digit is a control digit.

There are some special provisions governing the use and recording of an identity number. The identity number is used in accordance with these provisions, for instance, in the population register, the register of real estate and in the register of driving licences, as well as in credit data files. An employer is also obliged to inform the tax authorities of the identity numbers of his employees with taxable income.

When the Personal Data File Act was being enacted, the competent committee of the parliament paid attention to the widespread use of the identity numbers which is thought to constitute a threat to privacy. For purposes of general guidance, research on the basis for using identity numbers in different contexts has been carried out at the office of the Data Ombudsman.

The Personal Data File Act includes general provisions for personal data and thereby the recording, use and communication of the identity number. Only personal data that are necessary in view of the purpose of the personal data file may be recorded. The need for using the identity number has therefore to be considered from case to case.

France

Everyone born in France is allocated a thirteen-digit number made up of the holder's sex, the year and month of his/her birth, the *département* and district of birth and the sequential number on the birth register. It is known as the *Numéro d'identification au répertoire* (index identification number). The number is assigned by the National Institute for Economic Statistics and Studies. A variety of other numbers exist in both the public and private sectors to fulfil particular purposes (identity card numbers, military registration numbers, social security numbers, bank account numbers, etc.). The index identification number, as will be seen in a later chapter, has been prevented from becoming a multi-purpose number. It may, however, be authorised for use in other sectors, for example in regard to the administration of the social security system. Civil Service departments would like a wider use of the index identification number since they find context-specific numbers costly to create and administer for example, they require rewriting of software programs. The French data protection authority, the CNIL - *Commission nationale de l'informatique et des libertés* - is nevertheless pressing the administration to adopt specific identifiers. It has succeeded in encouraging the Directorate General for taxes to create a special fiscal number as a substitute for the index identification number on tax returns.

Germany

In brief, no unique all-purpose number exists. The way in which an individual is identified will depend on the particular administrative or private context. Attempts to introduce unique, single identifiers foundered on the hostility of the *Bundestag* and of the Federal Constitutional Court.

Greece

A law of 1986 made provision for the introduction of a single registration code number (EKAM) to be used for identity cards, birth certificates, electoral registers and electors' cards, passports, social security cards, driving licences, taxpayers' registers, municipal registers and registers kept by Greek consulates. The number is not used universally in the public sector. Its use is confined to day-to-day dealings between the state and the citizen. Its application is accordingly quite extensive.

In reality, the provisions of the law on EKAM have not been applied. Taking account of the reactions in the press, as well as public opinion, the government set up a working party entrusted with amending the provisions.

Iceland

With the establishment of the centralised national population registry in 1953, a PIN system was also introduced so as to facilitate management of the register for administrative and statistical purposes. At the present time, this PIN comprises ten digits made up of date of birth (day, month, year, century), a check cipher and two digits arbitrarily fixed for persons born on the same day. However, since 1987 it has been decided to make this ten-digit PIN of a more general application. Within the administration as a whole so as to avoid problems relating to namebased identification. Over and above its use in public administration, the PIN, which is given to everyone in Iceland within the first year of birth, is now also used in the banking sector and accompanies all financial documents relating to the holder.

A new Data Protection Law entered into force on 1 January 1990. According to Section 1, paragraph 4, of the new law, the provisions of the law shall apply to data which concern the private affairs of an individual, even though unnamed, if he is identified by a personal identification number. According to Section 6, paragraph 1, of the law, the interlinkage of personal data registers is not permissible. Nevertheless, it is permissible to add to a register data concerning a PIN even though the data have been obtained from the register of a third party.

Ireland

There is no universal multi-purpose PIN in existence in Ireland. There are, however, context-specific PINs in several areas of the public administration, for example, a social insurance number, which are used for specific purposes. There is no single basis underlying the manner in which these sectoral PINs are formulated. In the private sector

there is an increasing use of personal identifiers, particularly in the financial services sector.

It should be noted that there has been very little public discussion on the desirability or otherwise of introducing a state-issued multipurpose personal identifier. If such a debate does get under way it seems likely that the data protection issues associated with PINs will be carefully considered.

Luxembourg

An act of 30 March 1979 - the Numerical Identification of Natural and Legal Persons Act - provides for the allocation of an identity number to every natural person (as well as corporate bodies on the basis of different criteria) resident in Luxembourg at birth or on immigration, or any other natural person registered with a public authority or social security institution that is legally obliged to use the number. The number is composed of eleven digits representing the date of birth, sex, a distinguishing digit for people born on the same day of the same month of the same year, and a control digit. Its use is restricted to internal administration in public services or social security bodies and their direct dealings with the bearer of the number. The Grand Ducal Regulation of 7 December 1979, as later modified, stipulates the certificates, documents and files for which use of the identity number of legal and natural persons is authorised. The regulation contains one unfortunate provision which allows file owners who are competent to use the PIN to delegate their authority to use it to any intermediate person or body having a specific task to perform on their own behalf. The result is that, for instance, social security bodies ask people providing medical care to quote the national identity numbers of the people receiving treatment and employers to quote the national identity numbers of their staff in all documents forwarded to them. The data protection authority in Luxembourg is following this development with a certain degree of concern since the PIN seems to be circulating outside the circle of authorised users laid down in the Numerical Identification of Natural and Legal Persons Act of 30 March 1979.

Netherlands

A general administrative number has existed in the Netherlands since 1968. However, so far this number has only been used in the population registers kept by the municipalities. A white paper published in 1985 suggested a step-by-step approach for the gradual introduction of PINs for certain sectors provided there existed adequate legislation minimising the risk of undue encroachment on privacy. Along these lines, tax law now provides for systematic reporting of wage data along with the tax numbers of the persons concerned. Until 1989, tax numbers could only be used for tax purposes. Since then, the scope of the tax number has been enlarged so as to allow it to apply to the whole field of social security. The white paper proposals to integrate the general administrative number with the social fiscal number were the subject of criticism. Opponents of the proposals emphasised the need for legal safeguards and in particular the need for data protection legislation since the PIN would cover the whole field of public services. Accordingly, the Netherlands is now witnessing a step-by-step approach to the introduction of a single

identifier for the public sector on the basis of legal safeguards. The use of the general number will not be allowed in the private sector.

Norway

Inhabitants of Norway are each allocated a PIN in accordance with the provisions of the Population Register Act.

The PIN is an eleven-digit number. The first six figures contain the date of birth: two figures for the day, two figures for the month and two figures for the year. The next three figures are given successively for each birth on the same day. The ninth figure is an even number for females and an uneven number for males. The last two figures are control numbers. Besides their use in the population register, the PIN is now used in several other branches of public administration which need to identify citizens, for example, for social security and taxation.

The use of the PIN as a means of identification has also spread to some branches of the private sector, for example, banking and insurance.

Public bodies which need information about the PIN to carry out their functions are normally by law or regulations given the right to demand such information from the citizens. The lawfulness of private enterprises demanding such information will depend upon whether or not the disclosure of such information is considered a legitimate condition for entering into a contract.

According to the Personal Data Registers Act, the establishment of personal data registers and the use of the PIN in the registers are subject to the control of the Data Inspectorate. According to the legislation and to regulations, the registration of the PIN is forbidden in many types of registers. In other types of registers, the registration of the PIN is subject to conditions laid down in law or statutes, or to the permission of the Data Inspectorate. As regards the granting of permission, the Data Inspectorate lays down certain conditions related to collection, storage and use of the PIN.

Portugal

The allocation of a single national number to members of the public is strictly forbidden under Article 35 of the Constitution of April 1977 as amended in 1982 and 1989. A law of 1973 had in fact sought to allocate a PIN to all legal and natural persons. The PIN was intended to be compulsorily entered in all official documents and registers as from 1 January 1975 onwards. This law fell into abeyance with the prohibition clause in the 1977 Constitution. If no single identifier exists in Portugal, there are nevertheless context-specific numbers: an identity card number made up of non-significant data, an electoral register number, a fiscal number (a serial number of no significance), a social security number, etc. Needless to say, Portugal shares with other countries the presence of a range of different numbers in the private sector serving distinct purposes.

Spain

Despite attempts in the course of the 1970s to introduce a universal personal identifier along Scandinavian lines, Spain still links its PIN system to the issue number of the citizen's identity document. Decree No. 196/76, as modified by Decree No. 1245/85, declares the identity card number - which really identifies the place where the card was issued and not the date and place of birth of the holder - to be "a general personal identification number". This number is used for dealings between public administration and the individual as well as for regulating affairs between certain parts of the private sector (for instance, banks) and the individual. However, the number is extended by the addition of other control digits by the public and private bodies which use it. In accordance with the provisions of Law 7/1985, non-Spanish nationals are accorded along with their residence cards, work permits, etc. a serial number which must be used in their dealings with public bodies. However, a special and separate social security number has since 1966 been allocated to non-Spanish nationals. It comprises a number revealing the region of registration, a serial number and one or two control digits.

In 1990, a new fiscal number was introduced which is composed of the identity card number, plus a number of control digits which are unknown to the individual. The number is allocated to everyone at the time of birth.

Sweden

As far back as 1947, a birth registration number was introduced into Sweden so as to allow for a more uniform and manageable method for identification of persons other than through their names. It gradually merged into a civic registration number which came to be widely used in many different fields and replaced a host of context-specific numbers. At the present time it is a ten-digit number and is officially designated a personal identification number. This PIN contains an individual's date of birth (two digits for the year, two for the month and two for the date). The birth registration number is constructed in such a way as to allow the sex of the holder to be known and to avoid confusion over persons born on the same day. Digit 9 in the Swedish PIN means that a person is born abroad. This person can be a Swedish or a foreign citizen. Digit 9 can also mean that a person has had his original PIN changed. This system will go out of use next year. In the future the PIN will not be constructed so as to reveal whether a person is born abroad or not. Finally there is a control digit. The PIN is given to every person who is registered as a resident of a parish in Sweden.

Over and above its use in the context of civic registration, it is widely used in a whole variety of branches of the public services (tax, health and social services, passport, customs, elections, criminal investigations, legal proceedings, execution of judgments, driving licences, etc.). It is also widely used in the private sector where personal data files containing the PIN exist on employees, members of private companies, landlords and tenants, credit card holders, etc.

In short, the PIN in Sweden is the universal, multi-standard identifier *par excellence.* The Commission on Data Protection and the Principle of Publicity has made proposals to tighten up the use of the PIN. For example, it has been suggested that the Data Protection Act be supplemented so as to reduce the circumstances in which the PIN may be recorded. The Data Inspection Board would be competent to supervise use of the PIN by file keepers. Alternatively, the PIN could be regulated by its own separate law which could provide, *inter alia*, that a PIN should not be used in an electronic data processing (EDP) file if the data subject has not consented to its use or if its use lacks legal authorisation. The commission's report is now being considered by the government.

Switzerland

Although no unique number of general application exists in Switzerland, the social security number (AVS) tends to take on this role. The social security number is in fact used by many private and public bodies for purposes of managing the sickness insurance fund, personnel departments, the population register, etc. It is even used by the military authorities. The number is made up of coded information relating to the insurer's name, sex, status - Swiss or foreign - and a control digit.

So acceptable has the widespread use of the social security number become that a study on the creation of a new system for identifying people concluded that it would be preferable to stay with the social security number.

Turkey

The certificate of citizenship in Turkey refers to the number of its holder as well as name and family name, the names of both parents and the date and place of birth. The civil status register holds this information. The citizenship number is not, however, a universal multi-purpose identifier.

United Kingdom

A large number of context-specific PINs exist within the public administration, for example a national health service number, a national insurance number, a tax number, a driving licence number, etc. Such numbers may be composed on the basis of name and birth date along with other digits, or take the form of simple, sequential serial numbers. The practice differs in accordance with the sector. Not surprisingly, private sector identifiers are quite numerous. Current discussions on the introduction of identity cards as well as a new form of local taxation have raised the issue of single numbers and the dangers which they may constitute for freedoms in general.

CHAPTER 2
Perceived justifications and advantages; perceived risks for the individual

i. *Perceived justifications and advantages*

With the increased contacts between the state and the individual brought on primarily by the welfare state, it became increasingly important to devise accurate means for identifying the recipients of social goods and services. Post-war increase in population inevitably entailed an increase in the number of those administered which in turn increased the administrative burden (and hence the need for rational population registers). The state as a provider (social security, grants, education, health, etc.) and a controller (police powers, prisons, tax levies, people's movements, people's entitlement to operate vehicles, run businesses, etc.) gives rise to the proliferation of administrative files. In such an increasingly complex state of affairs the allocation of a unique identifier to each citizen within the jurisdiction of a particular state considerably eases the control and regulatory functions of the administration. However, benefits in terms of administrative efficiency may be gained whether from the introduction of multi-purpose PINs or from context-specific PINs. While PINs predate the advent of automatic data processing (for example population registers in many countries existed long before EDP), the arrival of data processing technology within public administrations allows PINs to be of even greater benefit to the administrator.

The national reports on the basis of which this study was drawn up frequently reflect the utility of PINs as a cost-saving device in the promotion of administrative efficiency. For example, the legislative decree of 30 November 1979 which introduced the taxpayer's fiscal number into Portugal was premised on the administrative benefits which would flow from the new PIN. According to the preamble, the PIN would ensure rapid accurate identification of a taxpayer; facilitate efficient monitoring of compliance with fiscal obligations; and make contacts between the authorities and the taxpayer easier. The Lindop Committee, whose findings led to the introduction of the Data Protection Bill in the United Kingdom Parliament (which later became the 1984 Data Protection Act), also recognised the value of a system of single and unique identifiers

"It can be argued that if a single and unique Identifier were given to every member of the population and if it were to be used by all data users on all occasions, the overall costs to users might be reduced. It could also be argued that the citizen too would benefit by not having to remember or record different means of identification for each of his many activities" (Chapter 29, paragraph 6, of the Report of the Committee on Data Protection, 1978).

A PIN system also makes for accurate identification of individuals in ensuring the accuracy of personal information held on computer systems. There are two issues at stake here. In the first place, the PIN is seen as a way of avoiding confusion created by members of the public having the same name. The point was made in at least two reports (France and Luxembourg) that surnames and forenames are totally inadequate for the

purposes of unambiguously identifying an individual, especially in cases where identification has financial consequences (entitlement to allowances, checklists of unreliable debtors, etc.) or social repercussions (for example, police records). Many nationals in many countries share the same name, partly owing to the decreasing number of names in circulation, partly owing to the fact that at certain times particular forenames become fashionable, etc.

In the second places accuracy has another dimension. A PIN may enable the administration to check on the correctness or reliability of information contained in an administrative file. This view of accuracy is concerned more with controlling or checking the information submitted by individuals to administrations with a view to establishing their entitlement to certain rights, benefits or privileges (social security, grants, reimbursements, etc.) or with a view to establishing their dispensation from certain penalties or impositions (taxes, rates, community charges, etc.). The fact that information exists on individuals in several administrative files for distinct administrative purposes allows the administration to check on the accuracy of information submitted to it by consulting other personal data files. A universal identifier considerably facilitates the filelinkage or matching process. And, of course, EDP improves and encourages this process even more. By Way of example, an individual may apply for an education grant to a particular administrative body. He will submit certain information regarding his financial means so as to justify his entitlement to the scholarship. A cautious administrative body would, with knowledge of the individual's PIN and with EDP facilities, have real time access to the individual's tax file held by the administrative body responsible for fiscal matters. A rapid check can therefore be made on the accuracy of the information submitted by the applicant in regard to his earnings, disposable capital, etc. In verifying the accuracy of information submitted to it for various purposes, the administration, thanks to the acceptance of one identifier for a range of administrative purposes, is also able to combat fraud. And this aspect of single identifiers is also seen as justifying their existence.

ii. Perceived risks for the individual

It is noteworthy that in certain countries debates in regard to the introduction or use of PINs triggered off the debate on data protection. In some countries the debate culminated in the adoption of data protection legislation. By way of example, the French Data Protection Law of 6 January 1978 had its genesis in the discussions surrounding the proposed SAFARI project in the mid-seventies which envisaged file-interconnection on the basis of the index identification number. Germany may also be seen as another country where the dangers of coupling PINs with EDP engendered discussions which resulted in the introduction of the Federal Data Protection Bill (which became law in 1978). Article 35 of the 1989 Portuguese Constitution is also interesting in this regard since it juxtaposes a prohibition on file-matching (Article 35.3) with a prohibition on the allocation of single identifiers to members of the public (Article 35.5), and all this against the background of a recognition of the rights of the citizen *vis-à-vis* EDP.

Whether justified or not, these factors reveal strong psychological and emotional concerns in regard to the introduction and use of single identifiers. It is interesting to note that the Constitutional Court of Germany has stated that the introduction of universal PINs would constitute a possible attack on human dignity by opening up possibilities of social control through increased possibilities for file-interconnection and individual and group profiling. This issue of human dignity is also reflected in public fear that individuals will be reduced to "numbers". The state, this argument proceeds, will fail to treat the individual as a human being worthy of respect. This sort of widespread belief goes hand in hand with fears of the gradual emergence of a state endowed with Orwellian characteristics of total control and with increased possibilities for constant surveillance of its members.

There is no doubt that, at least in so far as universal PINs are concerned, real doubts are again being expressed in regard to their introduction and use. For example, the 1989 Privacy Act of Australia was foreshadowed by a vigorous campaign against the surveillance possibilities of a proposed so-called "Australia card" equipped with a number for each holder of the card. The project was dropped and the new Privacy Act has considerably circumscribed the use of the tax file number. In Canada, successive Privacy Commissioners have sounded warnings in regard to the "creeping" general application of the social security number. For example, in his annual report for the year 1985-86, the Privacy Commissioner stated that "unwanted information linkage through a social insurance number may still be easier than through any other single piece of personal information". The Privacy Commissioner here expresses his concern in regard to the fact that the social insurance number (SIN) launched in the mid-sixties has rapidly surpassed the context of social insurance and has become the most frequently used PIN in Canada and is now providing the key to the matching of administrative files containing personal data collected and stored for different administrative purposes. Again in Canada, the 1987 report of the Standing Committee on Justice and of the Solicitor General ("A review of the Access to lnformation Act and the Privacy Act") made strong recommendations on the need to contain the use of the Canadian social insurance number. The report noted that the number was "so important, so special and so much a symbol of the need for the data protection that it demands certain controls over its use". In its response to the parliamentary committee, the federal government indicated that it would act to ensure that the SIN did not become a universal identification number. In June 1988, the federal government restricted the use of the SIN. Any new uses of the SIN by federal government institutions after that date required parliamentary approval. A companion policy issued by the federal government in June 1989 required that federal government institutions notify individuals of the purpose for which their SIN was being sought and whether any rights, benefits, or privileges could be withheld or any penalties imposed if the number was not provided. The federal government is also working with provincial governments to determine whether the use of the SIN in their jurisdictions could be restricted as well.

In the United Kingdom, new proposals continue to arise for the use of PINs in both the public and private sectors - for example in connection with the new local tax, the community charge, and for the use by credit reference agencies. The Data Protection

Registrar has commented on these and other proposals and has warned of the risks attendant on the uncontrolled use of PINs.

So PINs are again topical. The Data Protection Law of the Netherlands adopted in December 1988 was brought on by the discussions on PINs. The Swedish Government saw fit to ask its Commission on Data Protection and the Principle of Publicity to examine the privacy risks attendant on the use of the PIN.

There is no doubt that PINs, in conjunction with automatic data processing, tend to increase the power of the administration. As stated above, file interconnection via the use of unique identifiers allows administrative bodies to match up personal information held in various distinct files. Accumulating data in this way excludes the data subject from the information circuit. It is no longer necessary for a particular administrative body to contact the individual with a view to acquiring information or checking information he has already furnished. The administrative body can conduct checks and controls by referring to other personal data files held by different parts of the administration. The administrative body can also "top up" the information it holds by borrowing information held by other such bodies for different administrative purposes. A single multi-purpose identifier for each member of the population is a critical part of this administrative process which can lead to an enormous increase in power within the administration.

When a single, unique PIN is not confined to public sector uses, but also applies to the private sector, the risks posed by increased administrative power are naturally even greater. Such assessments of PINs in terms of "power" not unnaturally raise questions relating to individual freedoms and control, since the citizen's anonymity is reduced by a number which may stay with him for life, making it easier for the authorities to trace his whereabouts, movements, etc., to compile information from different personal data files without his knowledge and to take decisions affecting him on the basis of such accumulated information. This analysis applies at the level of groups as well as at the level of the individual.

Over and above these considerations, other risks may be identified:

a. the fact that the PIN may contain coded information which is intelligible only to the authorities to which it is presented, and possibly only intelligible by virtue of machine-readable facilities;

b. the fact that the PIN may be composed of information of a sensitive nature or information of a strictly personal nature (for example, some people may not like to carry a number which reveals that they are divorced, or that they are 50 years old, or 60 years old, or whatever);

c. certain PINs may not be immutable. Their composition may change in accordance with significant events in the life of the holder. For example, the sex of the holder may change. In such circumstances it is necessary that the old number is destroyed or at least kept secure;

d. there is a risk that a PIN may enable information contained on statistical data bases to be matched to individuals if the statistical data are related to the PIN;

e. pressure may be brought to bear on the holder of a PIN to release the number to authorities providing goods and services, although such circumstances may not have been contemplated at the time the PIN was allocated. For example in Sweden, it has been noted that disclosure of the PIN is often a *sine qua non* of obtaining credit facilities, services, membership of an association, etc. If a person is unwilling to disclose his PIN, he must be prepared to accept a negative reply.

f. this last factor gives rise to a more general, indeed more significant consideration, namely the possibility (and some of the national reports show that it is a reality) that a context-specific PIN will gradually creep out of its original defined context so as to enjoy acceptance in other contexts and, at worst, become of general application. Lack of safeguards at the time when single identifiers or context-specific identifiers are introduced in regard to their subsequent use, or overly vague restrictions on their subsequent use and the bodies which may use them, brings about this situation.

CHAPTER 3
An analysis of the legal safeguards on the introduction and use of PINs

No specific reference is made in international human rights instruments to PINs. Neither the European Convention on Human Rights nor the data protection convention alludes to them. However, both international treaties are of particular relevance to the use of PINs.

For example, the use of PINs by public authorities in certain ways for certain purposes may raise issues under Article 8 of the European Convention on Human Rights (the right to private and family life, home and correspondence). Consistent with the approach of the European Court and the European Commission of Human Rights who regard the Convention as a living document which evolves so as to meet new problems, data protection has come to be regarded by both organs as a right falling within the scope of Article 8 of the Convention. The Commission has on at least three occasions been confronted with issues relating to the use of PINs by public administrations:

Lindquist against Sweden (No. 10879/84);

Lundvall against Sweden (No. 10473/83);

Kolzer against Sweden (No. 11762/85).

Although these cases were rejected by the Commission as disclosing no breach of Article 8, it is nonetheless important to note the fact that PINs may in certain circumstances raise Article 8 issues.

As regards the data protection convention, it is no doubt the case that the basic principles laid down therein act as measures of control on the use which can be made of PINs. This

view is premised on the fact that PINs are intimately linked to personal data processing. As noted above, they are the key to personal data files. Even a serial number of no particular significance may open up a personal data file containing sensitive information. It is with these considerations in mind that care should be taken so as to conceive of PINs as:

i. bits of personal information linked to personal data files;

ii. key instruments in the whole field of data processing.

Applying the provisions of the data protection convention to PINs, the following conclusions could be drawn:

- PINs fall within the definition of personal data set out in Article 2.a of the convention;

- data users should obtain a PIN from an individual fairly and lawfully in accordance with the requirements of Article 5.a of the convention. This could mean that there must be a statutory requirement of lawful authority to enable a PIN to be requested from its holder. In the absence of such superior justifications, the individual's free and informed consent should be sought before it may be collected;

- PINs should respect the purpose for which they have been initially envisaged and should not be used in a way or for purposes which were not contemplated (Article 5.b of the convention). For example, it is doubtful whether this principle would be respected if a context-specific PIN, the use of which was strictly defined by statute, were to be used as an aid to file-matching or were to be used in a whole variety of other situations;

- a PIN should not be composed of too many personal data, given the purpose for which it is to be used (Article 5.c of the convention);

- PINs should be accurate and reflect changes in the circumstances of the bearer (Article 5.d of the convention);

- PINs should not be composed in such a way as to reveal the categories of sensitive data referred to in Article 6 of the convention;

- PINs should be kept secure against unauthorised access or dissemination to third parties (Article 7 of the convention);

- the holder of the PIN should be able to exercise rights of access, rectification and erasure in regard to the data contained on a coded PIN as well as, of course, to the personal data files to which the PIN relates (Article 8 of the convention).

To conclude this section on safeguards at the international level, reference should be made to Principle 5 of Recommendation No. R (86) 1 of the Committee of Ministers of the Council of Europe on the protection of personal data used for social security

purposes. The drafters of the recommendation intentionally alerted governments to the dangers accompanying the introduction or use of a single, uniform, social security number. Principle 5 of this recommendation states that adequate safeguards should be taken in the event of the introduction or use of such a number. In drafting this provision, it was recognised that fears are often aroused by identifiers. The explanatory memorandum to the recommendation notes in addition that what was originally planned as a number issued for the social security context could quickly become an all-purpose standard number. The drafters felt that such all-purpose standard identifiers should not be introduced in such a clandestine manner. It is also interesting to note that the drafters of the recommendation encourage governments to provide safeguards in respect of information contained on social security numbers or similar means of identification. For example, such information should be readable and not excessive having regard to the purpose for which it is used.

Safeguards set out in national legislation

The links between the introduction and use of PINs and data protection are confirmed by the specific reference to them in certain national data protection laws - for example both the French legislation and the Norwegian legislation make specific reference to identifiers. Section 18 of the French law of 6 January 1978 states in fact that the use of the national index identification number with a view to personal data processing may only be authorised by order of the *Conseil d'Etat* after an opinion from the CNIL. Since 1978 the CNIL has only issued about fifteen favourable opinions on the use of the number. The CNIL has built up extensive case law on the interpretation of Section 18 and has sought, among other things, to restrict the interpretation of the meaning of the word "use". For example, the CNIL considers that the mere fact of consulting the national index, even where the number is not retrieved (for example, to check identities), comes within the scope of Section 18 and requires the order of the *Conseil d'Etat.* In Denmark, the data protection legislation governing private registers provides that the PIN may only be stored by private bodies if this is authorised by law or if the individual has given his consent, and provided it is necessary for the body to possess the information to satisfy legitimate requirements.

The link between data protection and PINs is also established even in the absence of specific reference to the competence of data protection authorities to intervene on occasions when the use of PINs raises problems of a data protection nature. For example, in countries such as Austria, Iceland and Luxembourg the data protection authorities have shown their willingness to police the use of PINs. Even though there are in principle no provisions which expressly prohibit or restrict the use of PINs in Sweden, this has not prevented the Swedish Data Inspection Board from asserting its competence when authorities seek to match files with the aid of PINs. Under the Swedish Data Act, it is in principle necessary to have the approval of the Data Inspection Board before matching can take place. The Data inspection Board, in accordance with Section 6, paragraph 1, of the Data Act, may prescribe how the PIN should be used in the file or it may prohibit the use of the PIN altogether, The Data Inspection Board has also issued general provisions regarding the use of PINs in customer files. When associations according to their

regulations have decided that the PIN of the members should be registered, the individual has to accept that he will be refused as a member, if he is not ready to disclose his PIN. However, if the disclosure of the PIN can be considered as an unreasonable condition, the Data Inspection Board is competent to forbid the registration. The question can also be reported to the National Swedish Board for Consumer Policies. As noted earlier, in the case of Canada and the United Kingdom the competent data protection officials are prepared to engage in the political discussions surrounding the introduction or use of PINs.

Even in countries without data protection legislation it may still be possible to locate a body competent to supervise and issue guidelines on the use of PINs. For example, Belgium has an advisory and consultative committee on matters affecting private life and the committee has shown its readiness to regulate PINs, although the point was made at an earlier stage that the intervention of this body has not prevented the PIN from surpassing its original purpose.

Leaving aside the framework of data protection legislation, the laws which usher PINs into society may also contain specific safeguards regarding their use as well as the individual or bodies competent to use PINs. For example, this is the experience of countries which have legislation governing population registers (Denmark, Norway, the Netherlands) or which have introduced specific PINs in specific contexts (Portugal, Switzerland). In Spain, the legal framework created by Decree No. 196/76 as supplemented by Decree No. 1245/1985 for administration of the national identity card which incorporates a PIN, stipulates in Article 6 that "private life must be respected" in the management of the card by public authorities including the carrying out of identification inquiries by the services of the Interior Ministry responsible for the national identity card.

CONCLUSIONS

Conclusions and proposals to be borne in mind by data protection policy makers and data protection authorities in the area of PINs

As the above analysis illustrates, the introduction and use of PINs is not a neutral issue either in the countries which already have extensive experience of their use as universal multi-purpose identifiers or context-specific identifiers, or in countries where the introduction of universal PINs is mooted. At the very least, careful evaluation of the cost (in terms of data protection/privacy problems) or benefit (in terms of increased administrative efficiency and lower economic costs brought about by the use of PINs) is an essential part of the debate in either of the models.

It is felt that this cost/benefit analysis should be made up of the following factors:

i. Where a system of PINs is already in force, restrictions should be placed on their use so as to bring about the requisite balance between privacy and administrative efficiency. Such restrictions should take the form of legal controls exercised by means of intervention on the part of independent authorities such as data protection authorities, or which are built into legislation governing the use of PINs by public powers. Data

protection legislation may expressly provide for controls on the use of PINs by public powers. This is one option, and it is favoured by certain countries. Nevertheless, the absence of specific reference in data protection legislation to the use of PINs by public powers does not exclude the competence of the supervisory authorities instituted under such legislation. It is, after all, the case that PINs are the key to data processing. The collection, storage and use of personal data may be done on the basis of a PIN. File interconnection, as shown previously, is considerably facilitated by the use of the PIN. At a simpler level, PINs constitute personal data. In short, data protection authorities are competent bodies to supervise and regulate the uses which may be made of PINs.

ii. Where universal or multi-purpose PINs are already in existence or where their introduction is being considered, legal safeguards are essential. In the first place, they should only be introduced on a legislative basis. Their use should be carefully defined by that legislative framework. Where there is no legal basis for requesting an individual to disclose his PIN, the individual should be told that he is at liberty to withhold its disclosure without suffering any detriment. It is felt that this principle should be part of the legislative framework accompanying the introduction and use of PINs.

iii. The need for an accompanying legal framework for the introduction and use of universal or multi-purpose PINs is a guarantee that context-specific PINs will not surpass the frontiers of the original planned use so as to become of general application in all contexts, without the requisite public debate and legislative framework which must characterise the introduction of universal identifiers. With this in mind, care should be taken to ensure that specific PINs are confined to their specific contexts. In the absence of legal authorisation, an individual should not be obliged to disclose his PIN in a context in which it was not intended for use. Once again, an individual who withholds his consent to disclosing his PIN should not suffer any detriment. In fact, it should be unlawful for any public or private body to require communication of the PIN unless the request is authorised by law.

iv. File matching or relating personal data bases by means of PINs deserves particular attention. Specific controls and safeguards should govern the use of PINs for such purposes so as to avoid excessive power accruing to public authorities. Transparency should characterise any attempts to interconnect files held by different parts of the administration. The circumstances in which file interconnection within parts of the administration can take place should be known in advance. Legal authorisation should be sought so as to enable it to take place - for example, the approval of the data protection authority.

v. Since PINs relate to identified individuals they constitute personal data. They are thus subject to data quality principles. This factor was noted above in justifying the competence of data protection authorities to supervise the use made by public and private bodies of PINs. However, it is also felt that their introduction and use also attract the rights and remedies accorded to data subjects under data protection legislation. This would suggest that individuals should, for example, be entitled to rectify the composition of a PIN when it no longer reflects the situation or status of the holder. For example, where a PIN reflects the nationality or the marital status of its holder, a right of

rectification should be granted to enable the holder to have the PIN reconstructed in the event of a change of nationality, or a marriage or widowhood. PINs should not be constructed in such a way as to make use of or reveal sensitive data. It should not be possible for the PIN to hint at the nationality, ethnic origin, etc., of its holder. More than this, attempts should be made to construct PINs without having recourse to personal data at all. For example, consideration could be given to the use of serial or "clean" numbers. Should it be the case that personal data are the basis of the PIN, such data should not be unnecessary or disproportionate to the uses made of the PIN.

vi. PINs should be composed in such a way as to be intelligible to the holder. They should not be coded in a way which would prevent the holder from appreciating the significance of the digits or letters or references making up the PIN.

vii. Individuals should be instructed in how to manage and keep safe PINs so as to prevent their misuse by third parties.

In putting forward these proposals the drafters have confined themselves to various types of personal identification numbers. They were, however, conscious of the fact that other types of identifiers (name, address, etc.) may allow public authorities to match up different types of personal data files. It is felt that these ways of relating databases raise the same problems for individual rights and freedoms. Accordingly, the principles advanced above in regard to legal safeguards and transparency for file interconnection, as well as the principles of functional separation, apply to use of non-PIN-based identifiers.

The drafters were also conscious of new techniques for identifying individuals. For example, genetic fingerprinting, voice prints, iris identification. The drafters conclude that in regard to these new sorts of identifiers particular care is required before their introduction and use. In particular, public discussion should take place so as to find the right balance between privacy and the supposed advantages which they create.