DECISION 15 OF 1991: 13 APRIL 1991

ON THE USE OF PERSONAL DATA AND

THE PERSONAL IDENTIFICATION NUMBER

The petitioner sought constitutional review of several legal rules on the grounds that they violated the right to the protection of personal data under Art. 59 of the Constitution.

Act X of 1986 on the State Population Register provided *inter alia*, that under (a) s.1(1), the objective of the Register was to promote the enforcement of the citizens' rights and the fulfillment of their duties, to provide assistance for the activity of state and private organisations; (b) s.1(2) the duty of the Register was the collection of data necessary for unified personal data records and the keeping and supply thereof; (c) s.3 there was an obligation to supply data on education and professional training; (d) s.4 the Register was to contain the citizen's personal identification number ("PIN"), and basic identification and residence data, the scope of which data to be recorded being delegated to the Council of Ministers; (e) s.6(2) for the compulsory introduction of the PIN into the Register and into the procedures for the administration of justice and of the State; (f) s.7(1) the Register (for its services) could use data from other records if the organisation concerned approved; (g) s.7(2) a private person could request rightful interest, such application being certified by his own statement or by an official document. The Register was to supply data to state and private organisations to facilitate the performance of their duties; (h) s.7(3) the mandatory regular data supply to certain organisations for the performance of their basic

tasks, such organisations to be determined by decree of the Council of Ministers; (i) s.8, provision of data could be refused if it violated a citizen's personality rights; (j) s.10(2) the citizen had the right to correct the data on himself; and (k) s.10(3) personal data could only be made public in cases specified by an Act or by the Council of Ministers.

Two Decrees of the Council of Ministers were also issued to give effect to various provisions of the Act: Decrees 25/1986 (VII.8) and 102/1990 (VII.3). Under the former, it was provided, *inter alia*, that (a) in para. 1(1)(o) the registration of the PIN for the father, mother, children and spouse of the person in question was required; and (b) in para. 5(2) the person/organisation requesting data from the Register could only use it for the purpose indicated in its application, therefor.

The petitioner submitted that (a) the Act was unconstitutional because it did not fulfill the Constitution or the regulatory level necessary for the regulation of fundamental rights as required by Law Decree 11 of 1987 on Legislative Competence; (b) the provision of mandatory data was prescribed in such a way that the scope of data to be provided was to be determined by the Council of Ministers also conflicted with Law Decree 11 of 1987. The authorization did not specify the subject or the limit of its scope. Consequently the Council regulated fundamental rights and duties for which it could not be authorised; and (c) it was unconstitutional for a Council of Ministers' Decree to determine who received the mandatory data and who, based on such data, established rights and duties; moreover the protection of personal data in the hands of such recipients could not be guaranteed.

Held, granting the petition:

(1) In the absence of a definite purpose and for arbitrary future use, the collection and processing of personal data were unconstitutional. The right to the protection of personal data, the so-called right to informational self-determination, as guaranteed under

Art. 59, permitted everyone the freedom to decide about the disclosure and use of their personal data to the extent that the approval of the person concerned was generally required to register and use it. In addition Art. 59 ensured that such person could monitor the entire route of data processing thereby guaranteeing the right to know who used the data and when, where and for what purpose it was used. A statute could exceptionally require the compulsory supply of personal data and prescribe the manner of its use provided it complied with Art. 8 (page 00, line 00 - page 00, line 00).

(2) In addition the principle of adherence to the goal to be achieved was a condition of and the guarantee for exercise of the right to informational self-determination. Personal data might therefore only be processed for a definite and legally-justified purpose to which every stage of the process had to conform. The person concerned was to be informed of the purpose for the data processing in a manner which allowed him to assess its effect on his rights, to make a well-founded decision on its provision and to enforce his rights were the use of such data to depart from the original purpose. If there were any possible alteration in the purpose, the person was to be notified unless a statute permitted otherwise (page 00, line 00 - page 00, line 00).

(3) The definition by the Act of the purpose and scope of collection of data processing violated a person's right to human dignity. The protection of the right to informational self-determination in the process of data forwarding was to be ensured through guarantee-based regulations and the adherence to the purpose to be achieved which had to be present at every stage from the supply to the elimination of such data from a record. Since the Register the data processing for which was "for the purpose of storage" lacked any tangible objective, this resulted in a gap in continuity in purpose from

the data-forwarding stage onwards as well as the lack of legitimacy of an alteration in the purpose thereof. Moreover it was clear that a data processor with an undefined scope for data collecting would become familiar with personal data in their entirety and in their context. Taken out of its original context, the data used to create a "personality profile" violated the personality rights of the person concerned (page 00, line 00 - page 00, line 00).

(4) The collection of data and its processing were unconstitutional. Section 1 of the Act provided a definition of the objective of the Register and its duties which were inadequate and vague, incapable of guiding data processing in a definite direction or restricting it in any way. In addition under s.4, data collection for storage purposes had no definite purpose or scope. There was no detailed list of the data to be included in the Register and instead the Act gave a broad authorization to the Council of Ministers to draw up such list. However it had gone beyond its authorization under ss.3-4 when it included for compulsory registration the PIN of the person's father, mother, children and spouse thereby violating the personality rights of the person since it used relationships without his knowledge (page 00, line 00 - page 00, line 00).

(5) Further, s.7 was unconstitutional since it gave unlimited freedom to the data processing of the Register. The person concerned was not required to give his approval to the processing neither was there a duty that once the specific service had been completed the data was to be deleted or that a record of such amendments was to be kept with the data. Moreover, when combined with data from other sources, the data in the Register could provide different information on a person who would be ignorant of its provision. Consequently, in order to render constitutional the acquisition of data from other records

or its forwarding, the data would have to be used solely for the purpose of original record-keeping and made available only to the audience with whom the person would have to deal in connection with the original record-keeping. Data outside the collection remit of the Register would have to be deleted after forwarding while the request and forwarding of data would need to be documented (page 00, line 00 - page 00, line 00).

(6) In addition, different stipulations under s.7 provided for data supply or forwarding to private persons, i.e. having a "rightful interest" in another person's data, or to organisations "to facilitate the performance of their duties" which did not sufficiently take into account a person's right to data protection. These objective conditions were of themselves incapable of providing the requisite basis for protection under s.8 according to which subjective criterion, supply could be refused if it might violate personality rights. The supply of personal data for the performance of a specifically-defined task and the performance of which possibly justified the risk involved in the supply alone complied with personality rights protection. Only organs of state administration and the administration of justice were given such tasks so that identical restrictive conditions were to be imposed on providing data to these organs and to "organizations" other than private persons - the right to informational self-determination could be enforced if based on a right documented and certified in writing on the same footing as private persons. Finally the requirement of mandatory regular data supply in s.7(3) to local governments and to ministries for the performance of "their basic tasks" was insufficient to permit constitutional data-forwarding and those entitled could only be determined by statute not merely by executive decree (page 00, line 00 - page 00, line 00).

(7) The express guarantees of personality rights in the Act failed to meet all the criteria of constitutionality. For instance, s.10(2) only provided the right to make corrections for the person concerned. Since the essence of the right to informational self-determination was that the party concerned might know and follow the route and circumstances of the use of his personal data, the preconditions necessary for the exercise of this right were to be ensured: applications for data on certain subjects were to be officially documented in the Register, *i.e.* records on whose data was supplied to whom, when and for what purpose, as well as the use of other data systems. Certification would also facilitate possible corrections which would need to be made in all registers receiving the wrong item of data. Further the right to correction should also be extended to deletions. By s.10(3), personal data could only be made public in cases specified by statute or executive decree which general authorization of the latter, in view of the current decision, was also unconstitutional. The right to informational self-determination might be limited only in unavoidable situations, the justified exceptions to the rule being determined by statute. Therefore only where the person concerned could forbid the provision of his data recorded in the Register would the protection of personality rights satisfy the Constitution (page 00, line 00 - page 00, line 00).

(8) Finally the general and unified PIN available for unlimited use was unconstitutional. Section 6(2) permitted the use of PINs in any official document and record or computerized register system and was thus broader in scope than the Register: indeed, it failed to limit or impose conditions on the use of PINs. The PIN threatened personality rights particularly where data was acquired from various databases without informing the person concerned: he was therefore limited in or deprived of the possibility of monitoring the dataflow. Further this mass of interconnected data, of which the person

generally had no knowledge, rendered him defenceless and created unequal communication conditions so that one party possessed information giving a particular (distorted) image of which the other party concerned was unaware. The power of the state administration in using PINs was also markedly extended. Where they were used outside the ambit of the administration, this increased the power not only of the data processor over the parties concerned but also of the State since it further broadened (possible) control through use of such data. Taken together, they seriously jeopardized the right to self-determination and human dignity. Accordingly PINs remained contrary to the right to data protection, to the principle of divided information systems with adherence to the goal to be achieved and to the main rule that data was to be acquired from persons with their knowledge and consent (page 00, line 00 - page 00, line 00).

IN THE NAME OF THE REPUBLIC OF HUNGARY!

Pursuant to a petition submitted to request an investigation into the unconstitutional character of a legal rule in force, the Constitutional Court has made the following

DECISION.

The Constitutional Court rules that the collection and processing of personal data in the absence of a definite purpose and for arbitrary future use are unconstitutional.

The Constitutional Court rules that the general and unified personal identification number ("PIN") available for unlimited use is unconstitutional.

The Constitutional Court rules that Law Decree 10 of 1986 on the State Population Register as well as Decree 25/1986 (VII.8) MT issued by the Council of Ministers for the execution of this order and Decree 102/1990 (VII.3) MT issued by the Council of Ministers are unconstitutional; accordingly, the said Law Decree and its subsequent executive decrees are declared null and void.

The nullified legal rules shall be ineffective as of 31 December 1991, with the exception of their provisions listed hereunder which shall become null and void upon the publication of the present Decision in the *Hungarian Official Gazette*:

In the Law Decree:

The second sentence of s. 4,

Section 5(2),

The second and third sentences of s. 6(2),

Section 6(3),

The second sentence s. 7(1),

In s. 7(2): "unless otherwise provided for by the legal order...", "or its rightful interest...", and "or with its declaration...",

Section 7(4), as well as

In s. 10(3), the words: "in statutory instrument or decree by the Council of Ministers...".

Accordingly, in the period between the publication of the Constitutional Court Decision and 31 December 1991, s. 4, s. 6(2) of the Law Decree, and s. 7(1) and (2), and s. 10(3) thereof shall remain in force with the following text:

"*Section 4*: The state population register contains the citizen's PIN, his basic personal identification data and the address of his residence."

"*Section 6(2)*: The PIN shall be used for the purposes of identification in the computerized registers which contain, among others, personal data as well."

"*Section 7(1)*: The state population register provides data to private persons, and to organizations for the performance of their duties.

(2) A private person may request from the state population register data and issue of documents pertinent to other persons to which he is entitled. The applicant shall verify this entitlement by a `written deed.`"

"*Section 10(3)*: Data related to the citizen's person, family status and other circumstances may be made public only with the approval by the citizen concerned, or in cases determined by an Act of Parliament."

The Constitutional Court orders the publication of its Decision in the *Hungarian Official Gazette*.

REASONING

I

The petitioner contested the Law Decree 10 of 1986 on the State Population Register (hereinafter the "Act") and its two executive decrees, Decree 25/1986 (VII.8) MT and Decree 102/1990 (VII.3) MT by the Council of Ministers in their entirety, on the grounds that these are contrary to the constitutional right to the protection of personal data (Constitution, Art. 59). The petitioner requested all three legal rules be repealed.

The petitioner argued that the Act fails to fulfil either the Constitution or the regulatory level required for the regulation of fundamental rights by Law Decree 11 of 1987 on Legislative Competence and is, therefore, entirely unconstitutional. According to

the petitioner the fact that the Act prescribes the provision of mandatory data in such a way that the scope of data to be furnished is determined by the Council of Ministers is also in conflict with the 1987 Law Decree on Legislative Competence. This authorization does not specify the subject or the limit of its scope. Thus, the Council of Ministers regulates fundamental rights and duties for which it may not receive authorization. The petitioner also considers it unconstitutional that a decree by the Council of Ministers determines the recipients of the provision of mandatory data who, based on these data, establish rights and duties, furthermore the protection of personal data in the hands of these recipients may not be guaranteed.

II

According to Art. 59 of the Constitution everybody is entitled in the Republic of Hungary to the right to good reputation, to the inviolability of private premises as well as to the protection of private secrets and personal data.

The Constitutional Court, continuing to adhere to *Dec. 20 of 1990 (X.4) AB* (MK 1990/98), does not interpret the right to the protection of personal data as a traditional protective right, but as an informational self-determination right, with regard to the active aspect of this right.

Thus, the right to the protection of personal data, as guaranteed by Art. 59 of the Constitution, means that everybody is free to decide about the disclosure and use of his own personal data. Hence, approval by the person concerned is generally required to register and use personal data; the entire route of data processing and handling shall be made accessible to everybody, *i.e.* everybody has to right to know who, when, where and for what purpose uses his data. In exceptional cases, an Act of Parliament may order the

compulsory supply of personal data and may also prescribe the way these data may be used. Such an Act of Parliament restricts, the fundamental right of informational self-determination, and it is constitutional only if it is in accordance with the conditions specified in Art. 8 of the Constitution.

Any legal rule which, irrespective of the procedure to be adopted, provides for the taking, collecting, storing, handling, forwarding, publicizing, altering, preventing further use, producing new information or on any other use of personal data (hereinafter: processing of personal data) shall be in conformity with Art. 59 of the Constitution if it comprises guarantees that the person concerned is able to monitor the route of his data during the processing and to enforce his rights. The legal institutions for this purpose, therefore, have to secure the concerned party's approval to the processing and have to contain specific guarantees for those special cases when data processing may take place without the approval of the person concerned (possibly without his being aware of it). These legal institutions in charge of these guarantees for the purposes of verification have to contain the route of the data within objective limits.

Adherence to the goal to be achieved is a condition of and at the same time the most important guarantee for exercising the right to informational self-determination. This means that personal data may only be processed for a definite and legally justified purpose. Every single stage of the data processing shall conform to the declared and authentically set objective.

The person concerned shall be informed of the purpose of the data processing in such a way so as to enable him to judge the effect of data processing on his rights, and to make a well-founded decision on the provision of his data; furthermore, to allow him to enforce his rights if the use of his data deviates from the original purpose. For the same reason, the person concerned shall be notified about any possible change in the purpose of

the data processing. Processing with a new purpose is legal without the concerned person's approval only if it is expressly permitted by an Act of Parliament with respect to the data in question and to the processor. It follows from the principle of adherence to the goal to be achieved that collecting and storing data without a specific goal, "for the purpose of storage", for an unspecified future use are unconstitutional.

The other basic guarantee is the restriction on the forwarding and publication of data.

Data forwarding, in the strictest sense, means that the data processor makes the data accessible to a certain third party. Publication of the data means that any third person can have access to the data. Those, usually professionals, who are entrusted by the data processor to perform the physical or the computer-related activity of data processing are not considered "data processors", and their access to the data does not constitute "data forwarding". The responsibility of such a party can be regulated separately, without affecting the data processor's full responsibility with regard to its own data processing activity or that entrusted to somebody else by the data processor.

Personal data may be made accessible to a third party, other than the concerned party and the original data processor, and thereby to link up data processing systems, only if all the conditions required for data forwarding as related to each item of data are fulfilled. This, therefore, may mean that the recipient of the data forwarding activity (the one who requests the data) shall either have a specific authorization by an Act of Parliament to process the forwarded data, or it shall have approval by the concerned party. Adherence to the goal to be achieved is, of course, the major impediment to data forwarding. The requirement of adherence to the goal to be achieved, and the above specified conditions of change in the goal to be achieved and data forwarding also impedes the flow of data within and among state administrative organs.

III

The contested Act is unconstitutional because it fails to meet the basic requirement for the adherence to the purpose to be achieved. Particularly,

- it does not specify the objective of data processing;

- in connection with this it does not determine precisely the scope of data to be processed;

- it allows the use of other unspecified records and registers for services related to the population register;

- it does not secure adequately the rights of the affected persons, in particular it does not contain sufficient guarantees concerning data forwarding for the protection of the affected party.

1. The definition by the Act of the purpose and the scope of collection of data processing is unconstitutional.

Section 1(2) of the Act states that the duty of the state population register is the collection of data necessary for unified personal data records, the keeping of records and the supply of these data. According to s. 4 of the Act the register contains "basic data on personal identification and residence" (the definition of these is delegated to the Council of Ministers), but s. 3 also prescribes the obligatory supply of data on educational and professional training. These are traces of the concept, revealed also in the Act, to establish an integrated personal data bank which contains the most extensive possible data base on citizens, ranging from data on health status and property to data on personal affairs with official bodies. This concept required the compulsory introduction of the PIN into the

population register and in addition, into procedures of state administration and into the administration of justice (s. 6(2)).

This idea was incorporated even at the end of the eighties in the concepts for development of the State Population Register Office. Social opposition in the USA in the mid-sixties, and in France and West Germany in the seventies led to the abandonment of similar plans for integrated, central state-managed register. The problems which surfaced in connection with the creation of central data banks triggered everywhere legislative measures on data protection.

Data processing "for the purpose of storage", without a fixed purpose, and which in the absence of a defined goal is indivisible according to the different aims for use and is involved in the provision of any data to a previously undefined scope of agencies is not in and of itself unconstitutional. The absence of adherence to the goal to be achieved shall not be substituted by controlling data communication on the basis of guarantee-based regulations. Subjecting data-forwarding to certain conditions and to the adherence to the purpose to be achieved present combined and not alternate guarantees for informational self-determination.

Adherence to the goal to be achieved shall prevail from the supply of data to the cancellation of the same from the record.

No solution may be constructed constitutionally where one component of the constitutional right, the adherence to the goal to be achieved with respect to a central integrated data bank operating without a definite purpose, applies only to the data collector. The so-called "legal data quality" shall exist at all stages of the processing. The fulfillment of certain guarantees in certain processing stages is insufficient; this may not remedy the unconstitutional character of other phases. This is the reason why the provision in para. 5(2) of Decree 25/1986 (VII.8) MT of the Council of Ministers, which

rules that the party requesting data from the population register may only use these data for the purpose indicated in the application for data is insufficient. This otherwise self-evident obligation of the applicant is not a substitute for the absence of a tangible objective of the population register and for the resulting lack of continuity in purpose that is missing from the data-forwarding stage, or the lack of legitimacy of an alteration in the purpose.

Independently of the constitutionality of data forwarding in itself, it is obvious that a data processor with an indefinite scope for data collecting becomes familiar with personal data in their entirety and in their context. This leads to a complete exposure of those subject to data collection to the processor, also provides access to the private sphere of these persons, furthermore, it results in an unequal situation of communication in which the party subject to data collection does not know what the data processor knows about him. The so-called "personality profile" that is created from data taken out of its original context particularly violates personality rights, and the avoidance of this is a basic concern in judging the legal status of the various data-processing activities because this is concomitant to an extensive but undetermined scope of data collection in the data processing. For all these reasons such data processing violates human dignity.

The Constitutional Court has not found any constitutional right or interest that would make it unavoidable to restrict the informational self-determination right guaranteed in Art. 59 of the Constitution by the use of data processing with an indefinite purpose, or that would be equal to the harm caused by such a data system. The efficiency of the state administration particularly may not be such an interest because it may not be proven that a data-processing method which seriously violates the right to informational self-determination is the only possible way to the efficient operation of the state

administration system. The data processing system which stores data without a definite purpose is, therefore, considered as unconstitutional by the Constitutional Court.

2. The main provisions of the legal rules concerning the population register are also individually unconstitutional.

2.1 The definition of the objective specified in the Act (s. 1(1): "to promote the enforcement of the citizens' rights and the fulfillment of their duties, is to provide assistance for the activity of state organs, economic and social organizations, associations and associations of private persons' (hereinafter `organizations`)") is completely inadequate in light of the fact that the establishment of a data-processing system affecting the entire population of the country is in question, and, furthermore, this system fundamentally affects personal data and the course of the rights related to it (see: PIN). This vague text is incapable of guiding data processing in a definite direction or of restricting it in any manner, *i.e.* it does not allow at all for the mention of any adherence to a goal to be achieved. Section 1(2) says that "the duty of the state population register is to collect data for a basic unified personal record system...", it confirms that data collection for the purpose of storage and without a definite purpose is involved here which, as stated under s. 4(b) of Decree 25/1986 (VII.8) MT of the Council of Ministers, "will provide for occasional data demands" along with a regular but in the Act unspecified scope of collection (see s. 7(3) of the Act).

2.2 The scope of the registered data is determined in s. 4 of the Act: "The state population register contains the citizens' personal identification number, his basic identification and residence data. The scope of the data to be recorded is to be determined by the Council of Ministers."

This authorization is unconstitutional. Article 8(1) of the Constitution provides that the rules and regulations related to fundamental rights and duties are determined by

an Act of Parliament. The regulation of the processing of personal data obviously refers to a fundamental right, to the right to the protection of personal data specified in Art. 59 of the Constitution.

"Personal record keeping" has already been included with the legislative subjects under s. 5(1) of the 1987 Law Decree on Legislative Competence. Anyone shall be able to determine from the Act on the processing of personal data which of his data are referred to in the Act. In the contested Act the determination neither of the objective of the state population register, nor of its duties (s. 1), nor of the scope of the recorded data (s. 4) is sufficient to specify unambiguously the scope of the data recorded therein.

Given the importance of a state population register, the Act should have given a detailed list of the data to be included therein. Instead, the detailed determination of these data was left to the Council of Ministers in such a way that the scope of this authorization in its contents has not been determined. The term "basic personal identification data" is not specific enough to act as a guarantee. By doing so, the Act gave a free hand to the Council of Ministers on the one hand, while, on the other one, it failed to provide concrete information to those concerned. Otherwise, the Act itself makes the interpretation of its own definition impossible when it requires the obligatory supply of data on education and professional training in s. 3. The executive decree includes these items in the data of the population register, although these may not be included based on the authorization in s. 4 of the Act. Decree 25/1986 (VII.8) MT of the Council of Ministers, however, went beyond even the broadest interpretation of the authorization provided in ss. 3 and 4 of the Act when it, in addition, prescribed the registration of PINs for the father, the mother, the children and the spouse (s. 1(1)(o)). These data may not belong to the basic personal identification data of the concerned party. The chain of personal identification numbers allows, *e.g.* to detect even the remotest relatives. The use of such data can particularly

violate personality rights because it indicates and makes the use of relationships available, without the person`s knowledge, independently of whether the person knows of or visits these relatives; the family tree programme thus conceals dangers similar to those already mentioned in the personality profile.

Furthermore, s. 5(2) of the Act empowers the Minister for Internal Affairs to order the keeping of separate records on persons who reside at certain locations specified in the legal rule. The complete of the definition of the purpose and of the persons concerned makes this authorization unconstitutional even in its content.

The apparent restrictions on the scope of data collection listed in the Act are made completely nonsensical by s. 7(1) which states that the population register "for its services, may make use of data from other records if the organizations concerned approve this." This provision is unconstitutional both from the aspect of the scope of data collection area and from the aspect of adherence to the goal to be achieved.

This provision gives unlimited freedom to the data processing of the state population register, and makes this organization uncontrollable for several reasons: first, the Act stipulates approval only by another data-processing unit and not by the concerned party; second, there is no stipulation concerning the deletion of these "alien" data after the completion of the specific service or the requirement that a record on such amendments shall be kept along with the data of the concerned party; third, when combined with data from other sources, the data of the state population register may provide qualitatively different information on the person who is not aware of the provision of such information. The only constitutional way to acquire data from other records or to forward such data is if these data were used only for the purpose of the original record-keeping, and were not made available to a wider audience than those with whom the concerned party had to reckon in connection with the original record-keeping. Data not belonging to

the state population register's scope of data collection would have to be deleted after forwarding the same while the fact of the data request and the forwarding would have to be documented.

2.3 All legal rules in force concerning data forwarding are unconstitutional.

The Act provides different stipulations for data supplies to "private persons" and to "organizations".

According to s. 7(2) a private person may request another person's data to which he is entitled or in which he has a rightful interest. The applicant shall certify this by his own statement or by an official document. The state population register supplies data to organizations (according s. 7(1) organizations are: state organs, economic and social organizations, associations and associations of private persons) "to facilitate the performance of their duties."

These conditions for the supply of data do not adequately take into consideration the concerned persons' right to the protection of the data but, however, favour those who request the data and the organs of the state population register. They are even unsuitable to serve as a starting point for the implementation of the population register's obligation for personality protection (s. 8).

According to s. 8 of the Act the provision of data shall be refused if it might violate personality rights. This obligation was obviously meant to serve as a subjective filter to be applied after the objective criteria specified in s. 7 are fulfilled. However, the objective conditions: the verbally stated "rightful interest," and the "performance of task" by any organization are, in themselves, insufficient to provide for the protection of personality rights; how could they provide a starting point for the population register to weigh whether the use or supply of certain data violates the personality right of the person concerned. The terms "task" and "rightful interest" are equally tenuous and intangible and

they do not even differ from one another. For example, the "task" of enterprises (and the rightful interest of the entrepreneurs) is to have a profitable operation. Is the National Population Register free to decide whether supplying practically a sale, *e.g.*, for the purpose of advertising as specified under s. 9 of the Act the names and residential addresses of ten thousand people of a certain sex, age and given residential location with given schooling violates their personality rights?

Obviously, only the supply of personal data for the performance of a "task" that is specifically determined and the performance of which possibly justifies the risk involved in supplying personal data is in accordance with the protection of personality rights. According to the Constitutional Court, it is only the organs of state administration and of the administration of justice which are provided with such tasks. If the applicant organization proves that it needs data in order to carry out lawfully a task within its scope of activity, then this limits the types of data the organization may request. If, in addition, this organization specifies the circumstances which guarantee the compliance with the adherence to the goal to be achieved and the security of the data, furthermore if the request for the data is documented by the state population register (to the person concerned as well), then this kind of data forwarding meets the objective requirements for the protection of personal data. After this there should still be an investigation into whether the provision of data based on s. 8 of the Act shall be rejected. The Constitutional Court mentions this example only to show the level of protection that is necessary for the right of informational self-determination, and wishes to illustrate its view that in the absence of such or similar guarantees, s. 7 of the Act is unconstitutional.

It follows from the foregoing that identical and restrictive conditions should be imposed on the furnishing of data to "organizations" other than private persons, state administrative bodies and organs for the administration of justice. For example, the right

of informational self-determination can be enforced in this case if, based on a right (possible "rightful interest") documented and certified in writing, the state population register may, in general, disclose the residential address.

The private person should acquire any additional data from the concerned party if he is really entitled to it, he may even resort to obtain the court's ruling on the matter. On the other hand, the investigative duty mentioned in s. 8 is also applicable to this case: for the protection of the right of the concerned party, the state population register may refuse to disclose even the residential address.

The Constitutional Court wishes to ensure the constitutionally required protection of the right even for the period while the Act is in force. At this point, however, this could only be achieved, with the nullification of certain parts of the legal rule, by preventing the possibility of data supply to organizations unauthorized to regular data supply, and by requiring a written certification of the right of data supply in case of the furnishing of data to private persons. The furnishing of names and residential addresses is theoretically considered constitutional by the Constitutional Court in case the rightful interest is documented in writing. However, since the Court may resort only to the means of annulment, it is not in the position to distinguish between the various users and methods of use of the data stored in the state population register. Subsequent to the annulments ordered by the Court's decision, a private person, may request any of the currently stored data, *i.e.* not only names and addresses by presenting a written certification of his right; any application for data beyond this recall may be restricted based on s. 8 only by the state register weighing the matter. However, it seemed too big a risk to rely on this insecure protection in the case of data being requested on the basis of "rightful interests," and by organizations on the basis of "its tasks."

According to s. 7(3) of the Act, the legal rule may prescribe mandatory regular data supply to certain organizations for the performance of their basic tasks.

These organizations are specified by the two executive decrees. Obviously, the "basic task" of the organizations specified in the decrees, such as councils and ministries, is not in itself a sufficient criterion for a constitutionally acceptable data forwarding. For this reason, and because the personal files and record systems of the local governments and ministries do not constitute a unit and because the principle of adherence to the goal to be achieved limits the interaction of intra-office data-processing systems, the issue as to what data to what registers has to be regularly forwarded shall be determined by an Act of Parliament.

In addition to the content-related unconstitutionality of data forwarding, the unconstitutionality of the formal character of the related authorizations is also applicable in this case: those entitled to regular, compulsory data supply shall not be determined by a decree issued by the Council of Ministers, and a "legal rule" is even less acceptable to specify the scope of the data to be made available.

2.4 The abovementioned shortcomings in the regulations seriously endanger the rights of the party concerned. The explicit guarantees of personality rights specified in the Act are not sufficient either to meet all the criteria of constitutionality.

The obligation of the population register to protect personality rights prescribed in s. 8 of the Act is not feasible since the conditions specified in the Act for data supply in themselves violate personality rights.

Furthermore, it is insufficient that s. 10(2) only provides the right to make corrections for the parties concerned. Since the essence of the right for informational self-determination is that the party concerned may know and follow the route and circumstances of the use of his personal data, primarily the preconditions necessary to

exercise this right shall be ensured. In other words, the applications for data on certain subjects shall be officially documented in the population register, *i.e.* records on whose data were supplied to whom, when and for what purpose will have to be kept. The use of other data systems should also be recorded (s. 7(1)).

Another reason for the certification is that possible corrections would have to be made in all registers which received the wrong item of data. In addition, the right of the person concerned to make corrections shall also extend to deletions as well.

For example, if the population register fails to delete data received from other records, the person in question may require the office to do so. This would naturally also necessitate the right to the inspection of the data (s. 10(1)) to extend to the above certifications; and this right shall not be refused according to art. 83(2) of the Civil Code on the grounds of violating "state or public security interests."

According to the Act personal data may only be made public in cases specified by an Act or by decrees of the Council of Ministers (s. 10(3)). In view of the foregoing, a general authorization provided for the Council of Ministers is also unconstitutional. The Constitutional Court notes that the state population register would satisfy its obligation to the protection of personality rights only, if it forwarded or published personal data in those cases only when the task requiring the supply of data could not be performed by data precluding the possibility of personal identification (anonymous). In the cases of aggregate data request for planning, statistical or business purposes, anonymous data are also of much help to the local governments or to business associations without jeopardizing personality rights.

Since the right to informational self-determination may be constitutionally limited only in unavoidable situations, the protection of personality rights satisfies the Constitution only if the person concerned may forbid the provision of his data recorded in

the state population register. The "unavoidable situations": the justified exceptions to the rule may be specified by an Act of Parliament.

3. The unlimitably general and unified personal identification code (PIN) the use of which is unresricted (*i.e.* the PINs assigned to all the citizens and residents of the country according to the same principle) is unconstitutional.

Section 6(2) of the Act states: "The personal identification numbers shall be used as identification data in the computerized records which contain other personal data; it shall be entered into official documents and records, and shall also be used in state administration and judicial procedures."

According to the restrictive interpretation of this passage the PINs shall be stored in the computers of the population register as identification codes, and that these PINs shall be entered into the files and records of the state population register. In its wider sense, however, this passage allows the use of PINs in any official document and record, moreover, these code numbers have been used for every sort of computerized register system on the grounds that s. 6 is made up of provisions broader than the scope of the state population register. The provision of the Act concerning PINs is, thus, ambiguous; as indicated by actual experience, this provision has failed to restrict unambiguously the obligatory use of PINs.

This ambiguity, however, is only a consequence of the much more serious shortcoming of the regulation from the aspect of constitutional law: this is that s. 6 imposes no limitations or conditions whatsoever on the use of PINs.

3.1 The PIN, as regulated in the Act, is a universal, multi-purpose identification code that may, in principle, be used in any register. It is also in this sense that the Constitutional Court applies the concept of PIN in the reasoning of this decision and in the discussion not strictly related to the Act. (Another type of PIN is an identification number

for the purpose of data processing and which may be used only for that, such as, the pension number and account number. These personal numbers of limited use raise other legal problems related to data protection.) The current legal problem of the relationship between the two types of personal number is that legislation prevents the general use of the personal number which is based on the adherence to the principle of the goal to be achieved.

The significance of the unified personal identification code is that it allows an easy and positive identification of personal data as well as their collection by means of a short and technically easily manageable code which is invariable and may not be interchanged. Thus, the personal number is an obvious concomitant of any sort of integrated record-keeping system; its introduction, both in Hungary and abroad, was a part of the plan to install large, central storage data banks. In addition, the unified personal code is perfectly suitable to the occasional link of personal data available in different registers. Through its use, the data are easily accessible, and may be checked against one another.

These technical advantages enhance the efficiency of data-processing systems utilizing personal numbers, and of the related administrative or service operations. Likewise, this system saves time and costs for those subject to data supply because it makes the repeated furnishing of data avoidable.

These advantages, however, involve serious risks for personality rights and particularly for the aspect of the right to informational self-determination. The PIN is particularly dangerous to personality rights. If the data are acquired from different data bases, without "bothering" the person concerned, by-passing him, then this person is precluded from the data flow, and he is either limited in, or deprived of the possibility of monitoring the route and use of his data. This method contradicts the basic principle of data protection that data should be obtained from the person concerned with his

knowledge. The widespread use of PINs results in impairing the private sphere because even from the remotest data-storage systems established for different reasons may be used to establish a personality profile which is an artificial image extending to an arbitrarily- wide activity of the person and penetrating into the person's most private matters; this image, due to its construction from data torn out of their context, is most likely to be a distorted image as well. In spite of this, the data processor will make its decisions on the basis of this image, will use this image to produce and forward further information concerning the person in question. The large amount of these linked-up data, of which in most cases the person in question has no knowledge, renders the person defenceless and creates unequal communication conditions. Where one party cannot know the information the other party possesses about him creates a humiliating situation, and prevents free decision-making. The power of the state administration in using PINs is unduly increased. If PINs may be used in areas outside those of the state, this does not only yield power to the data processor over the parties concerned but it leads to a further growth in the power of the state because it extends even further the possible control through the use of these data. All this combines seriously to jeopardize the freedom of self-determination and human dignity. The unlimited and unrestricted use of PINs might become a tool for totalitarian control.

The logic of PINs is thus contrary to the constituent elements of the right to data protection, to the principle of divided information systems with adherence to the goal to be achieved and to the principal rule that data should be acquired from parties concerned with their knowledge and consent. If the principles of data protection are applied consistently, the personal number loses its significance because the "advantages" inherent in it cannot be made utilized.

The PIN is the technically most advantageous tool to reliable link-ups of personal data as far as the currently existing data-processing techniques are concerned. Personal data may, of course, be connected to names, and, if necessary, to supplementary identification items like mother's name and residential address. Given the computer capacities available today, the extent of these shall not create a serious problem. "Natural" data might, however, change (*e.g.* names by marriage or name changes), and it might happen that further data are needed to make distinctions; furthermore, in case of variable data (like residential addresses) the permanent updating and monitoring of data is necessary. The difficulties and expenditure involved might constitute a significant item in the cost-and-benefit analysis of data processing, thus creating a natural brake on unjustified data acquisition which might otherwise be encouraged by the readily available PINs. The limitations arising from the right to informational self-determination apply, of course, to any data acquisition and processing. Due to their technical perfection, the PINs require the introduction of special safeguards in accordance with the increased risks. If personal data are updated by a central record-keeping system available through the PINs, then the data-processing body in charge of this operation, like the population register, acquires a key position which, therefore, requires an especially precise regulation by guarantees.

3.2 The PINs, therefore, by their very nature pose a particular danger to the rights to one's own person. It follows from the primary duty of the state concerning the protection of fundamental rights (Constitution, Art. 8) that this risk shall be reduced to a minimum, *i.e.* the use of the PINs shall be restricted by security regulations. This can be done in two ways: either the use of the PINs is to be restricted to precisely defined data-processing operations, or strict conditions and controlling measures are to be imposed on the availability of information connected to PINs and on the link-up of record-keeping

systems using PINs. On the other hand, it must not be ignored that any limitation of the unified and general code results in losing the essence of the code. A PIN available only for limited use is no longer a PIN in the sense of the Act.

3.3 The use of PIN varies widely from country to country. In a number of countries there are *de facto* universal PINs as a result of the unhindered introduction and application of an identification code originally adopted for definite purposes. The number itself was originally introduced for the purposes of the population register or as a social security number. Examples for the former one are Belgium, Denmark, Iceland, the Netherlands and Norway, while for the latter Finland or Switzerland. The Swedish personal number, considered as a copybook example of the universal personal number, was originally a registration number in the birth certificate records. In other countries, personal numbers are forbidden or even considered unconstitutional. In Portugal, a 1973 Act of Parliament ordered the introduction of the universal PIN starting in 1975. On the other hand, Art. 35(2) of the 1976 Constitution, issued after the downfall of the fascist regime, forbids the link-up of personal data storage systems, and according to para. (5): "It is forbidden to assign nationally uniform personal numbers to citizens." In France and in the Federal Republic of Germany, public opposition to the idea of a population register using PINs led in 1978 to the promulgation of the Acts on Data Protection and to the abandonment of integrated data storage systems and PINs.

The German Federal Constitutional Court declared as early as in 1969 that the "registration and catalogue-listing of citizens which affect the entire person of those citizens" are incompatible with the fundamental right to human dignity to which the state has no right even under the anonymity of statistical data acquisition (BVerfGE 27.01.06.), the so-called population census decision, which in 1983 formulated the informational self-determination right, considers PIN as a "decisive step" leading to personality profiles the

avoidance of which shall be accepted even by other means of limitation on informational self-determination (BVerfGE 65.1. 27,53,57).

Between the two extremes are those states where some personal numbers serving certain purposes are used for purposes other than the original one: however, these were successfully prevented from becoming universal codes. (This was the case in France, for example, where the identification number assigned to everybody born in France by the National Economic and Statistical Research Centre did not become a general PIN; similar legal constraints were imposed on the use of social security numbers in Canada.)

The dangers of electronic data processing to the autonomy of personality became widely recognized in the 70s. From this time on, the PIN has become a symbol for the total control of citizens, and for an approach to efficiency alone and for the treatment of persons as objects.

Although the PIN is only a tool, and its role may only be appreciated in the entire context of data-processing regulation, yet its introduction or application was sufficient to trigger the clash of the two value systems, the preference of technical possibilities or of personality rights. This resulted in the precise legal regulation, that is the limitation of the use of PINs becoming a general requirement, and this process started even in countries where the PINs had been introduced before the age of consciousness of data protection. (See, *e.g.*, the report of the Data Protection Expert Committee of the Council of Europe: "Introduction and Use of Personal Number: Issues of Data Protection," Strasbourg, 15 December 1989.) Even the application of the general principles of data protection similar to any other personal data present a limitation of the use of PINs. This means that legal authorization is required for anybody who demands the disclosure of the PIN; in the absence of such, no one may be disadvantaged for refusing to disclose his PIN. The PIN must not contain sensitive data (*e.g.* ethnicity or religion) but there is an increasing

demand that it should not be a "talking number" either, *i.e.* one that provides such information as the date or place of birth.The use of personal numbers shall be exactly specified and limited by law, and its use shall be controlled and supervised by independent data protection officials. However, beyond these general requirements, the risks inherent in PINs must be counterbalanced by separate safeguards as well. For example, the establishment of data and record storage units operating with PINs are subject to a special permission in Norway, and in certain record-keeping units the use of this number is forbidden. The link-up of registers operating with PINs shall be subject to particularly strict conditions and supervision, and shall be made accessible to the persons concerned as well. These safeguards were introduced, *e.g.*, by the Swedish data protection office.

The safeguards related to PINs shall prevail in case of identification documents that may be used similarly (*e.g.* identity card, passport or driving licence number), and with adequate modifications in case of personal codes used in other special areas (pension and social security numbers).

3.4 The current regulation of the PINs is unconstitutional because s. 6 of the Act allowed their unlimited use or made their unlimited use compulsory with state organs without providing safeguards against the dangers inherent in them.

Hungarian law allowed for all the dangers arising from the nature of PINs to be realized when it failed to regulate the use of such numbers, and introduced them in an unconditional way into such a legal environment where the fundamental guarantees of the right to data protection were unknown. (Only one of these safeguards, the right of inspection by the person concerned, was regulated: however, this being out of its context, it has never become an actual right.) The issue of the possibility of limiting the data flow within the state administration has never been raised by officials, and the handing out of

PINs was made a condition for the availability of services even outside the non-state sphere.

These circumstances resulted in a multitude of registers operating with PINs, frequently without the knowledge of the persons concerned, and with unimpeded communication between the various systems; today no one can know who, where and to what of his personal data has access.

In the face of such dangers the Civil Code and other legal measures on the protection of personality and secrecy are insufficient. It was with regard to the population register and PIN system set up in 1974 that through a modification of the Civil Code in 1977, a general clause was enacted to the effect that no computerized data processing may violate personality rights, and introduced the right to correction of the person concerned, and forbid the information supply to unauthorized persons (Civil Code, art. 83).

However, up to the present time there has not been a single legal rule or court ruling which gave substance to the abovementioned general clause, or indicated the constituent elements of the right to informational self-determination or of the right to data protection. Data processors were not, therefore, impeded either by adherence to the purpose to be achieved or by rules on data acquisition or forwarding, and the persons concerned could not be aware of their rights either. (The persons concerned have no legal possibility even today to learn about which registries they might be recorded in, and hence the practice of the right of inspection is illusory.) The independent control and supervision of data processing have been completely missing. Only the Act contained provisions concerning the more detailed regulation of the flow of personal data and of their protection. This Act has, however, been proved by the Constitutional Court to fall short of the requirements of constitutionality. The abovementioned, and generally insufficient safeguards are in no way capable of counterbalancing the peculiar risks inherent in the

nature of the PINs. Neither the Act nor Hungarian law contains measures directed at fending off the dangers inherent in PINs either by prescribing conditions for their use, or by allowing the control of the use of such numbers.

Based on these considerations, the legal rules in force concerning the use of PINs violate the Constitution: these measures are contrary to the right to the protection of personal data (Constitution, Art. 59), and limit these rights in a disproportionate and unnecessary manner.

3.5 It is the duty of the legislator to create an Act, in accordance with Arts. 59 and 61 of the Constitution, concerning the protection of personal data and the accessibility of information of public interest, and to give a concrete form in so-called area-specific Acts to the basic principles laid down in the above mentioned Act. It is the legislator's responsibility to decide whether to introduce within certain limitations the PINs which were annulled in their current form, and to specify the limitations and special controlling measures on the use of these PINs. In the present case, the Constitutional Court has declared the PIN-system to be unconstitutional because the Act contains no limitation whatsoever on the use of PINs. This, however, does not mean that any sort of restriction or limitation is sufficient to render the use of PINs constitutional. The Constitutional Court, therefore, summarizes its opinions expressed above on the limits within which personal identification codes are considered to be in conformity with the Constitution.

The Constitutional Court establishes that the universal personal identification number is, by its very nature, contrary to the right to informational self-determination. Only the use of an identification number limited for data processing with a specific purpose is, therefore, compatible with the Constitution. The Act introducing such "personal numbers" limited in use shall provide regulatory and control guarantees that preclude the use of this number for other purposes and in other contexts. Neither the "state

sphere", nor the entirety of state administration may be considered a unity within which a single, unified personal identification code shall be introduced or used.

4. The Act and its executive decrees create or maintain such a seriously unconstitutional situation that would justify their immediate invalidation. On the other hand, the Constitutional Court has paid attention to the fact that an abrupt reorientation of the registry created by these legal rules into a personal identification system which conforms to the Constitution would present a transitional but significant set-back to the operation of these organizations. In addition, the Constitutional Court has also considered the fact that the reform of these systems is already under way, and that an Act on Data Protection will soon be enacted within a foreseeable time. In order to facilitate the switch to a personal registration system that is constitutional, the Constitutional Court decided that those parts of the Act on the basis of which the state population register may perform data furnishing absolutely necessary for the protection of citizens' rights and the operation of administration will remain in effect until the end of the year. Data service may continue on a provisional basis to private persons if they certify in writing their entitlement to the data and to administrative bodies entitled by the decrees of the Council of Ministers to regular data supply. (See Point 2.3. above for the reasoning of this.) Data forwarding to private persons claiming only rightful interests, or unable to certify their right in writing, and to any organizations other than the above-mentioned is, however, discontinued with immediate effect.

In order to allow the performance of this limited scope of duty and to facilitate the reorganization, the decision leaves the scope of data acquisition intact until the end of the year, only the potential to expansion of this activity by a decree has been made impossible with immediate effect.

Due to the seriously unconstitutional character of the current use of PINs, the Constitutional Court annuls with immediate effect the Decree making the use of PINs compulsory in official documents, registers, administrative and in judicial procedures as well as the Decree which had prescribed the entry of PIN into the identity cards. From the time of publication of this Decision, no one has the right to require the furnishing of the PIN, or to make the exercise of any right or the grant of a service dependent on the furnishing of such number.

The Constitutional Court takes into account that the already existing PINs will not be deleted from the state-managed registers before the introduction of the new codes by an Act. It points out, however, that new subjects may no longer be registered with PINs, and that the link-up of various registers by the PINs is beyond the limit of tolerance within which the already existing PINs, used solely as internal indicators, are not to be deleted in the interim period. This danger involved in such limited use of the otherwise unconstitutional PIN is offset by the fact that, by its nature, this usage is doomed to be phased out: since the unified character of the systems is necessarily destroyed by the ban to register new data with the PIN, and by the fact that the persons concerned will not supply their former PINs.

The abolition of the unconstitutional situation is the duty of everybody who kept PINs on records; this applies to both the state-run and the non state-run data processors which have thus far used the PINs at their own risk theoretically depending on the consent of the persons concerned.

Only the state population register is entitled to issue new PINs until 31 December 1991 and to use them, along with the existing ones, as internal identification codes. This is necessary in order to keep the data base intact until the legislator makes its decision concerning the constitutional successor of the population register.

5. This decision of the Constitutional Court will be promulgated in the *Hungarian Official Gazette*, in accordance with s. 41 of Act XXXII of 1989 on the Constitutional Court.