HCLU ON THE PROTECTION OF PERSONAL DATA

What is informational privacy?

The right to the protection of personal data gives power to the individual to make the ultimate decision on how his[1] personal data can be stored and used. Informational privacy means that the data that are suitable for the identification of an individual – the so-called personal data such as his name, address, occupation, ethnic affiliation and state of health – may only be recorded and forwarded with the approval of the person concerned. "Informational privacy" is synonymous with "right to the protection of the personal data." The expression involves both the right that one's interest in privacy is protected that one has the right to make decisions on the ways his personal data can be handled.

Why personal data need to be protected?

Anybody who gets unlimited access to the personal data of an individual can formulate a fairly detailed profile of that individual without directly knowing him. In case our personal data could be stored and forwarded without our approval, various state agencies and other institutions could come to know our personal characteristics, facts of our private life, our opinions, our financial position or even our health status without we knowing about it. Those organizations could intrude into the most intimate details of our life. They could draw conclusions about us and perhaps they could make vital decisions about us without needing to ask for our approval.

Data that are devoid of personal traits – which are anonymous – do not need to be protected because, if an information cannot be associated to an individual, the fact that somebody else has access to it and uses it for statistical or research purposes cannot cause the individual any harm. It is, for example, an individual's right as a matter of conscience to opt for unarmed civilian service rather than serving in the army. The public does not need to know who opted for the civilian service. However, there is no restriction whatsoever on the publication of the impersonal data on the number of persons who year by year choose the civilian service.

What are the international principles of data protection?

Information privacy is a relatively new civil liberty. It was not firmly established before the second part of the twentieth century. The US and the UK have been in the vanguard in related legislation: the rules of data protection were first incorporated in a law in the United States in 1966 and in the United Kingdom in 1984. The first international document with a binding force dates back to 1981. That is the convention on data protection of the Council of Europe. In 1995 the European Parliament and the Council issued guidelines in response to a rapid extension of the amount of data that are

[*] "his" always means "his or her"

forwarded across country borders. These guidelines seek to serve double purposes: to ensure that information could flow freely across the borders and at the same time the priorities of data protection should be observed. The 95/46/EC directive of the European Community made the data protection rules that cover the automated data procession more stringent.

Separate recommendations have been issued concerning the users of sensitive personal data. Why do their activities attract enhanced international attention? This is because should sensitive data that they handle become public without authorization, that would cause particularly severe damage to the data subjects. In 1987 the Council of Europe issued recommendations regulating the use of personal data in the police sector and in 1997 on the protection of medical data.

Here are the key principles personal data protection as formulated by the above documents:
– the individuals have the right of access to data that are stored about them;
– personal data may only be recorded and used with the approval of the data subject or in cases defined by law;
– the recorded data have to be precise and updated;
– personal data may only be used inasmuch as justified by a particular purpose and only for a justified period of time, after that it has to be destroyed;
– only in exceptional cases may data users exchange personal data without the approval of the data subject;
– it is desirable that data handling be supervised by an individual (a Data Protection Commissioner) or an institution;
– violations of data protection provisions should be subject to criminal sanctions;
– the data subjects may request the cancellation of data that are not needed any more and the correction of mistaken data.

Convention for the Protection of Individuals with regard to automatic processing of Personal Data, Council of Europe, 1981. (Excerpts)

Article 6
Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 8
Additional safeguards for the data subject

Any person shall be enabled:
a, to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b, to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c, to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 if this convention;
d, to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Is there a need for a law on the protection of personal data?

Hungary and the other European states that have ratified the data protection convention have obliged themselves to observe the rules and principles pinned down by that document. To ensure informational privacy, these countries may enact even stricter provisions.

Informational privacy entered the constitution of numerous countries. That is a major step forward because fundamental constitutional rights cannot be restricted by means of provisions other than enshrined in law. Moreover, the constitution of Hungary and of many other countries provides that in so far as the "essential core" of a fundamental right is concerned, it may not be restricted at all, not even by legislation.

Some states have provided for informational privacy and for the right of access to information of public interest in a single piece of legislation. Such a law has to serve double purposes: it has to ensure that the individual is protected against the state's increasing appetite for information and, that, he gets access to documents that carry information on the workings of state agencies. In other words, the purpose of such a law is to make the citizens as opaque as possible and to render the sate itself as transparent as possible.

In some countries there are separate laws for the protection of personal data on the one hand and access to data of public interest on the other. In itself, such separation may not be sufficient in order for the Data Protection Act to be able to take care of all the complexities of the issue. Thus, further laws may be needed such as the law on the handling of medical data or the provisions on handling data by the police or by the national security services. The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECPHR) adopted by the Council of Europe provides that fundamental rights may not be restricted by any provision other than law and, that, such restriction must be limited to those accepted in a democratic society. There are certain fundamental rights that may not be suspended even in cases of emergency, informational privacy being one of them.

According to the HCLU
– informational privacy can be better asserted if a country has a separate law on data protection;
– it is of the highest importance that states respect the principle according to which informational privacy may only be restricted by law, but its "essential core" may not be restricted at all, not even by law;

– whatever restriction is provided for by a law, it has to be narrowly tailored to a specific purpose, it has to be necessary to reach that purpose and the burden imposed on the individual has to be proportional with that purpose.

What can the Data Protection Commissioner do?

In numerous countries – including Canada, the United States, the United Kingdom, New Zealand, Germany and Hungary – there is a Parliamentary commissioner for data protection or a separate institution that supervises the observation of data protection regulations. The Data Protection Commissioner sees to it that data users should abide by the relevant law, and he can put forward recommendations in case the regulations are infringed.

If an individual believes that an institution collected and stored data about him in violation of the law, he can turn to the data commissioner with a complaint.

It is an important function of the Data Protection Commissioner or of the institution in charge of data protection, that he/it can formulate an opinion about draft laws; the Data Protection Commissioner then directs the attention of the legislature to conflicts between the proposed bill and the principles of data protection; he also can recommend legislative action with the aim of improving on the practice of data protection.

What are the cases in which consent of the data subject is necessary?

As a rule, personal data need to be obtained directly from the data subjects. For a data subject to be able to give his well considered consent to data collection, he must be informed on
– whether disclosing the particular data requested from him is voluntary or compulsory;
– what is the purpose of data collection;
– will the data be forwarded to other data users;
– who will process the data and who will have access to them;
– the data user should also be informed that mistaken data have to be corrected if he so requires.

In case the source of personal data is not the data subject, the latter should be informed about the fact that his data have been collected and used.

Personal data of varying sensitivity may receive legal protection of varying stringency. For example, data on ethnic affiliation, personal convictions or health status are generally treated as sensitive. Sensitive data enjoy special protection such as, for example, requiring a written agreement of the data subject to the collection and use of his data.

Prohibition of connecting databases – what does it mean?

Various state agencies and local government authorities collect several types of data about the citizens. Originally, these databases were created for specific purposes and they operated separately. Sometimes, however, the state may find it advantageous to

use these databases for multiple purposes or even to connect one with another. The purpose of such connection may be to streamline or to make more efficient the work of administrative agencies.

If the various databases can be freely connected with each other, the state may learn practically anything about its citizens' financial situation, family relations, state of health, professional promotion and consumption habits. As long as the data used to be stored in paper files kept in cupboards, there were physical obstacles to connecting the databases of different offices. However, the advance of information technology has made the storage of data easier, and it has made it possible to interconnect various databases. Whoever has access to any of these databases, can use the others as well. That is why there is need for regulations that limit the connection of various databases. It is also the duty of data users to store data in such a way that persons without authorization should not be able to find access to those data.

Why is the use of an all-purpose personal identification code unacceptable?

The connection of files is especially easy if an all-purpose identification code is attached to personal data whenever these are collected. Such identification codes were introduced in numerous countries before the public became aware of the need in protection of personal data. Today, however, the use of an all-purpose identification code has been prohibited in several countries of Europe. Originally such identification codes were introduced in Belgium, The Netherlands, Iceland and Norway for population records, while in Finland and Switzerland they were used as a social insurance number. In Portugal, the general personal identification number was used under Fascist rule. Consequently, when the Fascist regime fell, the new constitution provided for the abolishment of the all-purpose personal identification number. In the Federal Republic of Germany, the Constitutional Court issued a statement in 1969 to the effect that "cataloguing people" violated human dignity. In 1983, the same Court ruled that all-purpose use of the personal identification number was unconstitutional. In Hungary – in a similar manner to France – the personal identification number was first introduced but then, in the wake of a ruling of the Constitutional Court in 1991, its use was gradually restricted. The major databases, such as the one held by Social Security and the taxation authority were required to introduce different identification codes. The Constitutional Court ruled that all-purpose identification numbers were unconstitutional. It is a particularly serious violation of personal rights, so the argument of the Court proceeded, to allow public authorities to combine various information on a citizen into a "personality profile."

Which are the most sensitive areas of data protection?

Data Processing by the Police

Informational privacy is sometimes invaded on the ground that disclosure of sensitive data is needed in order to protect public safety. In combating crime, police would like to get access to personal data as simply as possible and from as many areas as possible. Such special powers of police may endanger the constitutional principles of data

protection. Citizens have right not only to live in safety but also to have their personal data protected against illegitimate intrusion.

Police have no right to get access to personal data unless they have authorization by the law to do so. The law is supposed to make access to data conditional on data collection being necessitated by a legitimate purpose, on the data collected being necessary for reaching that purpose, and on the burden caused by a failure to get access to the data being proportionate to the burden the data collection imposes on the data subject.

According to the HCLU, police may only collect, store and use personal data under the following conditions:
– data may only be requested if a specific purpose for data processing is defined and if the nature of the data required is described in writing;
– it is inadmissible that police should collect personal and, particularly, sensitive data for general crime prevention purposes, just to "enrich" its database. That refers specifically to health care data;
– after a criminal investigation is finished and supposing that a suspect proves to be innocent, his personal data have to be removed from the police records;
– after an individual's criminal record becomes void, his data have to be removed from police records;
– all personal data unrelated to a concrete crime case, have to be removed from police records.

It would contradict the requirement "collect data only for specific purposes'', if police were allowed to collect data just to enrich their database on issues like the health status of people, their drug dependence, infectedness with AIDS or affiliation to any group. In our view police should only be allowed to handle such data if the information is specifically connected to a criminal offense.

In the opinion of HCLU
– the confidentiality of medical records may only be ignored in exceptional cases, for the interest of investigation into a crime case;
– the interests of the health care service and the personal rights of drug patients suffer serious damage if doctors and health care facilities that treat drug users are required to supply data about for police about their patients. We are convinced that it is inadmissible that police should be able to obtain data from banks and the tax authorities for general purposes of preventing or discovering crime. We believe that police should only be able to request information if there is suspicion of a specific offense and even then only about persons who are suspected of having committed a crime.

In 1987 the Council of Europe issued a recommendation on how police may collect, store and utilize personal data. That document provides among other things that while being stored, such data have to be separated according to their reliability: factual information has to be kept separate from data that are based on mere assumptions.

Surveillance by the National Security Services

In addition to the protection of public safety, appeals are made to national security interests to justify departure from the general rules of data protection.

Data processing, even if carried out by the national security services, must satisfy the tests of necessity and proportionality. According to the HCLU, the national security interest has to be given a narrow reading. National security is endangered by
– violence or threat of violence against the existence or integrity of the state;
– violence or threat of violence against a state's self-defense capability;
– attacks on the personal security of the supreme state officeholders.

The national security services may only conduct clandestine surveillance with a court or prosecutor's warrant. Informational privacy requires that the data subject is informed retrospectively about secret surveillance or any other use of secret service means. The data subject has to get such information even if the charges against him have not been substantiated.

Medical Data

The notion "medical data" includes all the diagnoses that are created in the course of medical treatment, the anamnesis and any information that is related to the patient's health status. Medical records may also cover genetic information from which wide-ranging conclusions can be drawn concerning the genetic profile of the person concerned, of his children and relatives. It might be especially important for a patient that his medical treatment are kept in secret. If for instance it becomes known that a person underwent psychiatric treatment, that can be the source of discrimination in his employment and personal relationships.

Consequently, medical data are of a sensitive character, and it is customary their handling is customarily subjected to very strict rules. With these considerations in mind, the Committee of Ministers of the Council of Europe adopted a recommendation in 1997 about the principles of the protection of medical records (recommendation R/97/5 on the protection of medical data).

It is a principle of major importance that medical data may only be disclosed to third parties with the consent of the patient or in case that disclosure is justified by the interests of the treatment. Even when a consultation of medical experts is undertaken, it is not always necessary to identify the patient by name; laboratory findings may also be forwarded wit a code attached to them.

A patient should have the opportunity to decide which of his family members should get information from the doctor. Even members of the family may not get access to information about a patient's disease against his will.

What kind of health information may be required by the law to be disclosed to specific authorities? Health care facilities are most often required to supply information with the following justifications:
– epidemiological considerations (information about contagious diseases);
– health care emergency (for instance, poisoning);

– combating crime;
– needs of law enforcement agencies.

The tests of necessity and proportionality apply even to the cases of compulsory data forwarding. When, for instance, in the case of a disease, the number of the incidence of a disease has to be counted, it is sufficient to forward anonymous data to the public health authorities. When police request data about a particular person, they have to tell the purpose of their request and have to specify what kind of data they are interested in. It is inadmissible for police to request that a hospital should send them all the medical records of an individual claiming that an investigation has been under way against that person. Such request for information may only be justified if that person is charged with committing a crime, and it is also a precondition that the data requested are directly connected with the offense.

It is regrettable that the Hungarian law on the handling of medical data (Act XLVII of 1997) gives a very broad interpretation of reasons which legitimize the demand for information delivery without the approval of the data subject. Under the above law it is possible for police to request data both when a person is charged having committed an offense and when an investigation is under way without a formal charge. Note that under Hungarian law the confidentiality under which lawyers have to treat information has to be observed under all conditions. In effect it means that, without the approval of the client, a lawyer can not reveal information about him *under any circumstances*. It is unreasonable that the same rules of confidentiality do not apply to the physician with respect to his client.

Intense interest displayed by law enforcement agencies in records kept by health care facilities that treat drug addicts raises special problems. Whatever the drug policy of a country, drug patients should be given to seek medical assistance without the danger of becoming subject to penal procedure. Prosecution of the traffic in drugs should not interfere with treatment of drug addicts. In case the ambulance service might report about them to police, drug users will be deterred from turning to a doctor even if they feel very unwell.

According to HCLU, the following priorities should be satisfied by the handling of medical records:

– a doctor has to give full information for his patient about his disease;
– health care facilities must see to it that there should not be any obstacle for a patient to exercise his right to informational privacy: he should get access to his medial records and he should be able to get a copy of those records;
– when data need to be forwarded for diagnostic or consultation purposes, they should be made anonymous;
– it is inadmissible that police should request medical data for general purposes of crime prevention (in cases when there is not any substantial suspicion that the patient has committed an offense or when it is uncertain whether or not data requested are connected in any way to an alleged crime);
– law should specify what kind of genetic information can be collected for combating crime and in what manner should that information be collected, stored and utilized; in

any other case the processing of genetic information must be subject to the approval of the data subject.

The right to the protection of personal data is not absolute, there are exceptional conditions under which it may be restricted by the law. As a matter of constitutional principle, that may only happen when it is required by the protection of another fundamental right. Even in such a case, the "essential core" of the right to personal data protection cannot be restricted. In cases when our right for data protection is violated, we can submit a complaint to the court against the data user concerned. Whoever suffers damage because of his data were used illegitimately, may claim damages under civil law.
The Data Protection Commissioner has to ensure that the right to informational privacy should be observed. He is supposed to make public his opinion about complaints submitted to him and whenever that is necessary he has to inform the persons concerned about their constitutional rights. The commissioner must have access to all kinds of records, and the various institutions are obliged to take his recommendations seriously.

The most important data protection instruments in Hungary

It is provided in the constitution that the citizens have a right to the protection of their personal data and that the Republic of Hungary must have a law on data protection. The general principles of data protection are formulated by the Civil Code as well. As for the specific legal instrument on that question, see Act LXIII of 1992 on the Protection of Personal Data and on Access to Data of Public Interest. According to that law, it is an objective yet to be attained that each citizen should have control over his personal data. That law defines the conditions under which personal data may be collected and processed in accordance with international norms.

Under the law on data protection, every citizen has the right to know what kind of data are stored about him, and each citizen may request that mistaken data about him should be corrected or canceled. Personal data may be handled by competent data users only for specific purposes, to a justified degree and only for a justified period of time. Before data are collected, the data subject has to be informed whether the supply of data is voluntary or compulsory. In case data supply is compulsory, information on the law which makes it such has to be given. Personal data may only be forwarded for a third party if the data subject has given his approval for that. An exception to that rule may be made only by law and only under very specific conditions.

Sensitive data enjoy a higher-level protection than mere personal data. Sensitive data are information on racial background, on national or ethnic affiliation, political views, religious or other conviction or any other data that refer to health status, pathological addition, sexual habits or criminal record. With the exception of specific cases to be defined by the law, such data may only be collected and processed upon obtaining the written agreement of the data subject.

The state does not have the right to keep a record about the ethnic affiliation of its citizens, and it may not oblige its citizens to issue a statement about that. Directive

281/40 of the European Union provides for the prohibition of the processing of data that refer to ethnic or racial affiliation, political, religious and other outlook, trade union membership, health status and sexual life. According to that directive, the only exception to that rule can be made by the explicit consent of the data subject or by a procedure that is to take place in his own interest.

The use of personal identity documents

Personal identification codes may be used only by specific instances authorized to do so by the law. In Hungary, such instances are the citizens' address records keeping agency, the registry office where births and marriages are recorded, police and courts. Banks are not authorized to request the citizens' personal identification number, nor do they have the right to produce a photocopy of documents that show an individual's personal data. When a contract is to be formulated, banks and investment companies are not authorized to request that citizens should make a declaration about their marital status, the occupation of the spouse or their social insurance number. For the same reason it is not justified and is against the rules that when somebody pays with a credit card, a copy is made about his personal identification document.

The increasingly widespread use of the Internet poses further challenges to data protection. In a particular case it seemed likely that the perpetrator of a bomb outrage learned how to produce a detonator by visiting a web site, and so it was lawful that Hungarian police received the personal data of the suspect from his Internet provider. However, when anonymous comments are sent to a discussion forum on the Internet, the Internet provider does not have the right to disclose to the police data that would make it possible to identify participants of the debate. The e-mail address is a piece of personal data just as the address of a person is as long as it is suitable to identify him.

The spread of making video recordings of people in public spaces is yet another recent development. In many countries authorities expect that the production of such video recordings will help combating crime and reducing the violation of traffic rules. It has not been clarified for how long authorities may store such recordings and in what manner can the personality rights of the individuals be protected against possible invasion. It might cause a bad impression about a person, even if he is not charged with committing any offense, if he is recorded entering a house, a shop, or doing this or that in the street. The advocates of such video recordings argue that people who use the street are in a public space and therefore they have no legitimate claim against being monitored. However, so far there has been no technical guarantee that cameras should not be able to record what is happening in a private garden or a private apartment. Neither has it been legally defined under what conditions can such recordings be digitized and stored. Note that such recordings are suitable for the identification of the face of persons.

Whatever the aims of public space video monitoring, it unavoidably gives rise to an Orwellian feeling that "Big Brother is watching you".

HCLU aims to a state where

- Hungary's data protection law is enforced in the day-to-day practice of state agencies;
- citizens come to know the rules that serve their informational privacy;
- the ban on the connection of the data systems of major state-run data users is strictly observed;
- basic principles of data protection are not violated on the grounds that invasion of privacy is needed to forward the interests of combating crime;
- the Police Act is amended in such a way that police should not have the right to request data for the interests of discovering crime;
- health care facilities are well informed on data protection regulations, and they refuse to fulfill any unauthorized requests for data;
- personal data of psychiatric patients, drug users and HIV positive persons receive special protection.
- As in the past, the HCLU will turn to Parliament, the Constitutional Court or the Data Protection Commissioner with recommendations whenever we think that is justified for the benefit of the protection of personal data.