<DATA PROTECTION IN HUNGARY>

<DATA PROTECTION IN HUNGARY>

Edited by Dániel Máté Szabó

Published by the Hungarian Civil Liberties Union, Budapest, 2003

The publication of this volume was supported by the Ford Foundation

CONTRIBUTORS:

Márta Faur, lawyer, Data Protection Project of HCLU

Eszter Csernus, lawyer, Patients Rights Project of HCLU

András Schiffer, lawyer, Legal Advocacy Project of HCLU

Andrea Pelle, lawyer, Legal Aid Service of HCLU

Balázs Dénes, lawyer, Drug Policy Project of HCLU

Dániel Máté Szabó, lawyer, expert in data protection, staff member of the Data Protection Commissioner

CONTENTS

FOREWORD

The Data Protection Act came into effect ten years ago. There is no denial that it works. As laws in general, it is not perfect, it has drawbacks, it is imprecise in some places, so at some points it makes life difficult for data processors – i.e., for everyone. It leaves a few things to be desired and modified, but it is good enough, on the whole. Thanks to the Act introduced in 1992, Hungary today is a country in which legal rules on the protection of personal data and on freedom of information are actually observed. Before 1993 there was no such law, and now that there is one, it has acquired special significance. Most citizens are aware of their right to the protection of personal data which secure privacy, a core of one's personal matters that is shielded from the penetrating eye of the social environment, and of the freedom of information which secures the transparency of the state, and most citizens want to assert these rights, too, protesting when these are violated. They do not leave the Data Protection Commissioner with nothing to do.

The Hungarian Act on the Protection of Personal Data and the Disclosure of Data of Public Interest has earned some international recognition: the model of a combination of two fundamental rights (that of data protection and that of freedom of information) is being adopted by an increasing number of countries, and the European Commission finds that the right to the protection of personal data enjoys a status that is equal to that practiced in the legal system of the European Union. Several authors from other countries have expressed their appreciation for the Hungarian regulations in professional articles.

The skeleton outlined in the general law is fleshed out in what are called 'sectorial' rules, i.e. rules relating to definite kinds of data or data processing done in various branches of law. It is these detailed rules that define the character of the data protection law of a particular state, and have an immediate effect on the ways in which citizens are able to exercise their right to informational self-determination. These sectorial laws tend to leave more room for criticism than those that set out the underlying principles of data protection, and Hungary is no exception in this respect.

In this volume we survey four sensitive sectors of data processing. Four articles discuss legal and practical problems arising in connection with one kind of sensitive data, namely medical. The first discusses the general problems haunting the handling of medical data. The next one is addresed to the handling of personal data relating to the HIV infection. This is followed by studies of an area of data handling which occurs in two special domains of social life characterized by a high degree of dependence of the data subjects, namely employment and penitential institutions. Another article criticizes certain provisions of the Police Act which bear directly on data processing, and the last article is devoted to the question of data protection at schools.

Budapest, March 2, 2003.

The Editor

DATA PROTECTION IN HEALTH CARE

Márta Faur

The aim of this paper is to present the importance of, and the need for, securing protection for data processed in the sphere of health care, and to indicate the areas in which data processing may threaten to be injurious to individuals' rights. In the first part I review the question of the protection of medical data in general terms. In the second part I briefly recapitulate the same question in an European context and take stock of relevant provisions in presently valid Hungarian legal regulations, i.e. the practice of the Hungarian Constitutional Court and legislation relating to medical data and its shortcomings. Drawing from cases and experiences of the Hungarian Civil Liberties Union in the third part, I then analyze specific issues and cases such as the unlawful handling and disclosure of the medical data of drug users and psychiatric patients, and one of the patient rights, the right to have access to medical records.[1]

1. THE INDIVIDUAL'S RIGHT TO INFORMATIONAL SELF-DETERMINATION AND PHYSICIANS' DUTY OF CONFIDENTIALITY

The idea that medical data should be protected applies not only to persons who, for some reason or another, find themselves in a position of dependence on health care institutions. Rather, it

1 The equally pertinent questions of data protection arising in connection with the rights of the HIV infected are discussed in another article in the present volume.

applies to any human being, since any one of us may find ourselves in a position in which we vitally depend on medical help and have to take recourse to health care services. Health care services are services which we may need at any time, and with which most of us actually come in contact at some time during our lives. Whenever this happens, we disclose some of our personal data in the interest of our recovery. We assent to our data being recorded without wanting anyone other than the physician or health care personnel involved in the therapy to get to know them. Information relating to state of health is an especially sensitive kind of personal data which affects people's private sphere more profoundly than other kinds of data. They are data which form part of people's private sphere, intrusion into which may have grave consequences for those who are affected, i.e. the data subjects.[2] It is especially important that the right of individuals to informational self-determination should have effect in the area of health care, i.e. that the individual should actually remain in control of his/her data. It is part and parcel of our right to informational self-determination firstly, that we should be able to decide who is to be allowed to get to know our medical data, and secondly, that we should be allowed to decide to whom the person allowed to get to know our data is supposed to be allowed to pass those data on. In other words, we may decide not only who is allowed to get to know our data but also who is to get to know them. Legal rules, however, may define situations which render data handling obligatory, and this stops individuals' right to informational self-determination from being effective. It is especially important in these cases that data be handled for a clearly defined purpose so as not to allow unjustified or unreasonable restriction of the right to self-determination.

2 A data subject is any person to whom certain data relate or may be related by someone else.

The protection of medical data is also important for the further reason that medical data are handled not only for the purpose of therapy but are used in the course of what may be called secondary data handling, i.e. for purposes of scientific research, health care-related planning, making social security arrangements etc. Such an extension of the range of data processing activities has been greatly facilitated by the staggering development of automatic devices in recent decades, which has created a situation in which the data subject is no longer able to keep track of the uses that are made of his/her data. The enormous flow of information defies the individual data subject's capacities. Undoubtedly, the easiness of access to information made possible by the development of technology can be exploited to a great number of valuable purposes. At the same time it has also created the hazard of the abuse or inappropriate handling of data. This may have rather undesirable consequences for the individual. Data which are inappropriately handled, or unlawfully disclosed are a possible source of danger for the individual. They may put him/her in embarrassing situations by giving rise to social prejudices or disadvantageous discrimination toward him/her. Without appropriate guarantees, data subjects may find themselves exposed to possible blackmailing, may lose their jobs or have their privacy invaded.

In discussing the nature and protection of medical data we must not omit to discuss the distinguished role of physicians' duty of confidentiality. Like the protection of personal data and private secrets, the duty of confidentiality protects the individual's right, it is a fundamental requirement which has to be fulfilled in order for the right to self-determination to become effective.

The duty of confidentiality is not merely a legal norm for physicians. Although it has been incorporated into legal instruments as a legal obligation in several countries for some

time, it has also been a moral prescription, a fundamental requirement on physicians for several centuries going back to times well before the introduction of institutions for data protection. A document as early as the Hippocratic Oath contains the following words: "What I see or hear during treatment – or outside treatment in social intercourse – I will not divulge but keep to myself." The ethical requirement of keeping confidentiality can also be found in international regulations concerning physicians. The International Code of Ethics, issued by the World Medical Association in 1949, includes a list of physicians' obligations, among which we find the requirement that patients' data should be handled in a confidential manner.[3]

The patient-physician relationship is a relationship based on trust in which the patient reveals confidential information in the interest of his/her recovery and which, in this way, necessarily presupposes the acknowledgement of the right to self-determination. This is the foundation which justifies the requirement that the duty of confidentiality should be fulfilled. At the same time, the fulfillment of this duty is dictated not only by respect for the patient's right to self-determination but it is also the case that medical intervention can hardly be successful without the atmosphere of trust. If people feel reluctant to disclose their health problems, therapy will be impeded. Thus it is in the physician's interest also to treat data confidentially if he/she wants to maintain a successful medical helping relationship. Somewhat indirectly, it is even in the interest of the public, since people's reluctance to seek medical help for lack of trust may have harmful consequences for the state of public health.

People's right to informational self-determination and physicians' duty of confidentiality may be restricted only under

3 http://www.cirp.org/library/ethics/intlcode/

rare circumstances, and even then within strict limits. Child abuse or injuries from gunshots or stabs are cases which obligate physicians to report them. In such cases the interest in child protection and public safety is considered to override the duty of confidentiality. Such cases are to be handled with care, however. Although the justification underlying compulsory registration is easily seen to override the duty of confidentiality at first glance, it may often release undesirable effects in practice if the physician, afraid of the responsibility or insufficiently informed about the rules, reveals too much information. It is therefore important to circumscribe exactly and narrow down the range of cases in which physician's duty of confidentiality is overridden by other considerations.

In the Hungarian health care system medical confidentiality is regulated by law from two sides, as it were: as the patient's right to have his/her data handled confidentially, on the one hand, and as the obligation of those employed in the health care provision system, on the other. Breach of the duty of confidentiality may lead to disciplinary proceedings or, if certain further conditions obtain, to civil suits or even criminal proceedings.

2. REGULATIONS ON MEDICAL DATA

2.1. AN OVERVIEW OF EUROPEAN LEGAL INSTRUMENTS

2.1.1. The Legal Practice of the European Court of Human Rights and the Legislative Activity of the Council of Europe

The idea of medical data as special and the demand for their special protection can be found at work in the legal practice of the European Court of Human Rights. The relevant case law of the Strasbourg Court deserves mention here for the reason that

it influences the legislation and legal practice of all member states, including Hungary. The Hungarian Constitutional Court frequently refers to Strasbourg cases in the arguments attached to its decisions.

The right to the protection of personal data cannot be found in an explicit form among the rights secured in the Convention for the Protection of Human Rights and Fundamental Freedoms accepted on November 4, 1950 in Rome. This did not prevent the European Court of Human Rights from proceeding with reference to Article 8, Section 1 on the right to privacy, in a case which involved an infringement of the right to the protection of personal data. Thus the Court held in *Oosterwijk vs Belgium*[4] that the protection of medical data is part of the individuals' right to privacy, and this right must be considered to have been violated if someone unacceptably reveals facts about another person's physical state or state of health. In another case, *Z.v. Finland*[5], the Court made it clear that medical data are to be defended with reference to Article 8 in certain cases. The case is also important in the further respect that the Court stated its reasons for the protection of medical data in its argument. The case involved, as claimant, a woman with HIV infection whose husband, also HIV infected, had been indicted on the charge of rape and attempted homicide.[6] The claimant's HIV test served as decisive evidence for deciding the question, but she refused to cooperate, fearing that the information would not be handled confidentially. Finally the claimant's physicians were obligated to make the documents available and bear testimony, the claimant's entire health records were seized and attached to the court file. Court proceedings ended with the verdict that the man was guilty and the verdict

4 Decision No.7654/76, DVO v. Belgium, March 1, 1979. (European Court of Human Rights.)
5 Decision No.22009/93, Z.v.Fnland, January 25, 1997. (European Court of Human Rights.)
6 In order to substantiate the charge of attempted homicide the court had to find out whether the man was aware of his infection.

was sent to the leading Finnish daily for publication. The verdict disclosed that the claimant was the convict's wife and also an HIV positive person and ordered that the case files should be publicly available after 2002. The European Court found the inclusion of the claimant's name and infection in the verdict as well as the full publicity of the materials after 2002 to be in contradiction with Article 8. Applying the test of necessity and proportionality the Court found it proper that the claimant's health data should be released and that physicians should be obligated to bear testimony. The Court had to weigh the public interest, physicians' duty of confidentiality and the claimant's right to the confidential treatment of her data. The Court explained why the protection of medical data had an indispensable role to play especially with people who are in such a situation of dependence as the HIV infected. According to the Court protecting medical data is an indispensable part of respect for privacy and thus the confidential treatment of these data is a fundamental requirement. This not only protects the right of individuals but is also indispensable for maintaining an atmosphere of trust in health care provision. Without trust those in need of health care services will not contact health care establishments, and may thereby endanger their own or even other persons' health. This is especially true to say of the HIV infected.[7] The Court emphasized that states are under an obligation to secure effective protection for these data so that they should not be publicly disclosed in ways or under circumstances that would violate the fundamental right to privacy. According to the verdict the publication of the case files after 2002 violates the claimant's right to privacy since the consequences of those data becoming publicly available may cause the claimant considerable difficulties in her later life. The Court also declared that the

7 See Article 95 of the work quoted in footnote 4.

release from the duty of physicians' confidentiality, with reference to another interest is to be accepted only if it serves some very important public interest. Law appliers have to identify an especially strong public interest which cannot be served in any other way, and examine very thoroughly whether the public interest really deserves to be treated as of special importance.[8]

The idea of protecting personal data in general, and of the enhanced protection for medical data in particular, underlies the practice not only of the Strasbourg Court. The General Assembly of the Council of Europe and the Committee of Ministers also adopted conventions and recommendations concerning the area we are discussing. Although these documents were made primarily with a view to regulating the automatic processing of data, the recommendations remind readers that they may be applied to the non-automatic handling of medical data. The Hungarian Act on the Protection of Medical Data which was accepted in 1997, makes no distinction between automatic and non-automatic data handling. The recommendations of the Council of Europe undoubtedly served as an example for Hungarian legislators in drafting the Hungarian legal instrument.

Adopted in 1981, the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[9] provides that data revealing racial origin, political opinions or religious or other beliefs as well as personal data concerning health or sexual life may be processed automatically if this is accompanied by appropriate guarantees anchored in the national legal system. Regrettably, the Convention does not determine what is to count as an appropriate guarantee. The Recommendation by the Committee of Ministers on the

8 See Article 96 of the work quoted in footnote 4.

9 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, No.108.

Protection of Medical Data was made to remedy the problems created by this gap.[10] The Recommendation lays down the requirements which are to be applied in the sector, enunciating principles for the handling and collection of data, for the provision of information for data subjects, for exceptions, the data subject's rights, requests for data, data security, the storing of data, scientific research and data flow across country borders. The Recommendation, however, as opposed to the Convention, has no binding force. The Preamble to the Recommendation emphasizes the values which are to be protected as of special importance in the sphere of enhanced data protection: the confidential handling of medical data, and the respect for the data subject's fundamental rights. According to the Recommendation all personal data relating to the data subject's health and data closely and clearly related to the subject's state of health count as medical data. It is a positive advance in comparison with previous recommendations that the Recommendation extends the full protection usually envisaged for medical data to genetic data. It lays special emphasis on the idea of respect due to the data subjects' privacy, in the course of data processing, and the requirement that medical data may be processed in any phase of data handling with appropriate safeguards. Although the Recommendation upholds the principle of strict aim-dependence, the range of aims it authorizes is too broad. Notions such as "real danger" or "another important public interest" as indications of legitimate aims for data handling are not sufficiently definite. The Recommendation also enunciates the subject's rights, including access to their own medical data and the right to the rectification of erroneous data. The requirement that selective access to personal data should be secured, is another requirement which clearly serves the

10 Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data.

protection of data subjects. This means in specific terms that personal identifiers, medical data, social data and administrative data about a given individual should be accessible independently, not only in conjunction, "in one package".

2.1.2. The Directive of the European Union on the Protection of Personal Data[11]

The Directive adopted by the European Parliament and the Commission, like the Recommendation of the Committee of Ministers of the European Council, embodies the most important principles of data protection. Aiming to create harmony between the national legal systems of member states, the Directive obligates member states to integrate its provisions into their national legal systems. In a way the Directive creates a stricter and more elaborate model than the Convention of the European Council in prescribing that member states should establish an independent supervisory authority which is supposed to act as a mechanism of control over the implementation of the content of the Directive. Despite these positive features the Directive has several weaknesses. It gives member states too broad discretion in their integration of the rules and, unlike Hungarian or German data protection law, it does not follow the conception of the right to informational self-determination. It makes the range of data which may be handled within the confines of the data subject's consent much narrower by obligating member states to give broad discretionary powers for data handling based on no more than the data processor's rightful interest in data processing. Its

11 Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

foundations in terms of legal dogmatics are different from those of the Recommendation: for instance, it does not demarcate the idea of strict aim-dependence so sharply from the legal ground of data handling, making in many cases the mere existence of a purpose to be served by data handling sufficient to justify data handling. This leads to a much lower level of protection than that provided by e.g. the Hungarian law on the protection of medical data.

In Article 8 of the Directive we find general rules for the handling of sensitive data, including medical data. Paragraph 1 provides, as a main rule, that member states should prohibit the processing of medical data. Later paragraphs list cases in which the prohibition does not apply (Paragraphs 2, 3 and 4).[12] While in these exceptional cases data handling serves a fairly narrowly delimited purpose, Paragraph 4 gives member states rather broad authorization to extend the class of exceptions if they see fit for the purpose of protecting substantial public interests, and this leads to discretionary powers that are too broad, 'substantial public interests' being a much too imprecise term. It may be noted in passing that according to the practice of the Hungarian Constitutional Court reference to a public interest would simply count as unconstitutional, as the Constitutional Court does not (with the exception of the restriction of the right to property) normally accept the public interest as a ground for justifying a restriction of a fundamental right. The necessity side of the necessity/proportionality test requires weighier reasons than those, if we judge matters from the Court's adjudicatory practice.[13]

12 These include cases in which the data subject gives his/her express consent to data handling, in which rights and obligations arising under labor law need to be examined and this examination makes data handling inevitable, if it is in the data subject's vital interest that his/her data should be handled, but he/she, if incompetent or physically prevented, cannot give the required consent, if the data subject has previously published the data or if the publication of data is necessary for the exercise or protection of legal claims. Medical data may also be legitimately handled for the purpose of preventive medical therapy, medical diagnosis and therapy and the management of medical services. In all these cases, of course, the duty of medical confidentiality applies.

13 Constitutional Court Decision 64/1993. (XII.22.)

In addition to the shortcomings we have just reviewed, the Directive does not define the notion of an appropriate guarantee required for medical data processing. This implies the danger that the level of protection will be different in the member states. To counterbalance this, the European Union set up, as part of its supranational system, a working team to supervise the implementation of the Directive, whose tasks include the monitoring of the unified application of national regulations.[14] The Directive has a further positive feature: it creates the arrangement of prior checking for cases of data processing which involve specific risks to the rights of data subjects. It would be salutary if the handling of medical data was included in this category with reference simply to its nature, but the Directive gives no provisions expressly about this.

2.2. THE HUNGARIAN REGULATIONS WITH REGARD TO MEDICAL DATA

2.2.1. The Hungarian Constitution and the Hungarian Constitutional Court in their Relation to the Protection of Medical Data

The right to private secrets and the right to the protection of personal data are guaranteed as constitutional fundamental rights in Paragraph 59, Section (1) of the Hungarian Constitution. Paragraph 8, Section (2) states, as a main rule, that regulations pertaining to fundamental rights and duties applying in cases when the above-mentioned constitutional fundamental right may

14 Stefan Walz, "The European Data Protection Directive", in: *Data Protection and Freedom of Information* , p. 24-25, edited by the Hungarian Civil Liberties Union, Budapest, 1997.

be restricted, are determined by law which are however never to restrict the basic meaning and content of fundamental rights. In judging questions of the constitutionality of restrictions of fundamental rights the Constitutional Court applies the test of necessity and proportionality: the condition of proportionality imposed on norms which restrict the fundamental right "requires that the importance of the aim to be achieved and the weight of the injury to the fundamental right caused to achieve the aim must be in harmony. The legislator in imposing the restriction is obligated to choose the mildest means that is suitable for achieving the end being envisaged. If the restriction to be applied is unsuitable for achieving the aim, the fundamental right is justifiably said to have been violated."[15] The Decision reveals that the right to the protection of personal data is not an absolute right: it may be restricted under exceptional circumstances, but such restriction may count as constitutional only if it meets the requirements set for restrictions by the Constitution, Paragraph 8, Section(2) in particular.

The adjudicative practice of the Constitutional Court also reveals an interpretation of the content of the right to informational self-determination and of the notion of strict aim-dependence to be observed in disclosure of data.

"The Constitutional Court (…) does not interpret the right to the protection of personal rights as a traditional protective right, but taking its active aspect into consideration, as a right to informational self-determination. The right to the protection of personal data secured in Paragraph 59 of the Constitution thus has as its content that every person makes his/her own decisions about the disclosure and use of his/her personal data. Personal data may be recorded and used only with the data

15 Constitutional Court Decision 20/1990. (X.4.).

subject's consent and the entire process of data handling must be made recoverable and controllable to everyone, i.e. everyone has the right to know who is using his/her personal data, when and for what purpose."[16]

Two details need emphasis with regard to medical data. The right to informational self-determination comprises, firstly, the right to being informed and access to information. The physician is under an obligation to inform the patient about his/her state of health. It is the patient rather than the physician who has control over the data. That is what the principle of informed consent is based on, according to which the physician is allowed to perform necessary interventions on the basis of the patient's voluntary consent. In accordance with the right to self-determination the patient may waive his/her right to being informed. The right to informational self-determination comprises, secondly, the patient's right to inspect registers containing data about him/her, look into medical documents and make copies of them. According to the main rule, persons other than the patient may only be informed about the patient's state of health with his/her written consent.

The necessity aspect of the test of restrictions of a fundamental right was made more specific by the Constitutional Court in the form of the oft-quoted requirement of strict aim-dependence. "The condition and at the same time the most important guarantee of the right to informational self-determination is the requirement of strict aim-dependence. This means that personal data may be processed for definite and legitimate purposes. Data processing must be in harmony with the aim which must be expressed and recorded in publicly credible form. The data subject should be informed of the aim

16 Constituional Court Decision 15/1991. (IV.13.).

of data processing in such a way that he/she should be able to judge the effect of data processing on his/her rights so as to enable him/her to decide whether he/she is willing to disclose his/her data, and to exercise his/her rights if the data are not used according to the purpose. (…) It follows from the idea of strict aim-dependence that collecting and storing data without a specified aim, for "pooling" for an undefined future purpose is against the Constitution." "It is legitimate to make personal data accessible to persons other than the data subject and the original data processor – via a connection of data processing systems as the case may be – only if all conditions permitting disclosure of data are met with regard to every single bit of data. (…) Subjecting disclosure of data to conditions and the idea of strict aim-dependence as guarantees of the right to informational self-determination are always to be applied in conjunction, never disjunctively."[17]

Data relating to a person's state of health may be recorded, stored and disclosed to a third party only with the data subject's consent or for a purpose which is stated in law, precisely defined and constitutionally permissible. The data subject must be informed even in the latter kind of case. The foundation of this principle is the right to informational self-determination itself, and the recognition that those who seek medical help are, by the nature of the case, in a position of dependence which makes it difficult for them to assert their rights. Citizens have an important interest in not having information about their physical and mental condition, their state of health, disclosed to persons who are not authorized to get to know that kind of information, and in not having their data stored in public administration registers for no justified

17 Ibid.

reason. To avoid all this, strict guarantees must be introduced in the handling of medical data. Constitutionally acceptable aims that may exceptionally justify the use of a clearly defined set of data are to be carefully distinguished and specified.

2.2.2. Laws on the Handling of Medical data

Drafted in 1992, Act LXIII/1992 on the Protection of Personal Data and the Disclosure of Data of a Public Interest (henceforward "Data Protection Act") follows the constitutional principles which have been outlined above. The Act defines principles of data processing, its detailed rules and the instruments of legal defense. Among the principles of data processing we find – in harmony with international obligations – those relating to strict aim-dependence, the quality of data, disclosure of data, the conjunction of data systems, and data security. Data about state of health are defined as data which enjoy special protection, which may be handled only with the data subject's written consent, or if ordered by law. The right to informational self-determination is to be given enhanced effect with respect to sensitive data. Hungarian regulations allow this right to be restricted by a law or – somewhat more narrowly – by local authority decrees, both of which, in turn, have limits set by the Constitution.

The processing of medical data is specifically regulated in sectorial laws: in Act CLIV/1997 on Health Care, which enunciates norms relating to patient rights and physicians' duty of confidentiality, and Act XLVII/1997, on the Handling and Protection of Health Information and Related Personal Data (henceforward 'Act on the Protection of Medical Data').

2.2.3. The Act on the Protection of Medical Data

The promulgation of this Act was a historic moment in Hungary in that it was the first comprehensive legislative act to regulate the processing of medical data. This act created the possibility of protecting sensitive data relating to diseases and state of health. The aim of the Act is to delimit the kinds of aims for which data may be collected and the kinds of data that may be collected, and regulates the class of persons who are entitled to handle data. The Act is in harmony with the Recommendation of the European Union on the Handling of Medical Data, which we have just been discussing.[18]

As far as the application of the Act on the Protection of Medical Data and the Data Protection Act is concerned, it is to follow the principle of *lex specialis derogat legi generali.* This means that the Data Protection Act as a general rule is to be applied with regard to medical data when the question in hand is not regulated by the Act on the Protection of Medical Data.

2.2.3.1. What is Included in the Class of Medical Data?

According to the Act on the Protection of Medical Data the notion of medical data covers all data relating to a person's physical, intellectual and mental condition, addiction, the circumstances of falling ill with a disease and dying, all data relating to the cause of death disclosed by the diseased person or some other person, or such data perceived, examined, measured, projected or derived, as well as all data that can be linked with the foregoing or have influence on them (e.g. about

18 Recommendation No. R (97)5 on the Protection of Medical Data, Council of Europe Committee of Ministers, 1997.

conduct, environment, profession etc.). The Constitutional Court abrogated, as of April 30, 2003, the provision of the Act which defined data relating to a person's sexual life as medical data in the context of medical treatment, arguing that it violated the right to the protection of privacy and personal data secured in the Constitution, and because it conflicted with the prohibition against discrimination.[19] The Court argued that the aims defined in the Act did not justify the processing of data relating to sexual life and that in their original formulation these aims allowed the handling of a disproportionately broad and abstruse class of data relating to sexual life. Their processing therefore was not deemed ineluctable and thus violated the principle of strict aim-dependence.

Paragraph 26 of the Health Care Act sets out the patient's duties. The patient is obligated to inform to the extent made possible by his/her abilities and knowledge, persons participating in his/her medical treatment, about all that is necessary for arriving at the diagnosis, for making the required therapeutic plan and for the appropriate performance of medical interventions, i.e. about all previous diseases, therapies, medication or the taking of other therapeutic substances, and the possible influence of factors which pose a risk to his/her health. The data thus disclosed qualify as medical data, but it is important to note that this obligation of patients must not lead to an indiscriminate piling up of irrelevant data, i.e. the patient may not be obligated to disclose data that are not strictly necessary for arriving at the diagnosis.

The same paragraph obligates patients suffering from a disease classified as infectious that they should name the

19 Constitutional Court Decision 65/2002. (XII.3.)

persons who may have transmitted the disease to them or those they may have infected. This obligation may lead to questionable consequences. For instance, with the HIV infection, which is listed with infectious diseases under the present regulations, it makes anonymous HIV testing impossible.[20]

2.2.3.2. Critical Remarks on the Act on the Protection of Medical Data

In what follows we will comment on those provisions of the Act on the Protection of Medical Data which impose unnecessary restrictions on the rights of data subjects or are not tied to a sufficiently definite aim.

Chapter II. of the Act contains the provision on possible aims for which data processing may be performed. Paragraph 4, Section (1) lays down treatment as the primary purpose of the handling of medical data, while Paragraph 4, Section (2) lists other possible data processors. There is an underlying taxonomy to the list and in accordance with the argumentative part attached to the Act, it contains cases in which authorization by a law is required for data processing. Part of the list contains justified cases of data processing supported by reasons, although it leaves the impression as if the legislator had been trying to collect all conceivable aims for data processing rather than trying to impose limitations on the set of aims for which medical data may legitimately be processed. Even if we skip the question that the authorization seems too broad, two kinds of possibility cannot be left without comment, for the reason that the legitimacy of the aims indicated is strongly questionable: the cases of prevention of

20 See the article on HIV testing in this volume.

crime and cases falling in the scope of the authorization given to perform certain tasks defined in Act XXXIV/1994 on the Police are insufficiently definite classes of case. The constitutionally acceptable aim for which a clearly defined class of data may be handled is not sufficiently specified. The too broad authorization given makes the protection of data subjects – one of the most important objectives of the Act – impossible.

Paragraph 31 on the erasing of false medical data, also raises questions. According to it, false data are to be erased in such a manner that the original should remain recoverable. The argument is that the original data must be preserved so that they can be used as grounds for settling questions of responsibility and for the purposes of court proceedings. Be that as it may, the purpose of erasing false data is thus nullified, as the handling of unlawful data is practically continued. Paragraph 5 of the Data Protection Act says in connection with strict aim-dependence of data handling, that only such personal data may be handled as are indispensable for the realization of the aim of data processing, suitable for the purpose, and to the extent and for the time required for the realization of the aim. Paragraph 11 of the Data Protection Act also says that the data subject is allowed to request the correction of his/her data and their erasure, with the exception of data handling prescribed by law. This right of the data subject is restricted by an arrangement under which data are to be erased in such a way that the original data should remain recoverable. As regards the restriction of this right, the Data Protection Act says that it may be restricted by a law only in the interest of the security of the state from within and without, thus national defense, prevention or prosecution of crime, in the interest of state or local authority financial matters, and in the interest of the protection of the right of the data subject or some other person.

One might wonder whether the handling of medical data may fall in any of these categories of restriction. In any case, the recording of false or unnecessary data may often violate the patient's dignity. The statement of the Data Protection Commissioner in this issue[21] gives no guarantees for the patient's dignity. In the particular case, which led to the Commissioner's statement, the complainant contacted the Commissioner because he claimed that he had been entered in the register of the Hungarian Army's Hospital as a psychiatric patient but his repeated requests for the erasing of the false information had been rejected. In our view, in such cases it is up to the hospital to examine whether it is in fact due to a mistake that the data are in the register. If this is ascertained, the Hospital is under an obligation to erase the false data. According to the Act, the data are to be erased in such a manner that they should remain recoverable. In our view, in cases where the data are simply false, they should be erased completely rather than simply crossed out.

The Commissioner did not comment on the question of erasing. In his statement he referred to Paragraph 30 of the Act on the Protection of Medical Data, which provides that health care documents are to be preserved for at least 30 year from the date of recording the data, and hospital bulletins for at least 50 years. According to this, the Commissioner thinks the data processor's obligation of registration excludes the possibility of erasing false data.

Chapter III. of the Act gives rules for data processing outside the health care provision system. The elaborate exposition of rules for the handling of data recorded in the course of medical treatment is ordered to apply automatically to the processing of data outside the health care provision system. The rules are to be

21 Statement 13/A/2001. of the Data Protection Commissioner on falsely recorded data.

applied "according as is appropriate", but it is not always unambiguous what would count as appropriate extension. It is not immediately obvious, for instance, why it is necessary for data processors outside the health care system to store medical data for the same period of time – normally thirty years, exceptionally fifty – as it is obligatory with data processors within the health care provision system. It would be more appropriate if the Act expounded rules for data processors outside the health care system separately and more elaborately thus avoiding the present unhappy device of simple extension and securing the introduction of rules which really fit their purpose.

Paragraph 23 gives rules for disclosure of data at the request of bodies outside the health care provision system. It obligates physicians in charge of a person's treatment to comply with written requests for medical data and personal identifiers. Paragraph 4, Section (4) enters as a guarantee in this connection, providing that the processing of medical and personal data is restricted in quantity and kind by the idea that both the quantity and the kind of data disclosed should be strictly restricted to what is inevitably required for the attainment of the goal of data processing. Despite this rule situations may arise which lead to conflicts of interest between the aim for which data are requested and the success of the therapy, the patient's personality right and the rules of physicians' ethical code. To take an example, requesting data from a patient's psychiatrist in the context of a civil suit may be seen as rather problematic. It is by no means obvious that therapy and an obligation to disclose data can be reconciled, especially when the patient does not consent.

Let us imagine a situation in which a wife, betrayed by her husband, seeks medical help because the mental and emotional strain has been too much for her. The ensuing events lead to

divorce, as a result of which the court has to decide about the placement of children. The man argues that the woman has been treated by a psychiatrist so she is unfit to bring up the children. He refers to the "evidence" stored by the ex-wife's psychiatrist and requests the court to procure the data from the woman's psychiatrist.

It would be rather opportune for the court in a typical case like the above to appoint a forensic medical expert and provide that he/she should not be entitled to obligate the therapist to disclose data. This, however, would contradict the rules of request for data mentioned above and Paragraph 8, according to which the health care provider has no duty of confidentiality vis-à-vis the forensic medical expert.

The data subject is entitled to prohibit his/her medical data from being disclosed to a third party, with the only exception of cases indicated in Paragraph 13. This is stated in Paragraph 10, Section (2), which provides that data may be disclosed against the data subject's prohibition. In this connection, it does not seem reasonable that it should be obligatory to report the mere suspicion of certain diseases which are listed in Supplement 1 to the Act. Some of these cases cannot reasonably be regarded as grounds for compulsory data provision, e.g. sexually transmitted mycoses. Compulsory reporting might be justified in cases where the person concerned does not cooperate and thereby endangers other persons' health. In other cases it does not seem justifiable to restrict the right to informational self-determination. In addition, according to Paragraph 10, Section (3) data related to previous diseases which have no link with the present one may also be disclosed. This part of the Act is completely without justification. It is difficult to perceive the need for data about previous illnesses which are unrelated to the present one.

3. HCLU CASES OF DATA PROTECTION

Ever since its formation the Hungarian Civil Liberties Union has taken an active part in furthering the cause of data protection by concentrating on the handling of data of drug users and psychiatric patients as well as on questions of the effective observance of patient rights in general. In what follows we will be discussing questions arising in these areas of data protection.

Breaches of rules on medical data and abuses of such data are always to be considered as serious and some kinds of medical data are admittedly to be counted as the most sensitive. Information about drug addiction and mental disorders are undoubtedly among them. Such data are in need of special protection because their inappropriate handling may expose patients to unbearable situations in their work, at their place of living or in other situations in life.

3.1. DRUG USERS

The personal data of drug users may be in need of special protection because someone who turns out to be a drug user may become the target of social prejudices, discrimination, may lose his/her job, or under presently effective criminal law information about his/her drug use may give rise to criminal proceedings against him/her. In addition, drug users may often find themselves in need of medical help because of a variety of health disturbances.

The personal data of drug patients are protected by the constitutionally grounded guarantee that the patient is entitled to having medical and personal data about him/her disclosed to

health care staff in the course of medical provision disclosed only to such persons as are authorized to know them and to having such data treated in a confidential manner.[22] As a main rule, medical data, i.e. sensitive data, may be disclosed with the data subject's written consent only[23], the sole exception to this rule being data processing ordered by a law. The Act on the Protection of Medical Data provides, in Paragraph 24 Section (1), that a physician is under an obligation to report to police (even without a request from police and independently of the patient's consent) in one special case: when the patient has suffered an injury which takes longer than 8 days to heal as a consequence of a supposed criminal act. In our view this cannot apply to drug patients. This opinion will be supported in detail below.

3.1.1. Unlawful Reports to Authorities

The question of unlawful reports to authorities needs to be discussed because physicians often report to police drug users who seek medical help.[24] The legal aid service run by the Hungarian Civil Liberties Union has dealt with several cases of unlawful reporting. Two of these cases, in which HCLU undertook legal representation, will be described below.

In one of these cases a young man had drunk too much at a company party, had gotten sick and was taken to hospital by friends. In the hospital, he was subjected to a variety of examinations, including a drug test, which was positive for

22 Paragraph 25, Section (1) of Act CLIV/1997 on Health Care.

23 Act LXIII/1992 on the Protection of Personal Data and the Publicity of Data of Public Interest, Paragraph 3, Section (2).

24 This is not true to say of health experts specializing in health care provision for drug users. They know and comply with data protection regulations. Physicians working at drug outpatient clinics do not comply with requests for information made by police if they have the slightest doubt about the legality of the requests.

THC. The hospital reported the case to police. Detectives duly turned up at the hospital the following morning, interrogated the young man on the spot and started criminal proceedings against him. During the young man's stay in the hospital, his employer, who had helped him get to the hospital, happened to inquire about his state of health. Hospital staff reported the results of the drug test to the young man's employer, as a result of which he dismissed him from his job.

In the other case an intravenous drug user had sought medical help with an abscess on his arm from the needles he had applied to it. When the physician who was treating him learnt about his drug use, he contacted police, explaining to his patient that it was his "professional obligation". As in the previous case, the report led to criminal proceedings.

One might wonder why physicians feel that they have to report to police a patient who happens to be a drug addict or casual drug user with a specific health problem. There may be two explanations: either the physician simply as a citizen thinks he has to report, or wishes to report, a crime which has come to his/her notice, or he/she thinks he/she is under an obligation to do so under Paragraph 24 of the Act on the Protection of Medical Data, which provides for the physician's obligation to report to police on pain of being considered liable for failing to do so. The result in both cases is a serious breach of the law, or rather the breach of the physician's duty of confidentiality in the one kind of case. One might also note that there is no such thing in Hungarian law as a "citizen's duty to report crime", except for a few, rather rare cases of crime. Drug abuse is not among these rare cases.

According to the above-mentioned paragraph of the Act on the Protection of Medical Data physicians do indeed have an obligation to report to police, namely in cases in which the

person has suffered an injury which does not heal within 8 days, and the injury is a result of a supposed criminal act. When this is the case, disclosure of data is not conditional on the consent of the person concerned. This rule however, cannot be interpreted to the effect that it is to be applied to cases of drug abuse. The mere idea of a physician being obligated to report a patient to police is rather questionable, since people tend to seek medical help with some health problem rather than to have themselves reported to police by a health care provider. Even if we accept this rule with reference to the public interest and accept further that in certain cases there should be compulsory reporting for citizens, the prescription must be interpreted cautiously and with restrictions. Rather regrettably, the locus just quoted is not precise enough and the explanatory provision of the act does not give sufficient guidance, either. If we let ourselves be guided by the wording, we find that the word 'injury' used there cannot be taken to refer to the physical (let alone mental) states of drug patients. The legislator had in mind the compulsory reporting of injuries from gunshots and stabs. This provision cannot be applied to drug patients' attempts to seek medical help: that would be at variance with the interest that drug patients and their environment should be allowed to seek medical help in case a drug patient is sick. In other words, the interest in health care provision should override the interest in the prosecution of crime, in such cases, because unlawful reporting not only violates the drug patient's right but also leads to the serious consequence that drug users, afraid of the criminal law consequences, will refrain from seeking medical help even when they need it.

This interpretation is supported by the Data Protection Commissioner's recommendation, which was given on February

27, 1998[25], in response to a motion submitted by the Hungarian Civil Liberties Union, in which the Commissioner gave a statement about practices injurious to patients' rights in cases involving problems like those sketched above. This statement may be applied, by analogy, to drug patients seeking medical help at hospitals. In the case examined by the Commissioner, the ambulance service had informed police about a person who was sick as a result of drug use. The Commissioner argued that the National Ambulance Service is not entitled to report to police drug users in need of medical help, except when there is good reason to suppose that the life or bodily integrity of ambulance staff arriving at the scene are likely to be endangered. The Commissioner also stated that the personal data of patients are to be given enhanced attention and protection, in conformity with the duty of confidentiality incumbent upon physicians and medical staff generally as well as the observance of the prescriptions of the Data Protection Act.[26]

3.1.2. Police Requests for Medical Data about Drug Patients

Legal rules on police requests for data show great variety as a result of the different drug policies pursued by different governments. The restriction of legal rules on drug use in 1999 led to the introduction of a number of rules which are seriously controversial on several counts. Until 1999 police requests for data from therapeutic establishments could count as legitimate only with regard to persons suspected in accordance with

25 Recommendation 522/A/1997 of the Data Protection Commissioner issued in connection with the ambulance service's unlawful practice which violates the rights of drug users calling an ambulance because of sickness caused by drug consumption.

26 This Recommendation was confirmed by the Commissioner a few years later by a statement addressed to the meeting of the Head Physicians of the National Ambulance Service (515/K/1999)

Paragraph 80, Section (1) of Act XXXIV/1994 on the Police, i.e. when criminal proceedings had been started against a particular person, and some well-grounded suspicion had been disclosed to the person involved. The new legislation introduced with the purpose of fighting organized crime in 1999 introduced some modification into the prescriptions relating to police requests for data. Act LXXV/1999 on the Rules of Police Action against Organized Crime supplemented entitlements for data processing by police, providing that police involved in secret search for information in the course of the investigation of a drug trafficking case were entitled to request data from drug outpatient surgeries and hospitals even when the drug user did not yet have proceedings against him/her going on, i.e. was not a suspect, but could be linked as a drug user with a drug trafficking case. According to the explanatory provisions of the Act Against Organized Crime drug use is to be treated as something linked with drug trafficking. In the opinion of therapeutic experts and of the Hungarian Civil Liberties Union this interpretation of the relevant law threatens to undermine drug patients' willingness to seek help at drug outpatient clinics. The new legislation on organized crime, which became effective on March 1, 2003 and which incorporates a different notion of a case linked with drug trafficking, put an end to this unhappy situation. Under the new law drug consumption no longer qualifies as a state of affairs linked with drug trafficking. This means that requests for data by investigating authorities are again made legitimate only by previous well-grounded suspicion. It is also necessary now that the request for data should be linked with the act of the suspect of which the suspect is being suspected.[27]

27 This question was addressed and answered in the Data Protection Commissioner's statement 172/A/1996.

Another instrument which protects drug patients' medical data is the rule enunciated in Paragraph 23 of the Act on the Protection of Medical Data, which prescribes that the requesting body must indicate the scope of data requested and the aim of data processing. It is then up to the physician to decide whether all the data requested are really necessary for achieving the purpose indicated, it being laid down in law that the purpose limits the quantity and quality of data that may be processed.[28] In his critical comment on a case involving a request for data of the kind we are discussing, the Data Protection Commissioner argued that the entire health care documents cannot be handed over to police, as the entire health care records could not, by definition, meet the requirement of strict aim-dependence.[29] The inquiries conducted by the Commissioner disclose that requesting bodies often omit to indicate the purpose of their requests for data, or often overstep their authorization by requiring information about other persons.[30] It is part of physicians' duty of confidentiality also that the physician is entitled to notify authorities only after a legitimate request for data and only about certain kinds of data.

3.1.3. On the Physician's Duty of Confidentiality

Since physicians are bound by their duty of confidentiality, the well-grounded suspicion of drug abuse must not come from physicians or any member of staff involved in the health care service. These persons acquire confidential data as an inevitable result of the performance of their professional tasks,

28 Paragraph 4, Section (4), Act XLVII./1997 on the Protection of Medical data.
29 Statement 25/K/2001. by the Data Protection Commissioner.
30 Statement 499/K/1999 by the Data Protection Commissioner.

and must proceed with the greatest caution with regard to other persons' data.

The physician's duty of confidentiality is prescribed by Paragraph 138 of the Health Care Act. According to it, every person employed in the health care service and every person under a contract for work with the health care service is bound by a duty of confidentiality with respect to all data and facts about the patient's state of health and other matters disclosed in the course of the health care work irrespective of the way in which the data are disclosed, e.g. directly from the patient, during examination or therapy, or indirectly from health care records or in any other way. Exemption from the duty of confidentiality may be given by the patient or by a legal instrument which prescribes that the data should be disclosed. On the basis of Paragraph 8 of the Act on the Protection of Medical Data the health care provider – with the exception of the patient's family physician or the forensic medical expert – is under a duty of confidentiality vis-à-vis the health care provider who has not taken part in the medical examination, the establishing of the diagnosis and/or in an operation, unless the disclosure of the data is necessary for establishing the diagnosis or in the interest of further therapy for the patient.

From what has been said we can conclude that there is no legal rule which would obligate or authorize health care staff to report drug cases to police. Consequently, the physician who does this violates not only the most fundamental ethical and legal rule of his/her profession but also violates the Constitution, the Act on Data Protection, the Health Care Act and the Act on the Protection of Medical Data, and even commits a criminal act, under Paragraph 77/A of the Penal Code.

The Hungarian Civil Liberties Union took the following legal steps in connection with the unlawful reports: it started proceedings in the ethical committee of a county chamber of physicians, and filed a complaint with the head of a hospital. To promote a solution at the national level it addressed an open letter to the president of the Hungarian Chamber of Physicians on September 10, 2001, asking the said body to help to put an end to the unlawful practice.

3.2. USERS OF PSYCHIATRIC SERVICES

Persons suffering from mental disorders are like drug patients in being exposed to prejudices on the part of society and they may suffer from disadvantageous discrimination by having their data published by others. These facts alone are reason to build up a system of guarantees for their protection. The Health Care Act devotes a separate chapter to psychiatric therapy and care, emphasizing the enhanced need for protecting patients' personality rights. By contrast, the Act on the Protection of Medical Data contains no rules specifically geared to the need of mental patients for protection. They are treated within the framework offered by the general rules expounded previously.

The Data Protection Commissioner has conducted several examinations on matters relating to the protection of mental patients' medical data. In 1996 the Hungarian Psychiatric Society reported in a petition submitted at the Commissioner's office that police had requested a list of "persons under neurological treatment" from a hospital in the course of an investigation. The relevant provisions of the Police Act on requests for data apply to the case, i.e. data may be legitimately

requested only about a particular suspect in connection with a specific act. The Commissioner argued that involving a number of mental patients as possible suspects in an investigation on a poorly specified suspicion violated the right of the persons concerned to informational self-determination. Compiling a list of the data of all patients treated at an establishment represents an unreasonable extension of the class of possible suspects.

With users of psychiatric services patient rights may occasionally be realized in a restricted form, in comparison with other patients' rights. The Health Care Act treats the restriction of these rights as an auxiliary measure for exceptional circumstances and makes their application dependent on certain conditions. The right to have access to medical records, e.g. may be restricted according to Paragraph 193 of the Health Care Act only when there is good reason to suppose that it would greatly endanger the patient's recovery if he/she were to get to know his/her diagnosis, or if it violated another person's privacy.

The legal aid service of the Hungarian Civil Liberties Union was contacted by a client in 2000 who had been treated at a psychiatry department a few years earlier and who had his right to have access to his medical files denied with reference to the above-mentioned Paragraph. The client had not had any contact with the hospital for 8 years and was leading a normal life, working in a job. There was no reason to suppose that his recovery would be endangered by his getting to know his medical data. HCLU undertook to represent the patient in court, proposing that the court should obligate the hospital to make the documents available. The court finally obligated the hospital to do so, but it also obligated the "ex-psychiatric patient" to prove that his getting to know the medical documents would not have any harmful effects on him, thus laying the onus of proof on him. In HCLU's view the

hospital should have been made to prove the reasonableness of the exceptional restriction of the right instead of the patient being made to prove the unreasonableness of the restriction of his right.

The case reveals that the application of this provision to mental patients becomes real not as an exception but as an automatic response without the effect of the documents on the patient being ascertained. This restriction should only be applied in exceptional cases, and it should be proved by the physician refusing to make the documents available that the case was exceptional. As it is, the legal rule does not give sufficient guidance for hospitals concerning the circumstances under which the restriction may be applied. In its statement issued on October 22, 1998, the Professional College of Clinical Psychologists argued that the restriction was to be applied primarily in cases of mental disturbance "which essentially, i.e. as a diagnostic criterion, involved the lack of an awareness of being ill, and was coupled with a distorted perception of reality or its representation in a distorted frame of reference and all these features were present in the patient to a high degree". According to the statement "the law does not license the treating physician to use restriction as an automatic response to the fact that certain diagnostic criteria are met; rather, cases must be judged on an individual basis".

3.3. THE PATIENT'S RIGHT TO HAVE ACCESS TO MEDICAL FILES

We have discussed the question of the patient's right to informational self-determination, whch means that it is the patient who has control over data handled by the health care

establishment contained in his/her medical documents. Closely related to this is the right to have access to medical files and information about data processing. These are fundamental entitlements belonging to each and every patient. Complaints about the restriction of this right often form the subject matter of petitions dealt with in the Data Protection Commissioner's reports.

The right to have access to medical files confers on the patient not only the entitlement to look into medical data about him/her but also the right to be given copies of the medical documents at his/her own cost. Many people are unaware of the further possibility of asking only for inspection and during inspection choose the documents they want copies of. Medical documents often add up to thick files and patients rarely need the entire collection. It is essential for the effective exercise of this right of the patient's that the fee of photocopying should not be as high as to act as a deterrent. The Health Care Act gives no guidance on this matter. In many establishments the price of photocopying is set arbitrarily with reference to the need to employ an extra person for the job and to the electricity bill. It is easy to see that thirty thousand HUF (EUR 120) for thirty pages is a forceful deterrent. It is interesting to look at the Dutch regulations in this connection, in which one of the executive decrees attached to the Act on the Protection of Personal Data[31] orders that the health care provider charge a reasonable fee for photocopying. The maximum fee allowed for providing a copy is EUR 4.50.

One of the patient's entitlements somewhat indirectly related to the right to have access to medical files is his right to ask for correction if he/she perceives that the data do not match

31 Thee Hooghienstra: "The Implementation of Directive 95/46/EC in the Netherlands, with special Regard to Medical Data." In: *European Journal of Health Law,* Volume 9, No.3. September 2002, 227.o.

the facts and he/she may even ask for his/her data to be erased except in cases of data processing ordered in law. Also related to this is the rule referred to earlier, according to which the false data are not erased but crossed out in a way which leaves them identifiable. In the opinion of the Hungarian Civil Liberties Union, which we have expounded earlier in this article, this may often violate the patient's dignity.

4. SUMMARY

The aim of this article was to highlight the importance of the protection of medical data on account of their sensitivity and vulnerability and to emphasize that the related right to informational self-determination must be secured as widespread effective observance as possible. We have tried to highlight some shortcomings in the protection of medical data and the directions we think legislation should take to promote lawful practices, by analyzing questionable provisions of the Act on the Protection of Medical Data and by discussing questionable practices experienced by the Hungarian Civil Liberties Union. In this connection we have wished to draw attention to the need to always keep in view, when thinking of regulations affecting medical data, that individuals' right to informational self-determination may be restricted only in very rare cases and within strict limits.

ON THE SIGNIFICANCE OF ANONYMITY

Eszter Csernus

It has been over twenty years now since the HIV infection which causes AIDS was first diagnosed and the epidemic caused by the virus has since assumed world-wide proportions. According to a UN estimate there are 42 million persons infected with HIV, 5 million were infected during 2002, and 3.1 million died of AIDS in 2002. The fight against the disease is made difficult by the fact that virus carriers may live without any symptoms for several years and that neither an effective antidote or therapy, nor a vaccine has been found till the present day.

The number of the HIV infected in Hungary is relatively low. Officially registered data show that there are 1000 or so people with HIV living in the country, and UNAIDS estimates that there may be an additional 3000 undiagnosed cases. This favorable situation may be due to a number of factors. There have been regular information campaigns in this country since the late 1980s and preventive and educational activities among the at that time most endangered group – that of gays – has also been rather intense. HIV testing facilities were established at a rather early stage, and already in 1988 a decree was issued for the testing of blood used in medical interventions. Another circumstance that helped the country avoid a major epidemic wave was the fact that the country had been relatively closed against the world until 1990.

At present however the spread of the virus is at its fastest in the region and intravenous drug use is undoubtedly the leading mode of transmission. The number of those infected through

heterosexual contact is practically the same as the number of those infected through homosexual contact. In light of all these facts it is now requisite to work out and apply new strategies and, in light of international experiences our approach to HIV/AIDS-related data is an important part of these strategies.

Medical data are treated in Hungarian law as especially sensitive data whose protection requires special attention. This special attention must mean enhanced protection for data related to the HIV infection and AIDS, this being the only disease which is associated in the public mind with negative overtones, discrimination and stigma. Questions of the protection of HIV/AIDS-related data arise at several points. The informational self-determination of those affected by HIV/AIDS must be examined in terms of HIV screening, collection of data to find out about the percentage of the HIV infected among the Hungarian population, measures taken to affecting the partners and environment of people with HIV, and control examinations of and therapy for people with HIV. Besides outlining real or supposed conflicts of interest I will recapitulate international recommendations and practices and finally I will present the domestic legal background.[1]

1. QUESTIONS OF DATA PROTECTION RELATED TO TESTING

We have to study two issues: that of voluntariness and that of anonymity. These two criteria are closely related: when screening is obligatory, there is no practical possibility of securing anonymity, while anonymous testing is sought on a

1 In the discussion of the above issues I drew significantly on the publications of the Canadian HIV/AIDS Legal Network (www.aidslaw.ca).

voluntary basis. Which of these options a state will take traditionally depends on which interest it favors: the right to privacy, confidentiality and informational self-determination, or the public health interest, which is part of the public interest. Although the right to informational self-determination is one of the fundamental rights, it is by no means absolute and may be open to restrictions under specific circumstances such as for epidemiological considerations.[2] In what follows we will examine the expectations which have been expressed in connection with the protection or disclosure of data on people with HIV, how far these expectations can be regarded as well founded, and whether the protection of public health and respect for human rights are really contradictory aims.

1.1. SCREENING POLICIES

Before undertaking a closer examination of rules specifically relating to screening, it is as well to get clear about two fundamentally different approaches to infectious diseases.

The traditional epidemiological approach, which evolved in the late 19th and early 20th centuries, defines its basic concepts along the following principles and methods:

– identify infected persons,
– report identified cases to public health authorities with a view to registering them,
– seek out the contacts of the person found infected,
– separate persons infected from the rest of society, and finally
– heal the persons thus separated.

2 The decision of the European Court of Human Rights which weighs the interest in public health against the right to privacy is discussed in 2.1.1. of Márta Faur's article in the present volume *(The Editor)*.

This model was worked out to combat infectious diseases which are transmitted through ordinary contact, have a short period of latency, and for which there is a therapy. By contrast, HIV/AIDS is not transmitted through ordinary contact (only through sexual intercourse and contact with blood and certain other kinds of mucus). Transmission can be avoided by observing a number of simple rules of hygiene and conduct, and people with HIV can live without symptoms and are capable of working if they receive appropriate therapy. There is no effective therapy or vaccine against the disease as yet.

The other epidemiological approach was elaborated on the basis of the above considerations in the past few decades after a number of countries had recognized that the traditional methods were not effective in preventing the disease from spreading. This approach is based on the insight that the members of certain especially endangered groups – intravenous drug users, gays, sex workers – were rather distrustful to the state and that their readiness to cooperate was weakened rather than encouraged by authoritatively enforceable epidemiological measures. The modern approach is based on full respect for the fundamental human rights of people with HIV and on the informed consent and cooperation of those concerned.

1.1.1. International Recommendations

The participants in a consultation called 'HIV/AIDS and Human Rights' invited by UNAIDS and the UN High Commissioner for Human Rights held in Geneva in 1996 formulated certain International Guidelines.[3] They laid down the following ways of regulating the issue of HIV/AIDS:

3 International Guidelines on HIV/AIDS and Human Rights (23-25 September 1996, Geneva), United Nations Publications, New York and Geneva, 1998, (henceforward *'International Guidelines'*).

"States should review and reform public health laws to ensure that they adequately address public health issues raised by HIV/AIDS, that their provisions applicable to casually transmitted diseases are not inappropriately applied to HIV/AIDS and that they are consistent with international human rights obligations."[4]

As regards the recording and processing of data related to HIV/AIDS, experts called on member states to follow the principle that

"General confidentiality and privacy laws should be enacted. HIV-related information on individuals should be included within definitions of personal/medical data subject to protection and should prohibit the unauthorized use and/or publication of HIV-related information on individuals. Privacy legislation should enable an individual to see his or her own records and to request amendments to ensure that such information is accurate, relevant, complete and up to date. An independent agency should be established to redress breaches of confidentiality. Provision should be made for professional bodies to discipline cases of breaches of confidentiality as professional misconduct under codes of conduct discussed below. (...)."[5]

At the regional level the Council of Europe has emphasized the importance of voluntariness and anonymity since 1987:

4 *International Guidelines*, Guideline 3.
5 *International Guidelines*, Guideline 5, 30 c).

"2.2.1. Screening

(…)

– there should be no compulsory screening of the general population nor of particular population groups;

– health authorities should instead invest resources in the setting up of sites – when these do not already exist – for voluntary testing fully respecting confidentiality regulations (…);"[6]

and both were specified as preconditions of early pharmacological intervention:

'The Committee of Ministers (…) recommends that governments of member states (…)

vi. create optimal conditions for early pharmacological intervention, in particular:

a. (…) availability of (…) anonymous and voluntary testing (…)'[7]

Thus both universal and regional international organizations supported the practice of screening without recording personal identifiers. Nevertheless, in certain countries, including Hungary, rules were adopted which contradict these recommendations.

1.1.2. Arguments for Recording Personal Identifiers

One of the arguments most frequently propounded against anonymous testing is the idea that the more we can know about the HIV infected people in a given area, the more effectively we

6 Recommendation No R(87)25 Concerning a Common European Public Health Policy to Fight the Acquired Immunodeficiency Syndrome (AIDS).

7 Recommendation No R(94)10 on Early Pharmacological Intervention against HIV Infection.

can fight against the spread of the virus. According to the other traditional argument there are certain persons or groups who "have the right to know about" the HIV infectiousness of certain persons, and this "right" can be made effective only if a list of the names of people with HIV infection is kept.

I will develop these arguments in more detail in subsequent chapters.

1.1.3. The Hungarian Regulations

Until December 31, 2002 prescriptions for HIV screening were regulated by a Decree issued in 1988[8] (henceforward 'Decree') which was abrogated by the Constitutional Court for reasons of formal deficiency. The Court's decision rested on the consideration that a decree was not at the appropriate level of regulation in the hierarchy of legal instruments to qualify as a legal instrument for the purpose of limiting several fundamental rights and that according to the Constitution such a legal function could only legitimately be fulfilled by a law. The Court took care to leave enough time for the elaboration and enactment of the new legal instruments to replace the unconstitutional Decree, so the Decree was abrogated only as of December 31, 2002. The new Act that replaced the Decree at the appropriate level was promulgated on December 17, 2002.

Although the rules originally enunciated in the Decree did not expressly mention the possibility of anonymous testing, they did not feature any directions that excluded it either, as a result of which there were several anonymous testing facilities and counseling services all around the country which were "tolerated".

8 Ministry of Health and Social Affairs Decree 5/1988.(V.31.) on the Measures Necessary for Preventing the Spread of the Acquired Immune Deficiency Syndrome and on the Issuing of Directives for Screening.

Legal rules changed as of January, 1998: from then on HIV testing was possible only under conditions of "partial anonymity". The legislator acknowledged the fact of participation in the screening as a sensitive data which may gives rise to a justified right to protection on the side of the participant, and thus provided for the possibility of anonymity but only in cases of first testing[9]. What this so-called "partial anonymity" meant in practice was this: if the person concerned had participated in the first test without supplying his/her personal identifiers and he/she had tested positive on the first test, the verifying second test could only be performed on the condition that he/she laid his/her personal identifiers at the facility's disposal, i.e. relinquished his/her anonymity. If the person refused to provide personal identifiers he/she lost his/her chance to have the testing continued and get to know his/her HIV status. If the first examination ended with negative results, the person concerned came under no obligation to supply personal particulars, or if he/she had participated in the first test with his/her name, these data were erased.

If the first test ended with positive results, but the second, verifying examination with negative results, the health care facility again came under an obligation to erase his/her medical and personal data without delay. This obligation of erasure was motivated by a negative public image of and beliefs about HIV/AIDS. The mere fact, if it becomes known, that someone has been tested for HIV, immediately becomes a disadvantage for the person concerned, as it starts off a series of guesses as

9 In order for the results of HIV testing to be considered as positive, two tests are required, because the first examination is not 100% reliable. It may indicate positive results even in cases where the person examined is not infected. The second examination is based on a different procedure and is designed to confirm or disconfirm the results of the first.

to what reason he/she may have had to fear having been infected. Knowing, however, that under the Act on the Protection of Medical Data[10] data in the health care settings are to be erased in such a manner that erased data can be recovered later, the prescriptions enunciated in this provision come to look rather illusory and the range of persons to whom the data, otherwise "erased", may be passed on slips out of control.

The distinction between the two examinations in terms of data requirements cannot have been motivated by a public interest. It is difficult to understand why the interest in anonymity acknowledged on the occasion of participation in the first test should be overridden on the occasion of the second examination when clearly the information to be protected is even more sensitive than the first time, since it may give an opportunity for abuse by persons unauthorized to possess them. Indeed, it is more dangerous, in terms of public health, to "lose track of" a person of unclarified HIV status, potentially infected, without his/her knowing whether he/she is infected or not.

At the decision of the Constitutional Court Parliament adopted Act LVIII/2002, which provides for the modification of the Health Care Act[11] and introduces rules for HIV screening at the level of laws. It is important to emphasize that the only motivation for the modification was the Constitutional Court's decision. The Government acted only to fulfill its duty of law-making rather than from an underlying change in public health policy.

The modification had been preceded by heated debates. Proponents were intent merely on elevating to the level of laws the rules of the old Decree without any examination of its content. The first draft of the bill, however, met with fierce

10 Act XLVII/1997 on the Handling and Protection of Health Information and Related Personal Data.

11 Act CLIV/1997 on Health Care (henceforward "Health Care Act".)

objections from the Data Protection Commissioner, health care experts and civil organizations. Leaving constitutional requirements on content out of consideration, the proposal disregarded international recommendations and experiences and envisaged introducing poorly defined and vague specifications of groups of persons under an obligation to submit to screening. Those to fall under mandatory testing were to have included the members of the family, colleagues and neighbors of the HIV positive person. The proposal did not refer separately to HIV and AIDS, conflating prescriptions relating to HIV/AIDS with those for other epidemiological diseases.

Thanks to the media[12], the personal protest of the Data Protection Commissioner before the Parliamentary Committee for Human Rights, Minorities and Religion and a Statement[13] issued by the Hungarian Civil Liberties Union, which leveled a sharp attack at the proposal, were given sufficient publicity. As a result, the proposal was modified in several respects.

The most important of these achievements was the promotion of voluntary testing to the status of main rule. Voluntary testing may be done with personal identifiers or anonymously, and if a person opts for anonymous testing, he/she is not under an obligation to disclose personal data either at the first or the second examination. Thus the provisions make it possible for persons outside the groups of persons specifically listed who can be submitted to mandatory testing[14], to avail themselves of reliable testing results under conditions of anonymity.

It must be emphasized, however, that what we have is not a practice of testing facilities conducting anonymous testing as a

12 Tamás Virág, "Shared Responsibility", in: *Magyar Narancs,* October 31, 2002; Anna Danó, "With or without a Name?", in: *Népszabadság,* November 4, 2002; Judit Muhari, "Anonymity a Possible Hazard", in: *Népszava,* November 5, 2002.

13 Statement No 18 of HCLU.

14 These groups of persons will be specified in the following passage.

matter of course. What we have is only a situation in which "persons presenting for testing may refuse to disclose their personal identifiers at any stage of the examination"[15]. In other words, anonymity has to be requested by the person concerned and the law does not underline any express obligation on the part of the testing facility to inform those presenting for testing of the possibility of anonymous testing. A person presenting for testing can hardly be expected to stand up for something of which he/she is ignorant. Although the general obligation to inform clients, stipulated in the Health Care Act, applies automatically to HIV testing too, we find it desirable that the obligation of testing facilities to inform persons of the possibility of anonymous testing should be given special emphasis among the rules for HIV screening so that practical difficulties of interpretation are removed.

According to the new regulations, anonymity ends at the point where the person concerned presents for medical treatment, even then, however, only to the extent that is made inevitably necessary for the therapy he/she needs. Some confusion is created by the passage of the Act on the Protection of Medical Data which says that "if the testing results are positive, the person concerned is under an obligation to give his/her personal data at the request of the screening facility."[16] This provision is in straightforward contradiction with the new rules of the Health Care Act. It is highly desirable to remove this equivocation as soon as possible, especially because it is far from clear what sort of interest requires that the person's identifiers should be recorded prior to his or her presentation for medical treatment. The identification of infection carriers has a point only under the traditional infectious disease approach, but that approach is not applicable to HIV/AIDS.

15 Paragraph 59, Section (5) of the Health Care Act.
16 Paragraph 15, Section (6) of the Health Care Act

The new ministerial decree issued in connection with the modified Health Care Act[17] is also open to objections in that it makes a discriminatory distinction between two group concerning the right of HIV positive persons to informational self-determination. If tested anonymously, a person with positive results has the right to decide whether he/she will contact the health care institution designated for him/her. If, by contrast, the positive results are the outcome of a non-anonymously conducted examination, the physician taking the blood sample takes steps without further authorization and notifies the health care facility entitled to admit the person as its client, "which takes the person infected into care within a week from receipt of the medical files".[18] Rather regrettably, the legislator failed to think of considerations other than of technicality and feasibility in making rules affecting the right of people with HIV to informational self-determination – will people with HIV present for care, who do they entitle to have access to their medical files?[19]

Another objectionable feature of valid rules is the stipulation that the blood sample of a person taking part in non-anonymous HIV testing is to be sent to the laboratory in conjunction with a sheet which has the person's social security number on it.[20] The social security card number is a data which can be used to identify a person, and its inclusion on a sheet in this kind of case cannot be seen to have any reasonable purpose associated with it

17 Ministry of Health and Social and Family Affairs Decree 18/2002.(XII.28.) on Measures Necessary for Preventing the Spread of the Infection Causing the Acquired Immune Deficiency Syndrome and the Order of Conducting Screening Tests.

18 Paragraph 5, Section (1), of the Ministry of Health and Social and Family Affairs Decree 18/2002.(XII.28.)

19 The distinction between People with HIV and HIV negative persons is even more striking in light of Paragraph 12, Section (4) of the above decree. The passage in question orders that in case of non-anonymous testing the personal identifiers of persons testing negative on the second test are to be erased immediately.

20 Paragraph 12, Section (1) of the Ministry of Health and Social and Family Affairs Decree.

that could not be achieved otherwise. It is desirable that the blood sample should be given a code number even for non-anonymous testers as is usual in the case of anonymous testing.[21]

The reason why the person concerned has not been given the discretion to "change his/her mind" is again hard to penetrate. Why not give the person control over what happens to his/her personal data from the moment he/she has disclosed them for the first time? According to the Data Protection Act[22] "the person concerned (...) may request a correction in his/her data and – with the exceptions of mandatory data processing ordered in a legal rule – their erasure."[23] As in the present case there is no obligation to provide personal data – if there were, anonymous testing would be rendered impossible – the person concerned should have the freedom to revoke consent to the handling of his/her data which are suitable for personal identification, and if that were the case, the data would be barred from being transmitted to a health care facility.

1.2. MANDATORY TESTING OF PARTICULAR GROUPS

The modification applied also to the definition of cases in which screening is mandatory. The existence of mandatory testing is itself an offspring of the traditional epidemiological approach, which aims at identifying infected persons. Those who argue for mandatory testing for persons belonging to particular groups usually justify identification in two ways:

– either they subscribe to the idea of the existence of certain

21 Paragraph 12, Section (2), op.cit.
22 Act LXIII./1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest.
23 Paragraph 11, Section (1), b).

"endangered groups" in which the chances of HIV occurrence are greater than usual and therefore think it reasonable to screen those in these groups (such groups were defined by the abrogated Decree);

– or they define the class of those to be subject to mandatory screening with reference to individuals' conduct or the danger posed by their conduct (although the new regulation shows a clear shift toward this approach, certain remnants of the old conception still linger).

1.2.1. Regulation in Force until the End of 2002

Under the Decree those subject to mandatory screening included persons with venereal diseases, and persons in a condition indicating possible venereal disease, sexual partners of people with HIV, persons in the environment of people with HIV who could be supposed to have been infected, prisoners, young people in correctional facilities, and intravenous drug users.

These regulations occasioned serious objections and reservations. First of all, concepts were vaguely defined, expressions such as "those in a condition giving rise to a suspicion of venereal disease", "environment" and "suspected infection" were open to an unreasonably broad range of interpretations and thus came up against the principle of legal security.

One of the distinctive characteristics of HIV/AIDS is the fact that its symptoms, if any, are hard to recognize, and so practically anyone could have been subjected to mandatory screening with reference to the Decree. Secondly, it is by no means clear what arguments there are for the mandatory screening of persons serving prison sentences or young people in correctional facilities.

Legally justified deprivation of freedom gives no authorization to restrict the right of the person imprisoned to make health care decisions autonomously. Thirdly, there is no point in subjecting to mandatory screening such groups as the members of which are impossible or hard to identify: we think mandatory screening of intravenous drug users is practically not feasible. Intravenous drug users count as criminals who are likely to do their utmost to hide from the eyes of authorities. Compulsory measures and registration of HIV cases motivate them to avoid testing facilities. Equally there is no guarantee that every HIV positive person will disclose the names of all his/her sexual partners.

In addition to being injurious to a number of fundamental rights, mandatory screening was also incapable of dealing with the problems caused by what is called the "window period". The window period is a period of 4-6 weeks during which HIV test results are rather unreliable even when the virus is already within the organism. HIV testing during this period may yield misleading negative results.

It is also important to emphasize that as mandatory screening is necessarily non-anonymous, these rules brought with them a risk of discrimination exactly for those who were already stigmatized by society on account of their belonging to a risk group anyway.

1. 2. 2. The New Hungarian Regulations

As we have mentioned above, the main rule in the new regulations prescribes voluntary and anonymous testing. Nevertheless there are exceptions to the main rule which are specified in an itemized list. Screening is mandatory for

– "a person who may transmit the virus through his/her blood or mucus or may be infected by other persons' blood or mucus in the course of his/her job, whether regular or voluntary or earning activity;
– blood donors; women donating mother's milk to other women, organ or tissue donors or persons who did not while alive issue a directive prohibiting removal of their organs or tissue;
– persons suspected of, or indicted on the charge of, a crime against sexual morality, drug abuse, persons suspected of, or indicated on the charge of, assault leading to injury which may have involved infection, persons who have suffered such injury as a result of assault involving a risk of infection;
– and also persons who have been ordered by a court to be subjected to screening for the infection."

Undoubtedly a person receiving blood, organ, tissue or mother's milk from another has a rightful interest in being prevented from infection by the virus, but this aim can be achieved in ways other than screening the donor. Instead of screening the donor, the anonymously taken blood itself can be tested, and the risk of infection through mother's milk can be avoided by heating the milk, since HIV dissolves at 56 oC.

By contrast, we have objections in principle to screening the first class of persons, viz. those exposed to vocational hazards. First, the general rules of hygiene prescribed for health care institutions, if carefully observed, suffice for excluding the risk of infection. Second, in view of the window period (and the false negative results that can be obtained during it) the efficacy of screening is more than doubtful. Regular mandatory HIV screening only produces a false sense of security and all that is

purchased at the cost of serious violations of the fundamental rights of those affected. Coercive measures in connection with HIV should be seriously considered only in emergencies as the Data Protection Commissioner stated in his opinion written to the Constitutional Court:

"The right to informational self-determination may be legitimately restricted only in cases of a direct threat of infection. Unless this is acknowledged, the interest in preventing the virus from spreading opens up the way for the introduction of total control over the entire population, which could, and should be regularly repeated"[24].

Another objectionable feature of the rule is its imprecision of wording which opens up the possibility of divergent interpretations concerning the range of jobs, voluntary work and earning activities which are to be subject to mandatory screening. The imprecise reference to the mode of transmission ("blood and mucus") is another cause for concern. Nor do we get any guidance on what "may get in direct contact" is to mean and in light of all this it seems to be anybody's guess by what criteria a vocational health service is going to impose the HIV test as a precondition for employment[25]. Different practices may evolve in different places in the country. Despite undeniable advances in precision made by the new regulation it still remains unclear how frequently health care employees doing invasive interventions are supposed to be subjected to HIV testing, and how the insecurities resulting from the window period and of the first test results are supposed to be

24 Letter 663/B/1996. written by the Data Protection Commissioner.

25 In addition to occupational health service, the family physician may also find himself/herself having to decide about this question, but the family physician has to ask advice from an infectologist before making the decision.

removed; in addition, the results are like snapshots, which are a rather unreliable indicator of the person's state of health.

The fifth group of persons subject to mandatory testing may have been motivated by considerations of the interests of the aggrieved parties to certain criminal acts, presumably for the aim of minimizing the risk of infection as a result of violent conduct on someone else's part. If the person exposed to the infection is treated with anti-retrovirus medication without delay (within a few hours as latest) chances are that he/she will not be infected. In this case "without delay" means such a short span of time that the aggrieved cannot be expected to report the assault to police and get to the stage at which there is a proper suspect or accused. Indeed, not even as much delay can be allowed as is sufficient for positive results to be confirmed. If the person concerned makes the commencement of therapy conditional on the test results of the assaulter, he/she is more than likely to miss its beneficial effects. It is not clear therefore what is the rightful interest with reference to which the rights of persons in this class are to be restricted, or what the legitimate advantage may be that can counterbalance the right of suspects and perpetrators to self-determination.

It seems opportune to mention at this juncture the more than objectionable nature of the procedures that are applied with HIV positive inmates in penitentiary facilities. According to the earlier regulations persons serving prison sentences were also subject to mandatory HIV screening, and in accordance with the Decree on the Health Care Provision for Inmates "prisoners infected with the AIDS virus are to be placed in the penitentiary facility designated for this purpose independent of the stage of their disease in the interest of their enhanced protection, the protection of the community and their own state

of health"[26]. It is not clear what sort of "protection" is supposed to be accorded by separation either for the HIV positive or the other inmates. In addition, being referred to the 'K' unit of the Tököl prison immediately discloses someone's HIV status[27].

Under the new law persons belonging to one of the categories falling under mandatory screening are not to be tested anonymously under any circumstances. If a person anonymously tested turns out to belong to one or another of the categories falling under mandatory screening the examination ceases to be anonymous and is to be continued only on condition that the person concerned provides reliable, officially certified proof of his/her identity. This restriction is pointless partly because personalized screening is unnecessary with the groups specified (mother's milk, blood) and partly for the reason that anonymous test results could not be to anyone's disadvantage since they will not be accepted either by the employer or the court.

2. QUESTIONS OF DATA PROTECTION RELATED TO MANDATORY REPORTING AND REGISTRATION

There are, in principle, three reasons in support of the mandatory reporting with HIV/AIDS:

– to help educational and counseling facilities target and reach those groups which are really in need of information, i.e. which have a higher than average percentage of HIV infected among their members;
– to secure the availability of sufficient data for epidemiological establishments to help them form a realistic picture of the

26 Ministry of Justice Decree 5/1998.(III.6.).
27 For a more detailed account of the processing of medical data of inmates (including their data relating to HIV status) see Andrea Pelle's article in the present volume *(The Editor)*.

epidemiological situation, which is an important condition of an effective fight against the spread of HIV;

– to secure that the partners of people with HIV are informed about the risk of infection[28].

2.1. POSSIBLE WAYS OF COLLECTING EPIDEMIOLOGICAL DATA

Reporting HIV positive cases is an internationally accepted practice which is justified by the aims of a realistic assessment of the epidemiological situation and the ability of authorities to make any steps that are necessary (such as the organization of educational campaigns, budgeting in advance for the expenses etc.). It is indeed important for authorities and health care establishments to have a realistic picture of the distribution of the epidemic across the population in terms of age groups, sexes, manner of transmission, geographical distribution etc.

At the same time there are several methods for collecting data: active and passive, personalized and anonymous. The duty to report may fall only to those with AIDS or to people with HIV also.

Data are said to be collected passively when the establishment editing the statistics undertakes no surveys but merely records cases that are reported to it. Readiness to report cases on the part of establishments concerned is declining however, which results in less reliable statistics. Another drawback to this method is the way it is restricted to information about those people with HIV who have presented for examination, which is another way the resulting statistics

28 More about this argument will be said in the following chapter.

can be seen as unreliable. By contrast, the method called sentinel surveillance – based on active and targeted collection of information – is designed to get information about certain groups within the population through an examination of its members treated in some health care establishment. Data related to the spread of the HIV infection among pregnant women, for instance, can be gathered by subjecting to HIV testing anonymized blood samples of pregnant women in antenatal clinics. Sentinel surveillance leads to more reliable results than passive reporting and fully respects the right of persons to informational self-determination.

The irrelevance of personalized registers of people with HIV to the aim of surveying the epidemic is supported by the guidelines adopted at the Geneva consultation:

"Public health legislation should ensure that HIV and AIDS cases reported to public health authorities for epidemiological purposes are subject to strict rules of data protection and confidentiality."[29]

Several civil organizations have made public statements concerning the question of the manner of reporting and registration, and one of them, the National Association of Persons with HIV/AIDS (USA) summarized in fourteen articles its expectations concerning the guarantees associated with reporting[30]. First among them is the requirement of anonymity.

As far as Europe is concerned, a study completed in September 1997[31] reveals that most European countries run a reporting

29 *International Guidelines* 28.e).

30 National Assembly of Persons with HIV/AIDS – NAPWA Position Statement on HIV Surveillance, 3 October 1997.

31 Centre européen pour la surveillance épidémiologique du SIDA – Surveillance du VIH/SIDA en Europe. Saint-Maurice le Centre, Rapport trimestriel no 56, 1997(4).

system but only a tiny fraction of European states require reporting with personal identifiers which clearly pose a hazard of infringements of the right to protection for personal data.

The reasons usually advanced in support of the necessity of running registers include two aims – defining the target groups and collecting epidemiological data – which hardly require that the authorities should know people with HIV by name. Registration with personal identifiers may become a disadvantage not only because it may create an opportunity for abuse or give rise to distrust and motivate the infected to avoid screening facilities, but also data may "transpire" even under conditions of the strictest data protection regulations. In 1996, for instance, the data of four thousand people with HIV got out of the Health Ministry of Florida to land with the media.

2.2.THE HUNGARIAN REGULATIONS

In Hungary today there is mandatory reporting of new HIV cases, and there is, regrettably, a complete lack of harmony in this area between practices and the new regulations[32].

A legal rule orders that the health service establishment is to make an anonymized report on HIV infection to the Surgeon General's Office, but the competent municipal establishment of the Office may ask for the personal identifiers also with reference to a public health or epidemiological interest[33]. Other rules order that the Surgeon General's Office is to "run a register" of persons with HIV. In vain would we look for a definition of what exactly a "register" is supposed to be. By contrast, the fact that infected

32 The recently adopted modification affects the Health Care Act only.

33 Paragraph 15, Section (2) of the Act on the Protection of Medical Data and Paragraph 1, Section (1) and Paragraph 2, Sections (1)-(2) of the Ministry of Welfare Decree 63/1997. (XII.21.) on the Order of Reporting Infectious Diseases.

persons rather than cases of infection are to be registered does not seem to be an accident and the suspicion that we have to do with a personalized register is confirmed by the distinction made in the decree on infectious diseases[34] between the "Béla Johan" National Center for Epidemiology and the municipal and county institutions of the Surgeon General's Office. The National Center for Epidemiology "registers the medical data of persons with an infection who have been reported", while the municipal institute of the Surgeon General's Office, the county institution of the Surgeon General's Office and the family physician of the person concerned "register the patient with an infection reported". This suspicion is confirmed by the fact that, when a person reports his/her infection in a place which is not identical to his/her place of residence or stay, the municipal health officer informs the municipal authority competent in the infected person's domicile, which, in turn, informs the patient's family physician. This could not be done without knowledge of the personal identifiers, so we can conclude that the legal rule prescribes personalized registration.

In addition to the national list[35] which, in principle, features no personal identifiers, the data of persons with HIV are entered (and are to be entered under the legal rule) in the registers of the health care establishment, the municipal office of the Surgeon General's Office, the county office of the Surgeon General's Office and the family physician. None of the supposedly ineluctable registers are necessary for the fight against HIV. They have no influence on its effectiveness but they are

34 Ministry of Welfare Decree 18/1998. (VI.3.) on the Epidemiological Measures Required for Preventing Infectious Diseases and Epidemics.

35 Data are reported on forms which feature questions about personal data. They do not have to be filled in – according to Paragraph 4, Section (2) of Ministry of Welfare Decree 63/1997. (XII.21.) the form for reporting general infectious diseases is to be applied "as appropriate", but this is nowhere indicated on the form. It would be reassuring if the form featured only questions which have to be answered to.

injurious to the right of persons with HIV to informational self-determination and enhance the likelihood of abuses.

The question of reporting infectious diseases (including, under valid laws, HIV/AIDS) in conjunction with personal data has been examined by the Data Protection Commissioner. In his report for the year 2001 he stated that "with reference to the principle of aim dependence and the conditions of data transmission the Commissioner did not think the county offices of the Surgeon General's Office had a well-founded claim for data, which concerned a certain group of patients"[36]. Section ad) of Paragraph 3 of the Act on the Surgeon General's Office[37] speaks of "data related to state of health" in connection with the public welfare activity of the Office, thus the obligation to report infection can only extend over those data, and "there is no need to identify cases of infection uniquely" for the fulfillment of tasks defined in Paragraph 3, such as epidemiological analysis. In other words, the Commissioner for Data Protection found registers containing personal identifiers to impose unjustified restrictions of the right to informational self-determination. Despite this fact, the question of a need for appropriate modifications was not even raised at the legislative sessions held last fall.

3. THE DUTY TO WARN A THIRD PARTY

According to the main rule, information concerning one's HIV status may not legitimately be disclosed without the person's consent. However, cases may arise in which an HIV positive person's right to informational self-determination is

36 Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2001, p.90.
37 Act XL/1991.

counterbalanced by another person's interest in reliable information about a possible danger to his/her own health, and such situations cause physicians to face a serious dilemma of medical confidentiality.

3.1. INFORMING SEXUAL PARTNERS

Traditional and modern approaches to epidemiology diverge significantly on the question of attitude they dictate to the question of how the sexual partners of an HIV positive person are to be informed. While the 1988 Decree, conceived in the spirit of the traditional public health approach, straightforwardly imposes a duty on the person with HIV's physician to trace sexual partners, the participants in the Geneva consultation confine within strictly defined limits those cases in which physicians may have to inform sexual partners instead of, and without consent from, the HIV positive person. The following requirements were laid down in the *International Guidelines*[38]:

- the person with HIV must have received all the requisite advice and must have refused to achieve appropriate behavioral changes;
- the person with HIV has not agreed to notify his/her partner or has not agreed to others notifying them;
- there is a real risk of HIV transmission to the partners;
- the person with HIV has been given reasonable advance notice;
- the personal identity of the person with HIV should not, if possible, be disclosed to his/her sexual partners.

The obligation to submit to screening cannot, as has been

38 *International Guidelines* 3, Guideline 28, Section (g).

mentioned in connection with groups subject to mandatory screening, be of a general nature: compulsory screening can only be justified by real danger clearly threatening in a particular case. The rules of the abrogated old Decree did not live up to these standards, since under them the physician caring for the person with HIV was under a duty to identify the person's "endangered environment" with a view to medical examination, and the duty of tracing and screening the HIV infected person's sexual partners was incumbent upon the physician of the competent Venereal Disease Clinic. Persons thus "traced" were under a duty to submit to screening and could even be enforced by official measures.

Under the Health Care Act and the new ministerial decree the sexual partners of a person with HIV no longer fall within the groups of persons subject to mandatory testing. The emphasis has shifted to appropriate information being provided for the person with HIV and experience shows that the new arrangement usually motivates people with HIV to inform their partners or ask their physician to do so. Both practices come closer to meeting requirements of the protection of confidentiality than the earlier system did. No longer undertaking to trace partners, the physician merely has an obligation to offer the HIV test to persons whom he/she knows to belong to the group "exposed to an enhanced degree of danger".[39]

The need to inform sexual partners has been raised as a possible justification for reporting with personal identifiers. A simple argument can show, however, that the HIV positive person's identifiers may remain undisclosed without endangering the aim of notifying sexual partners, even when

39 Paragraph 9 of the Ministry of Health, Social and Family Affairs Decree 18/2002. (XII.28.)

the person infected with HIV expects health authorities to do the notification: he/she can name his/her partners without mentioning his/her own name.

3.2. THE INTEREST OF OTHER PERSONS IN BEING NOTIFIED

Ever since the appearance of HIV a variety of persons and groups have expressed a need to be informed about persons in their environment who are HIV positive. Requests for data relating to HIV status may be made in two kinds of situation: before and after exposure (the risk of getting infected).

Arguments for information before exposure usually refer to the consideration that knowing someone to be HIV positive gives them a chance to take precautions in interacting with the person and the claim that such knowledge is essential to effective prevention. Thus these people feel that they "have a right to know" e.g. employees in penitentiary institutions, or employers and colleagues. Similar considerations have given rise to the claim that HIV positive patients should inform health service employees who get in contact with them of their HIV status even on the occasion of the most elementary health care services. It is generally held, however, that observance of the basic and universally accepted prescriptions of hygiene are a much more reliable method of avoiding infection. Besides not infringing the right of those concerned to informational self-determination, it has the advantage of avoiding a sense of seeming safety, as opposed to the method which envisages an enhanced degree of caution with respect to people with HIV, which disregards the fact that as a result of the unreliability of

the first test and the window period the circle of the HIV infected can never be delimited with hundred percent certainty.

Exposure tends to breed strong fear and despair and in such cases regularly gives rise to the strong conviction that the person potentially infected has the right to get to know the potential infector's HIV status. What has been argued with respect to persons suspected of having committed rape or known to have committed it, also holds in this connection: disclosing the HIV status of the source person can produce no undoubtedly positive advantage for the person potentially infected, and therefore the restriction of the source person's right to informational self-determination is not proportional to the aim sought (being inadequate to achieve it).

4. SUMMARY

Fundamental rights – including the right to informational self-determination and the right to privacy – may be restricted to achieve legitimate aims, but these restrictions are always to be in conformity with the standards of necessity and proportionality. The restriction employed to achieve the legitimate aim must be necessary (in the sense that the aim sought cannot be achieved by employing other measures less restrictive of the right) and the disadvantage caused must be proportional to the aim targeted.

In addition to education and general safety precautions built into people's conduct, knowledge of one's own HIV status is of equally prime importance for the prevention of the epidemic from spreading. Experience shows that this aim is best served under the arrangement of voluntary cooperation, and the model underlying this approach is guided by the principle of the

greatest possible respect for persons' human rights. We can thus conclude that the more a given body of regulations respects the fundamental rights of persons, the more effectively it contributes to the protection of public health interests.

As a positive improvement in the Hungarian regulations one must mention the fact that anonymous testing is possible again. On the negative side one must register the need for profound changes in the reporting of people with HIV and in the surveying methods. Despite its several unique features HIV/AIDS has still not been released from the chapter on infectious diseases of the Health Care Act, which is making it more difficult to devise appropriate regulations. The regulation of this problem area could become more effective and consistent if legislation adopted a separate act specifically geared to the problems of the virus causing the Acquired Immune Deficiency Syndrome and to the status of people with HIV.

ANOMALOUS PRACTICES IN THE HANDLING OF MEDICAL DATA IN EMPLOYMENT

András Schiffer

1. INTRODUCTION

Interestingly enough, the "omnipotent" total state collapsed and the rule of law emerged in Hungary at a time when techniques for mapping the complete personalities of innumerable individuals had undergone dramatic improvement. The need for freedom of action and self-determination was a natural concomitant of these changes for the citizen of disintegrating socialist régimes. The problems underlying the Constitutional Court decision on what came to be called the "personal identity number" (in 1991) showed that people's sense of the law had not yet incorporated the recognition that the question of their self-determination had a special dimension which was becoming more and more important with the progress of information society. We are free to determine the things others are allowed to know about us, and we have the right to be equally equipped with information as those we contract with and those that make decisions which affect our lives. That statement captures succinctly the content of the right to informational self-determination. If we lose our right to control data about our private lives, personalities, psychological and physical condition, if we do not know what organizations (public service institutions, employers, authorities) know about us, we become as vulnerable and exposed as the subjects of twentieth century dictatorships who were deprived of their freedom to act by their political system.

The political transformation happened in Hungary at a strange time in another sense also. Appealing continuously to "the working classes", state socialism had destroyed genuine interest representation for employees, but its mendacious legitimation ideology had also undermined the credibility of institutions of collective action. In this way, the citizens of the late Kádár era were entering the teething market economy with a legacy of socialization based on a lonesome search for individual survival strategies rather than on solidarity. This was the case at a historical moment when the need for effective interest protection was poignant, in view of the faltering system of social provision and burgeoning capitalism. The open infringement of legally protected employees' rights became virtually the fashionable thing to do in the Hungary of the early 1990s and the majority of those fighting for economic survival decided that it was wiser to keep silent about it.

The report submitted by the Data Protection Commissioner on the year 1997 drew attention to the fact that Hungarian employees' attention to, awareness of the danger inherent in, and willingness to act against, infringements of data protection laws, was much lower than in other areas, a fact which was underscored by the low number of complaints of this kind reaching the Commissioner's office.[1] Another fact one might see as symptomatic is the fact that no case in which employees' informational self-determination is at stake has so far reached the stage of effective court judgment.[2] "In assessing this phenomenon (…) we may assign some role to the greater dependence of employees in the post-transformation period, the erosion of previous employees" rights (which had often degenerated into the merely formal), the worsened prospects for

1 Annual Report of the Parliamentary Commissioner for Data Protection, 1997, pp.93-94.
2 Katalin Vrannai, "Intim szféra" (The Private Sphere), in: *Figyelő,* 2003/2.

their enforcement, the phasing out of once effective interest representation at workplaces, and the spread of "classic capitalist employment relations", the Commissioner's Report said.[3]

The relevant guidelines of the Council of Europe make data handling by the employer conditional on the voluntary consent of the data subject, the free, explicit and informed manifestation of the data subject's wish to express his/her willingness to agree to the handling of his/her personal data. "The disproportionately grater power over information wielded by the employer creates a disadvantageous and unequal communication situation for the employee, while making this sector a critical area of the reality of informational liberties. This goes to show how the waning of the influence of the state as the prime data processor does not automatically lead to improvement in the data subject's position. It's role is partly taken over by the monopolies of the private sector, which, in turn, introduce new forms of inequality."[4] This is why László Majtényi, the first Parliamentary Commissioner for Data Protection spoke of gross negligence with reference to the insufficient attention paid by legislation to this area of data protection.[5]

The handling of medical data in employment is a sensitive area in three ways. Firstly, it is obvious that information on someone's psychological or physical condition typically belongs to our most personal secrets. Secondly, employment and medical treatment are the two situations in which data subjects find themselves in the most vulnerable position. Thirdly, it is a sensitive area because in some cases the handling of medical data by the employer is justified by considerations of the employee's safety or some other legitimate interest, which gives the legislator a very delicate task.

3 Data Protection Commissioner's Report, 1997, p.94
4 Ibid.
5 Op.cit.p.93.

2. A SURVEY OF THE HUNGARIAN LEGISLATION

If we want to trace the ramified connections of medical data in the sphere of employment we have to survey a multi-layered corpus of legal rules which run through several branches of law.

The sectorial law on the processing of medical data is the Act on the Handling and Protection of Health Information and Related Personal Data.[6] Article 3 a) of the Act on the Protection of Medical Data defines the legitimate routes of data disclosure. Article 4 (2) n) defines the goal of ascertaining ability to work as a legitimate aim of data handling. The Act on the Protection of Medical Data itself is a "hybride" legal instrument. To apply it appropriately, one has to know both the skeleton Data Protection Act[7] and the special Health Care Act.[8] Information relating to state of health is mentioned among the special data in the Data Protection Act. Article 24 of the Health Care Act sets out the main principles of the right to access to medical records, article (12) making reference to the Act on the Protection of Medical Data. Of equal relevance to out topic are the parts of Articles 53-55 of the Health Care Act on the main rules of health care at workplaces.

The Labor Code[9] is the most important source of labor law, which lays down the rights of employees in the competitive sphere. The Act on Public Servants[10] has the Labor Code as its subsidiary background. The Act on Civil Servants[11], the Acts on the Terms of Service of Members of the Armed Forces, of the Legal Status of Judges and Attorneys invoke the rules of the

6 Act XLVII/1997, henceforward Act on the Protection of Medical Data
7 Act LXII. of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest, henceforward Data Protection Act.
8 Act CLIV/ 1997 on Health Care, henceforward Health Care Act.
9 Act XXII/ 1992, henceforward Labor Code.
10 Act XXXII/ 1992 on the Legal Status of Public Servants, henceforward Act on Public Servants.
11 Act XXIII/ 1992 on the Legal Status of Civil Servants, henceforward Act on Civil Servants.

Labor Code at particular points. Work safety law is closely related to labor law. Its rules are set out in the Work Safety Act, which is a code neutral between various spheres of law.[12]

Based on the powers conferred by the above-mentioned acts there are decrees – also neutral between sectors – which define the ways in which medical data related to employment are to be recorded. Public Welfare Ministry Decree 33/1998. (VI.24) gives general guidance on medical examination and the reporting of ability for jobs. Rules for the vocational health care service are set out in Ministry of Welfare Decree 27/1995. (VII.25). The examination of carcinogenous substances is regulated in Health Care Ministry Decree 26/2000. (IX.30.), rules relating to the chemical safety of workplaces in Decree 25/2000.(IX.30), jointly issued by the Health Care Ministry and the Ministry of Social Affairs and the Family. Rules for vocational aptitude examinations are set out in a ramifying body of legal instruments mainly issued by the relevant Ministries. In the present study we will be examining lower level legal instruments for public servants, judges, members of the armed forces, inspectors of public places, railwaymen and sailors. It is important to note that there are no legal rules on aptitude and health care specially designed for these vocations, so the situation of employees in these careers will have to be examined on the basis of the general legal rules mentioned above.

Data processing at workplaces is affected by social security law. The government acts on social security services[13], health insurance[14] and the medical procedure for judging loss of earning capacity and its supervision[15] deserve special notice in this connection.

12 Act XCIII/ 1993 on Work Safety, henceforward Act on Work Safety.
13 Act LXXX/1997 on those Entitled to Receive Social Security Provision and Private Pensions and the Funding of these Services.
14 Act LXXXIII/1997 on the Services Available Under Obligatory Health Insurance.
15 Government Decree 102/1995 (VIII.25).

As far as an examination of the actual observance of the right to informational self-determination in particular areas of law is concerned, it is best to examine it in terms of the legality and constitutionality of recording, processing and disclosing the data and the right of the person concerned to have access to his/her own records.

In this paper we will not be looking into the processing of medical data in the areas of higher education, vocational training and penitential establishments. At the same time, employment is not excluded from the various areas of vocational training and aptitude examinations are conducted in the course of these training courses. As far as employment in penitential facilities is concerned, it is regulated by a number of special vocational health care rules additional to the general provisions.[16] The reason why I do not find it expedient to discuss these areas in the present paper lies in the different nature of the underlying legal relationship here, which is not typically one of employment. Similarly, the legal material relating to the employment of those with a reduced ability to work raises special problems.

3. THE GAPS

I will try to unravel the disturbances affecting the handling of medical data in the world of employment arranged under eleven headings, from legislation to job-seeking and the termination of employment, without laying a claim to completeness and – unfortunately – without a body of "precedent law" related to the topic.

16 Ministry of Justice Decree 2/1999 (II.11.) on the Rules for Safe Work Without a Health Hazard at Penitentiary Establishments and on the Health Care Service in these

3.1. THE LEGISLATIVE OUTLOOK

It is a revealing fact about the legislative outlook that while the Act on the Terms of Service for Professional Members of the Armed Forces[17] devotes a special chapter to the restrictions imposed on fundamental rights[18], the right to informational self-determination is not even mentioned in the document despite the fact that this fundamental right is restricted not only in the area of health care during the time of the service relationship. Complete neglect of informational self-determination is not exclusively a Hungarian "phenomenon". Becoming effective almost simultaneously with the Act on the Armed Forces, the government decree which promulgated the International Convention on the Training and Certification of Sailors[19] prescribes the following for sailing companies: "Documents and data on the sailors employed on their ships are to be up-to-date and accessible; they are to include, without any restriction, (…) documents and data on their physical and mental aptitude." The decree says nothing about the circumstances under which these data can be accessed, or the persons or institutions who are supposed to have a right to access them.

In sum, one can safely conclude that the fact that the entry of every officer entitled to handle these data brings with it further restriction of the informational right of the data subject remains completely unrecognized in the Hungarian body of relevant legal materials.

17 Act XLIII/1996 (henceforward Act on the Armed Forces)
18 Chapter III.
19 Government Decree 119/1997(VII.25.)

3.2. THE REQUIREMENT OF BEING PROVIDED IN POSITIVE LAW

Paragraph 3 of the Data Protection Act sets out, in conformity with the Constitution, that any operation performed on personal data is to be made conditional on the provisions of an Act (or a decree issued by a municipal authority empowered by an Act). This being so, it is open to constitutional criticism that the fundamental principles of vocational aptitude examinations are enunciated at the level of decrees rather than, as they should have been, in rules of the Labor Code on terms of employment. Paragraph 7, Section (3) of the Act on Public Servants goes as far as relegating to the level of lower-order legal instruments and employees' discretion the right to make decisions on the necessity, or otherwise, and the exact extent of a health care and mental aptitude test before concluding an employment contract for public servants. In a case examined by the Data Protection Commissioner[20] it came to light that public servants at the Ministry of Education are submitted to an aptitude test in conformity with its regulations on public service with reference to Paragraph 3, Section (1) of Public Welfare Ministry Decree 33/1998 (VI.24.). The aims, directions and extent of examining health, physical and mental aptitude – i.e. of the restriction of the prospective employee's right – are not defined even by the Act on the Legal Status of Judges[21], despite the fact that a provision such as the one in question can hardly be considered a rule for the regulation of particular details. In addition one looks in vain in Decree 1/1999 (I.18.) issued jointly by the Ministry of Justice and the Ministry of Health for guidelines for its implementation, failing as the Act does to tell us the exact aspects of state of health, and

20 File number 759/A/2000.
21 Act LXVII/ 1997.

the physical and mental abilities which are supposed to be identified in a prospective judge. Decree 14/1985 (XI.30.) issued by the Ministry of Transport on the medical examination and certification of the aptitude of prospective employees in the railway service prescribes for the employers that all details relevant to aptitude should be passed on to the company physician.

3.3. DATA ON MENTAL CONDITION AS OPPOSED TO DATA ON STATE OF HEALTH

Examinations of vocational aptitude often extend to details about mental aspects of the prospective employee's state. Someone who is unwilling to submit to a thorough psychological examination cannot even aspire to the job of manager's assistant in many companies, but a test designed for testing the professional aptitude of physicians also includes a test of psychological aptitude.[22] However, Item p) of Paragraph 3 of the Health Care Act, which defines the notion of medical data, does not include information relating to someone's mental condition, while Paragraph 55 does not instruct vocational health services to conduct examinations of this kind. Item a) Paragraph 3 of the Act on the Protection of Medical Data at the same time includes "information relating to a person's intellectual and psychological state" in the purview of medical data. The different conceptions of "medical data" enunciated in the two highly relevant Acts – namely the fact that information about a person's psychological condition and intellectual faculties are included within the notion in the Act on the Protection of Medical data and are not included in the Act on Health Care – are at least disturbing. In

22 "A Sane Personality as a Condition of Employment". In: *Népszabadság,* Nov.30., 2001.

view of Paragraph 55 of the Health Care Act, it is rather doubtful whether vocational health care services are entitled to possess data which do not qualify as health-related under the Health Care Act. If a test sheet contains both data which qualify as health-related under the Health Care Act and data relating to intellectual and psychological condition, the latter kind of questions should, in principle, be covered so as to prevent the company physician from seeing them, as he/she is not entitled to handle this kind of data by the governing legal provisions which define the scope of his/her activity. The situation is made more sophisticated by the fact that the Data Protection Act lists data on state of health and addictions as well as on sexual habits among special data and that in this way most of the data of "psychological" relevance qualify simply as personal.[23]

The anomalies which haunt the range of information included within the purview of the handling of medical data extend to the body of lower-order legal instruments. Virtually the skeleton law on vocational aptitude tests, Paragraph 3, Section (6) of Ministry of Welfare Decree 33/1998 (VI.24.) categorically excludes from examination particulars relating to intellectual abilities and mental condition. Ministry of Welfare Decree 27/1995 (VII.25.) describes the medical service as offering, among others, services of a psychological kind. It is even described as having to attend to the task of examining intellectual and mental stress, a healthy condition of the intellect and the mental state. This decree thus comes in contradiction not only with the Health Care Act but also with Decree 33/2998. (VI.24.). It was an exciting symptom of legislative anarchy when a short-lived ministerial decree prescribed mandatory psychiatric examinations for family physicians above sixty-two years of age.[24]

23 Paragraph 2, Item 2 of the Data Protection Act,
24 Ibid.

Psychiatric aptitude surfaced as of equal rank among the requirements of health aptitude for public servants. The decree on the career aptitude of judges conflates information that can be gleaned from psychological examination with the notion of health care data, while the decree on the vocational aptitude examination of railway company employees conflates the examination of health aptitude with that of psychological aptitude.

This inconsistency results in a situation in which the relevant declaration of patient rights, namely Paragraph 24 of the Health Care Act cannot be invoked to back a claim for access to the "psychological data". Paragraph 15 of Decree 78/1999. (XII.29.) jointly issued by the Health Ministry and the Ministry of the Interior, setting out the aptitude requirements on public place inspectors does provide for the handling of health documents, but it remains to be seen how far this rule can extend to documents containing information of a psychological kind.

An officer of the Revenue Office filed a complaint with the Data Protection Commissioner in 1998 in connection with the matter of an internal decree issued by the president of the Revenue Office for a "focused personality examination" of leading public officers employed at the Office, in collaboration with a counseling firm external to the Office. In his recommendation[25] the Data Protection Commissioner referred to Paragraph 61 of the Act on Public Service according to which data are prohibited from being handled in areas not named in Appendix 3.to the same Act (Basic Register for Public Service) – and a "focused personality examination" counts as such data handling. (Let me note, incidentally, that the Act on Public Service is itself rather contradictory: Paragraph 7, for instance, points in the opposite direction.) Data from "external" sources are not to be used for the

25 File-number 95/A/1998. Annual Report of the Parliamentary Commissioner for Data Protection 1998, p.236.

purpose of grading public servants in terms of qualification. The recommendation prescribed that personality testing should be conducted on a perfectly voluntary and anonymous basis, and thus the president of the Revenue Office was not entitled to link the names of persons examined with the results.

In a great number of cases employers employ graphological tests "to get closer to" their employees' personalities. In a pertinent case[26] the Data Protection Commissioner explained that the employer, pending legal authorization, is not entitled to pass the employee's hand-written CV on to a graphologist for an opinion unless the data subject has been informed about this. According to the recommendation the employer is entitled to have access to the summary of the results (the aptitude assessment) even in such a case, since he/she is entitled to have access to the full assessment on condition that the employee consents to it.

3.4. JOB-SEEKING, APPLICATION FORMS

Long gone are the days when firms looking for employees would themselves list the positions waiting to be filled and applicant had only to call upon the personnel officer with his/her identity card and start work the following day. In Hungary, as in most other European countries, a growing market of Human Recruitment firms has forged itself a place in between employees and employers. HR firms employ a variety of testing methods to test prospective employees' verbal skills, risk-taking proclivities and expectable loyalty.[27]

26 File number 227/A1999. Annual Report of the Parliamentary Commissioner for Data Protection 1999, p.247.

27 "A Sane Personality as a Condition of Employment", in: *Népszabadság,* Nov.30.

It is standard practice for these "head hunting firms" to arrange applicant's files in "out-packages" and to offer them to well-paying clients who are looking for human resources. It is up to the head hunter's competence to decide how many firm directors he/she will send the personality profiles to and which ones.

Unfortunately effective legislation does not keep pace with the differentiation that goes on on the HR market. The single norm[28] contained in the Labor Code prescribes that declarations made by applicants, or information forms filled in by applicants or aptitude tests conducted with applicants, are to meet the condition that they do not infringe the applicant's personality rights and are suitable for providing information relevant to the employment relationship. The fact that not only prospective employers but also head hunters are allowed to ask for data and that thus the regulation is valid for head hunters is not contained in the Act, only in the commentary.[29] Pertinent to employment agencies, item e) in Section (1) of Paragraph 10 in Government Decree 118/2001 (VI.30.) appears to provide us with a reassuring prohibition against the recording and using of personal data which are not necessary for assessing applicants' aptitude and have no connection with the kind of work sought. What the decree ignores is the fact that the abstract sketch of the kind of work sought by the applicant and the data requisite for the position to be filled, provided by the client, do not necessarily coincide. In addition, the decree contains no explicit rules on the communication of data or the time limit for data processing. Rather than fulfilling the traditional role of employment agencies, head hunting firms often mediate as advisers by "screening" or "filtering" applicants for a certain employer.

28 Paragraph 77.

29 Commentary to Paragraph 77 of the Labor Code. In: dr Anikó Bárány, Commentary on Act XXII. Of 1992 on the Labor Code, in: *Complex CD Collection of Legal Instruments,* KJK-Kerszöv.

Applicants for jobs at a chain of hypermarkets had to perform a number of tests including ones in which they had to choose from among a number of wild and domesticated animals, geometrical figures, mythological characters and characters from fairy tales the ones they liked and had to give reasons for their choices. Their results were sent to the parent company abroad to be assessed by a psychologist who undertook to make not only yes-no decisions but also comments such as that so and so "was not honest". Ferenc Zombor, an associate to the Data Protection Commissioner pointed out that despite the written consent given by the applicants, their consent had not been voluntary and informed consent because they had not been informed in advance about the kinds of standards along which their results were going to be interpreted and assessed and the kind of person who was supposed to do the job.[30] By contrast, applicants at Budapest Bank Ltd. are always given full information in advance and their consent is requested not only for the questionnaire examination but also for examinations conducted with the participation of a company other than the Bank. As far as employees are concerned, questionnaires are used only for the purposes of career development, on the basis of prior consent.[31]

A serious shortcoming of Paragraph 77 of the Labor Code is its lack of a prescription for the situation where the "prospective employer" does not become an actual employer – this is another distinction made only in the commentary. In other words, there is no employment relationship but a body of data are still left with the "only prospective" employer. The rules on personality rights set out in the Civil Code and the provisions for the observance of

30 Katalin Vannai, op.cit.
31 Ibid.

rights contained in the Data Protection Act amount to a rather meager defense against this kind of dependent position arising.

Another problem is the outcome of the fact that on a literal interpretation of Paragraph 77 of the Labor Code aptitude tests are allowed to be conducted only with those involved in an admission procedure as opposed to employees already working for an employer. In view of the fact that the Labor Code does not authorize the employer to handle data during employment, the consent of the employee, i.e. of the dependent party, is requisite for such steps. As far as the possible aims and scope of data supply are concerned, we have again nothing but a flexible interpretation of the law to rely on, according to which the restrictions introduced by Paragraph 77 of the Labor Code are governing for the time following the conclusion of the contract of employment. A few companies use questionnaires with those already employed only for purposes of training and career development.[32]

With its many gaps, the regulation offered by the Labor Code itself provides an answer to the question why there is no court case with data handling in employment at stake. Finding themselves in a dependent position, employees are likely to be unwilling to undertake a lawsuit even if supported by labor law instruments, while it verges on the cynical to expect them to have comprehensive knowledge and a correct interpretation of the entire Hungarian legal system. The lack of strict regulations for data handling at work is a latent encouragement to the superior party, i.e. employers, and discourages employment supervision from examining the area.

32 ibid.

3.5. POINTLESS EXAMINATIONS, UNNECESSARY DATA AND UNREASONABLE CONDITIONS

In areas where there are special regulations for aptitude, the concept of aptitude is left undefined (or is defined in all too general terms). The more sketchy and undifferentiated the definition of aptitude, the greater the room left for aptitude examinations and the more inevitably the right to informational self-determination suffers unjustified restriction. Without a previously defined goal it is difficult to make examiners accountable for keeping within the bounds set by the aim, and the same holds for the requirement that examinations should remain within the limits of what is laid down in law.

The body of legal instruments relating to judges fails to even circumscribe the "health-related reasons which exclude or affect aptitude for discharging the professional duties of a judge". There are no guidelines for examining intelligence or character traits. It is not clear when and on what ground the expert committee may legitimately deem someone inept, and this also undermines the function of supervision. As a result, the Act on the Legal Status of Judges and the decree impose disproportionate and loosely extensive restrictions on the right to informational self-determination. As regards the professional members of the armed forces, the qualification forms provided in appendices 4 and 5 to the Act on the Armed Forces give no guidelines for the aims and scope of the examinations. For instance, there are no clues as to the criteria along which a person's physique is to be ranked along a scale of 1 to 5. The criterion of aptitude is left tautologically vague in Ministry of Defense Decree 12/1997. (V.6.) which says "A person is psychologically fit if he or she lives up to the requirements of military service in terms of intellectual ability,

perceptual skills, personality traits and motivation for the career." The Act on Inspectors of Public Places[33] contains no provisions on standards of data handling. The legal instrument which regulates aptitude examinations for employees of the railway company at least obligates the employer to pass on detailed data necessary for decision-making on aptitude to the company physician.[34]

When based on no clearly defined aim and criteria, examinations tend to lead to the recording of health-related information which is not closely related to the kind of work in question, and even psychological examinations based on clearly identified tests tend to disclose sensitive information which is nonetheless irrelevant to the job in question (most legal instruments resting content with the formula "testing psychological aptitude"). A glaring example is delivered by the aptitude test for judges: the Rorschach test identified in the Decree is bound to reveal psychological information which is unrelated to the career of a judge. The questionnaires for applicants for security training at secondary schools and for training as police officers include questions such as "Have you ever consumed a drug?", and "Have you ever been treated for (…) the following diseases (…) attempted suicide?".[35] (HIV infection is recorded with applicants for a military career). A few years ago, the Data Protection Commissioner gave an opinion on an aptitude test for insurance agents which was effective in revealing not only the applicant's aptitude for the job but also facts about addiction and sexual orientation, and the employer insisted on seeing the entire results. The Commissioner stated that the applicant had to be informed

33 Act LXIII/1999 on the Inspectors of Public Places.

34 Paragraph 7 of Ministry of Transport Decree 14/1985 (XI.30.) on the Medical Examination and Assessment of Aptitude for Employees of the Railway Company.

35 Appendices 2-3 to Decree 21/2000 (VIII.23.) jointly issued by the Ministry of the Interior, the Ministry of Justice and a Minister without Portfolio.

about the kinds of details the test was likely to reveal and had to be asked for consent in possession of all this information. The results were to be shown to the applicant and passed on to the employer on condition of consent given by the applicant.[36]

Inquisitiveness is a general feature of legal instruments related to the particular professions. Health records relating to the applicant's or employee's entire past life can be subjected to examination. The Decree on the aptitudes required of inspectors of public places[37] simply declares that applicants are "to present all other records relating to their health" at the health aptitude examination.

A complaint which came before the Data Protection Commissioner concerned the practices followed at the Revenue Office in the course of aptitude testing. Applicants had to bring a certificate from their family physician which was to provide a detailed history of their diseases, hospital treatment, and the number of days spent off work for health reasons over the previous year. The Commissioner declared the practice unlawful and stated "this country has recently seen an increasing tendency on the part of employers to adopt the policy of trying to map not only applicants' skills and personality characteristics but also their state of health – even at the cost of breaking the law and exploiting the applicant's unequal position – as thoroughly as possible so as to make the best possible choice from the most suitable carriers of human resource".[38]

The examples dawn from the Data Protection Commissioner's investigations show that the fault does not lie simply with specific legal instruments. Besides the general lack of a firmly established background of unquestioned value judgements concerning

36 Katalin Vrannai, op.cit.

37 Item d), Paragraph 4, Decree 78/1999. (XII.29.) jointly issued by the Ministry of Health and the Ministry of the Interior.

38 File number 689/A 1998. The Data Protection Commissioner's Report 1998, p.75.

matters of data protection, there are also anomalies in legal norms governing for the labor market in its entirety. It took the joint efforts of both the first and the second Data Protection Commissioner[39] to press the Ministry of Health into supplementing Section (1), Paragraph 14 of Ministry of Welfare Decree 33/1998.(VI.24.) as follows: "The physician assessing career aptitude conducts no examinations unnecessary for the assessment of career aptitude; he/she strikes out the relevant rubric on the form." In the petition that started the affair[40] ministry officials complained that their health and physical state had been examined "from top to toe" on the pretext of an aptitude examination, while even the taking of medical data by a physician without consent was a breach of the right to informational self-determination. Another example of a lack of precision is delivered by the decree which regulates standards of the estimation of chemical safety risks, failing as it does to prescribe that medical data taken for purposes of a scientific survey conducted on a justifiably broad sample should be anonymized. For this reason, Decree 25/2000.(IX.30.) jointly issued by the Ministry of Health and the Ministry of Social and Family Affairs comes to clash with the Act on Data Handling for Purposes of Scientific Research.[41]

The lack of regulation differentiated along jobs and degrees of disease seriousness (disablement, psychical disturbances) is another great shortcoming of the governing body of legal instruments. Characteristically, appointments to the position of secretary to a judge have to be based on an examination of the applicant as encompassing as that of an applicant for the position of a judge. The decree makes no allowance for a less extensive examination with judges who have been active for

39 László Majtényi and Attila Péterfalvi.
40 File number 759/A/2000. The Data Protection Commissioner's Report 2000, p.90.
41 Act CXLX/1995 on the Processing of Names and Addresses Recorded for Purposes of Scientific Research and Direct Mail.

some time and have lived up to the aptitude test several times. The legal instrument prescribing details of the aptitude examination for sailors makes no distinction in terms of different jobs. It is almost beyond human comprehension why a university student signing a study support contract with the national railway company is supposed to submit to an aptitude examination prior to signing the contract.[42]

Aimless examinations, unnecessary recording of medical data and undifferentiated underlying standards naturally lead to the imposition of unreasonable and humiliating conditions on applicants and employees. A report to the general Commissioner complained about the admission procedure followed at the János Apáczai Csere Teacher Training College for the reason that the college made application conditional upon a prior medical certificate indicating health status with respect to a number of health problems including "disorders of dermatogenic organs", "acute asthma" and "TB" as absolute preconditions of admission.[43]

All-encompassing, total examinations may easily lead to cases in which e.g. a young applicant for a clerical job at an office at the armed forces is disqualified on account of his/her inborn vertebral disorder. The differences between the requirements on the driver of a tank and between an analyst of defense policies are – or should be – glaringly obvious. The decree which sets out the aptitude requirements for inspectors of public places defines depression and paranoia as reasons for exclusion – irrespective of the seriousness of the condition – while listing all personality disturbances along with the euphemistically indicated "immune deficiency conditions" as a health-related reason for exclusion. It is rather doubtful

42 Paragraph 2, Section 1, Item c) of Ministry of Transport Decree 14/1985.(XI.30.).
43 OBH 3941/1997. Report on the Activities of the Parliamentary Commissioner for Civil Rights and his General Deputy for the Year 1998, p.178.

whether the legislator can come up with a satisfactory answer to the question why it is excluded in principle that an inspector of public places suffering from an auto-immune disease or HIV-infection should be incapable of performing his/her job and so identify the legitimate aim which is served by recording these kinds of data with applicants for jobs of the kind in question.

In 2001 a physician with HCV turned to the Data Protection Commissioner with the complaint that he had been dismissed from his job as surgeon for burns at a hospital department.[44] A number of other HCV-positive persons have been dismissed from health care establishments as a result of an epidemiological decree which is still effective. What gives the story a peculiar twist is the fact that the most competent forum, the Professional College of Infectology stated: "HCV screening of health care employees has no epidemiological significance, so it is not justified. Being rather expensive, screening is not recommended (...) HCV infections contracted during health care provision pose a hazard to employees, not to patients."[45]

3.6. DISCRIMINATION

As can be expected, the first to suffer from total control and unreasonable requirements are members of the underprivileged social classes. The decree on the medical examination of career aptitude lists the homeless, immigrants and those who have grown up in foster care homes, as "employees exposed to psychosocial pathogenic factors"[46] and orders that "employees

44 OBH 3941/1997. Report on the Activities of the Commissioner of Civil Rights and His General Deputy for the Year 1998, p.178.
45 Professional Statement, in: *Magyar Orvos,* February 2001.
46 Supplement 6. To Ministry of Welfare Decree 33/1998.(VI.24.).

exposed to psychosocial pathogenic factors" are to be examined for aptitude more frequently – every year. As "the psychosocial pathogenic factor" is described as an "exposure" in the decree, the employer of the homeless person or of a person brought up in a state home may initiate an aptitude examination at any time.[47]

The fact that the supplement to Decree 1/1999. (I.18.) jointly issued by the Ministry of Justice and Ministry of Health prescribes "psychomotor examinations of locomotion organs" under the title of a "general physical examination" as part of the aptitude examination for judges, one may rightly suspect that someone with a locomotion disability can be excluded from the career of a judge in Hungary today.

3.7. VULNERABILITY AND LEGAL REMEDIES

The presently valid regulation for extraordinary aptitude examinations is a hotbed for abuses by employers even if the employee is not one of the underprivileged social classes. The employer is entitled to initiate an out of turn aptitude examination "after unusual exposure" and if "the employee suffers exposure as a result of unexpected events".[48] Psychosocial pathogenic factors are also included in the notion of exposure. The relevant legal rule includes in the definition of "psychosocial pathogenic factors" such "lasting social risk situations" as e.g. "conflict with a colleague or senior official at the workplace".[49]

In 2001 the Data Protection Commissioner received a complaint[50] about a case in which the complainant's husband,

47 Paragraphs 1 and 7 of Ministry of Welfare Decree 33/1998.(VI.24.)
48 Paragraph 7, Section (1), Items c) and f) of Ministry of Welfare Decree 33/1998.(VI.24.).
49 Paragraph 1, Items h) and i) of Ministry of Welfare Decree 33/1998.(VI.24.).
50 File number 673/A/2001.

who was working with cerebro-vascular problems, had been submitted to an extraordinary aptitude examination. The complainant submitted that the company physician had given the employer "exhaustive" information and had thus exposed her husband, who was able to perform his job as scientific research associate despite his partial loss of speech, to the prospect of losing his job. Cerebral hemorrhage, the deterioration of speech ability, unless it involves a deterioration of intellectual ability, is a poor reason for exposing a senior scientific research associate to compulsory retirement, which is bound to deepen his depression. The Data Protection Commissioner finally stated that an extraordinary examination of career aptitude does not entitle the company physician to provide the employer with "detailed medical information".

It is unclear in most career areas how much information is likely to land on the employer's desk and when, after an examination of aptitude. The basic information form defined by Supplement 3 to the Decree on the Aptitude Examination of Inspectors of Public Places includes everything from family anamnesis to sporting habits. In courts the employer is provided a summary opinion even in cases which end with "positive" results for the employee or the applicant (not just a notice of "apt" or "passed"), while with negative results, it is obligatory to give reasons for the decision.

In all areas of employment supervision of the aptitude examination results is a possibility. Where there is no special legal instrument for career aptitude, the possibility of legal remedies is offered by a Ministry of Welfare Decree.[51] Despite the opportunity for supervision, the assessment questioned lands with the employer before it reaches the supervisory decision-making stage.

51 Paragraph 12 of Decree 33/1998.(VI.24.)

No vocational health care related legal rule is an exception to this generalization. Accompanied by a justification, the expert opinion submitted to the employer appears to be impeccable. In reality, however, the complete health-related and psychological results can be imparted to the employer as a message coded in the justification. One rarely finds an unambiguous restriction in a legal instrument to the effect that assessments sent to employers are to be restricted to "fit/unfit" or an indication of degrees of aptitude.

In many ways, examinations of aptitude – and subsequent supervision – are like the administrative procedure: they start with an authorization by a legal rule, private organizations appointed by authorities, in some cases state authorities, proceed against the employee; it affects the rights and legally acknowledged interests of the employee, and may occasionally lead to the termination of the legal relationship against the will of the parties involved, the employee is obligated to take part, and its dynamics is similar to that of supervision by expert authorities. The terse wording of the rules and the lack of any reference to the state administrative procedure[52] deprives the employee of rights established in ordinary official proceedings which would be able to counterbalance the "inequality of arms". To take an example, the employee's right to possess deeds and documents (see further below) is left absolutely contingent. With no "equality of arms", and a considerable deficit of information a procedure such as the one in question is directly injurious to the employee's human dignity, and supervision has no real function of its own. Hungarian legislation continues to owe us a definition of the place of health-related procedures in the context of employment relations within the legal system, and as long as this debt is not discharged, it is the employees that are bound to suffer.

52 Act IV/1957. on the General Rules of the Administrative Procedure.

The institutions which assume a role in the examination of aptitude – as I have just argued – are quasi-administrative institutions. Therefore even questions of data protection aside, it is cause for constitutional concern that second-order assessments are not subject to possible court supervision. This possibility is absent from the Act on the Legal Status of Judges, too, despite the fact that disciplinary cases involving judges are handled by a special forum of judges. There are no arrangements for remedies to be sought by judges with respect to second-order medical assessments of incapacity for earning which belong to the discretion of the National Medical Expert Institution of the National Health Insurance Savings Bank.[53]

3.8. QUESTIONABLE LINKS BETWEEN DATA PROCESSORS

The complainant in the case of the scientific research assistant suffering from a cerebro-vascular problem also complained about the fact that the employee and the company physician who was examining him were employed by the same employer.[54] Although the Commissioner's statement does not respond to this aspect of the matter, it is disconcerting that there is no guarantee for the independence of physicians who conduct aptitude examinations from employer institutions. It is an important requirement that assessment should be free of bias, if only because of the weight of the possible future consequences of the decision: an unfavorable assessment can not only endanger the position of the person examined vis-á-vis his/her present employer, but may also put an end to his/her future in employment (see pensioning off for disablement, the

53 Government Decree 102/1995.(VIII.25.).
54 File number 673/A/2001.

rules governing for judges, sailors and railway company employees etc.). The legal instrument valid for employees of the Hungarian State Railway Company provides that the health examination is to be conducted by the company physician.[55]

Conditions for unbiased assessment are not much improved when vocational health care services are delivered by a private health care agency on the basis of a contract with the company. These medical firms derive most of their annual income from large companies, so their independence is questionable. No clear answer has so far been given to the question why the employee should not have the required examinations conducted by a physician of his/her own choice and why it should be an unfair arrangement that the employer should be entitled to request supervision in case of doubt.

The present situation is in many cases the exact opposite of the above. Employers and vocational health care services cooperating with them often approach family physicians or psychiatric caretakers for data – for reasons of cost–effectiveness. Unfortunately such requests are seldom turned down. In one of the rare cases in which they were turned down, the family physician contacted the Data Protection Commissioner.[56] What happened was that the vocational health care service of Borsod-Abaúj county had ordered that family physicians would be under an obligation to provide information about employees' state of health by filling in an information sheet.

It would also be reassuring if the decree on the medical adjudication and supervision of incapacity and capacity for earning[57] featured an express prohibition on the transmission of data to the employer.

55 Paragraph 9, Ministry of Transport Decree 14/1985.(XI.30.).
56 File number 519/A/2001.
57 Government Decree 102/1995. (VIII.25.).

3.9. UNIDENTIFIED HANDLING OF DATA BY UNIDENTIFIED PERSONS

In the case of the HCV infected physician[58] the complainant criticized the fact that the epidemiological procedure gave a number of people an opportunity to get to know highly personal information about him. The story can be regarded as typical. In vain do we have the general data security rule[59] in the Act on Data Protection and in the Act on the Protection of Medical data if they are not translated even as guidelines into labor law. Ideally, labor law instruments should give straightforward prescriptions for employers concerning the range of things they have to do to keep the employee's health-related (or other) data confidential.

It makes the observance of data security requirements difficult that relevant legal instruments give poor guidance for identifying the exact person or class of persons who are supposed to be entitled to handle data under the authorization given. As a result it is left to chance or at best to the "data sensitivity" of the particular employer's Regulations for Service and Operation who will be informed about, say, a colleague's HCV infection. The situation is not better in areas where there is a specific legal instrument designed to settle the matter. The Decree on the aptitude examination of employees of the railway company authorizes the "Health Department of the General Directorate of Hungarian State Railways to act as a quasi authority and supervisor. One might wonder what will happen if the leading organ of Hungarian State Railways should decide one fine day that the company will no longer have a Department of Health? Decree

58 File number 512/A/2001.

59 Paragraph 10 of the Data Protection Act, Paragraph 6 of the Act on the Protection of Medical Data

21/2000 (VIII.23.) jointly issued by the Ministry of the Interior, the Ministry of Justice and a Cabinet Minister without a Portfolio play down the question of who exactly is to be authorized to handle data by saying that 'test results are to be sent to the "personnel department" which has requested the examination'.

Other aspects of the legitimacy of data handling at workplaces give equal cause for concern. I have mentioned the increasingly wide-spread – and in itself salutary – practice of major companies relegating recruitment tasks and traditional "human resource policy" tasks to other companies and career advisory agencies. This trend is salutary in itself. The trouble is that effective law takes no notice of it, and this results in the practice of the advisory firm assessing, without permission from the employer, employees' personality tests. Typically, the Decree on Inspectors of Public Places entrusts private organizations, who are appointed under rather enigmatic conditions, with the task of conducting the aptitude examinations. Without legal authorization, however, and without the subject's consent, private organizations are acting against the law in doing what they are doing[60].

There are leaks in the legitimacy of data handling as a result of the disorderly regulation of 'psychological' data. The company physician is not entitled to handle psychological information, under the above-mentioned passages of the Health Care Act, while the psychologist who cooperates in conducting psychological tests has no right of access to medical data. In the testing of judges the physician and the psychologist employed by the same institution are doing partly overlapping jobs. The general practice is that which we have found expressly stated in the Decree for Inspectors of Public Places: the results of the

60 Paragraph 11, Section (2) and Supplement 1 of Decree 78/1999. (XII.29.) jointly issued by the Ministry of Health and the Ministry of the Interior

psychological examination are edited into a summarized assessment by the physician.

3.10. TERMINATION OF EMPLOYMENT, WINDING UP OF EMPLOYERS

As a result of shortcomings in effective labor law there is often no legal guidance on what is to be done with the health-related documents stored by the employer when the employment is terminated. Responding to a complaint about a possible collision between Ministry of Welfare Decree 33/1998.(VII.24.) and the Act on the Protection of Medical Data[61], the Data Protection Commissioner held that the employer had to make an official certified copy of the data stored by the employer and that the ex-employee concerned was to receive an extract of the register sheet if his/her employment was terminated "(...) an authenticated copy (...) may be kept by the data processor who is under an obligation to hand over the original."

The Commissioner's opinion of a complaint made in the matter of public service was more consistent. "(...) the employer is obligated to hand over data without making and keeping a copy of documents with respect to which he will be under no duty to handle them, after the termination of the public service i.e. with respect to which the aim of data handling will no longer make sense. With respect to particular documents the employer is under a duty to provide information about the continued validity of the aim of data handling[62]. According to the Data Protection Act only such personal data may be handled as are absolutely necessary for achieving the aim, are suitable

61 File number 812/K/2000.
62 File number 538/A/1999.

for achieving the aim and even such may only be handled to the extent necessary for achieving the aim and only as long as necessary[63]. The aim may cease to apply for several reasons during employment, but it inevitably ceases to apply when the employee leaves the company[64]. The employer is therefore under a duty to erase the personal data of an employee leaving the firm, except data related to taxation and social security which it is obligatory to keep under the relevant legal instruments, and with respect to which the employer may be under a duty to communicate them to the revenue authorities or pension and health insurance establishments even after the termination of the employment relationship.

In the case of the termination of an "establishment not related to health care" (i.e. a business firm), the Act on the Protection of Medical Data orders that what is to be done with health-related documents should be determined according to the rules which are binding for the termination of health care establishments[65]. The fact that bankruptcy law, which regulates the termination of businesses without a legal successor, provides for the discarding sorting out and depositing in archives of the body of documents without specially mentioning health-related documents raises problems of both a practical and a legal dogmatic kind[66]. To that extent, the Bankruptcy Act and the Act on the Protection of Medical Data, which provides that documents are to be transmitted to the National Health Office, are in contradiction and we do not know how thoroughly the liquidator, proceeding according to the Bankruptcy Act, studies the rules in the Act on the Protection of Medical Data.

63 Paragraph 5 of the Data Protection Act,
64 Vrannai Katalin, p.cit.
65 Paragraph 33 of the Act on the Protection of Medical data,
66 Paragraph 53 of the Act II./1991. On the Bankruptcy Procedure, the Liquidation Procedure and the Final Settlement Procedure,

One solution would be to have the Bankruptcy Act incorporate a rule providing that health-related documents shall be handed over to the Surgeon General's Office.

It would be worth our while to dwell upon the typical case in which by legal succession under labor law an entire business branch (with their personnel) is taken over (or bought) by another, business organization independent of the original data processor. Both the rules for data protection and the rules of the Labor Code apply to such a case in the following manner: "the employer is entitled to disclose data, facts or assessments concerning employees to a third party under conditions strictly defined by law or with the employee's expressed consent only"[67]. Continued data handling by the party which hands the business over loses its aim, but the other party does not acquire a lawful authorization to do the same.

The Act on the Legal Status of Public Servants provides precise rules for legal succession in labor law in cases where the budgetary body confers the right of maintainer on another natural or corporate person or establishes an organization falling in the purview of the Labor Code or the Act on Public Servants with the same task[68]. Unfortunately in modifying the Act on the Legal Status of Public Servants the legislator omitted to make express provisions on the disclosure, or deletion, of the data of persons remaining employed.

67 Paragraph 3, Section (4) of the Labor Code
68 Paragraph 25/A., Paragraph 26 of the Act on Public Servant

3.11. THE RIGHT OF ACCESS

A comparison between the relevant provisions of the Act on the Protection o Medical Data[69] reveals that the act provides a right of access exclusively with respect to documents recorded for purposes of medical treatment, not with respect to documents relating to career aptitude. In this way an employee may refer to Paragraph 24 of the Health Care Act, as well as the Data Protection Act, in requesting inspection of the health-related section of his/her examination file. He/she is not entitled to have access to "psychological documents" by the Health Care Act.

Although Ministry of Welfare Decree 33/1998.(VI.24.) prescribes[70] that the applicant should be given an explanation for inaptitude, it says nothing about the right to get to know the documents resulting from the aptitude examination. Nor does the legal rule on the adjudication of incapacity for earning[71] entitle the insured to have access to his/her the medical documents.

One complainant contacted the Data Protection Commissioner because his request to get copies of the documents of his industrial accident had been rejected by his employer[72]. According to the Commissioner the records of an industrial accident are to be sent to the injured, and he/she is also to be informed about possible legal remedies. The employee is entitled to get to know the content of the accident records both with reference to his/her right under the procedure and to the right to the protection of personal data. In connection with the above-mentioned complaint made by a public servant[73], the Commissioner argued that a public

69 Paragraph 3-4, Paragraph 7 of the Act on the Protection of Medical Data
70 Paragraph 13, Section (5)
71 Government Decree 102/1995. (VIII.25.)
72 File number 465/A/1999.
73 File number 538/A/1999.

servant is entitled to have access to the data kept about him/her in the public servants' register at any time.

Data subjects are entitled to get to know all their personal data that are handled by their employer or their would-be employer. The employee has the right to know whether his/her handwriting will be passed on for examination to a graphologist, and if it has been passed on, what the opinion is, and are also entitled to request that the data be deleted[74].

4. SUMMARY

My aim was to present a small area, that of the processing of medical data in the sphere of employment as reflected in presently valid Hungarian law. By contrast, the conclusions we can reach point well beyond this narrowly defined area. They are as follows.

– The real effect of a constitutional right depends on a number of factors other than the quality of the enactment containing the constitutional right in question. To take an example, the relatively satisfactory regulation offered by the Data Protection Act, those applying the law in particular areas – such as employment, health care, education etc. – have to deal with a body of legal instruments which are insensitive to the requirements of data protection or are straightforwardly alien to its spirit.

– The legislator is able to provide effective safeguards for a civil liberty only if he incorporates special guarantees for the sectorial legal instruments which regulate the individual's unequal legal relationships (e.g. the employment relationship, the student-school staff relationship, other legal relations within institutions).

74 Katalin Vrannai, op.cit.

– The challenges leveled against our liberty are coming increasingly from market actors rather than the state. The legislator's task is to work out and maintain the delicate balance between the autonomy both of the individual and of the market.

– Labor force is increasingly becoming a market commodity like a car or an office block. It may no longer sound odd to say that employers "buying" employees from head hunting firms might soon be trying to assert warranty claims on account of "hidden psychological defects". And a commodity has no human dignity. Or has it?

THE HANDLING OF MEDICAL DATA IN PENITENTIAL INSTITUTIONS

Andrea Pelle

Inmates in penitential facilities are in a special situation in that they are not free. They do their daily activities according to a strictly defined order, their freedom of choice is limited even in minor matters. Their days roll by according to directives and disobedience leads to punishment. Their rights may be restricted with reference to the purpose and security of punishment, and the convicts are, to varying extent, exposed to the ways their guards may happen to behave toward them.

Medical data are sensitive data: if they are disclosed to persons unauthorized to possess them this may result in serious violations of the rights of those to which they relate. The reasons in support of strict regulations for the handling of medical data are set out in another study in this volume.[1] In what follows I will focus on the problem of the way the penitential system, an institution that is highly restrictive of constitutional rights, handles the particularly sensitive, health-related, data of criminal convicts.

The relatively compact body of legal instruments relating to the administration of punishment comprises no provisions expressly directed at the defense of medical data or to data handling by penitential institutions. It is one of the fundamental principles of penitential law that although during their time convicts lose their personal liberty, their constitutional rights and duties are intermitted or restricted only to the extent ordered by the verdict or valid law.[2] According to this Decree

1 See Márta Faur's article in this volume. *(The Editor.)*

2 Law-decree 11./1979. on the Execution of Punishments and Measures, Paragraph 32. (Henceforward: Decree on the Execution of Punishments'.)

convicts' right to assembly, or to strike are intermitted, and some of their rights undergo modifications in their content, such as their right to choose physicians. The legal rule expressly mentions the right to the protection of personal data in providing that convicts are entitled to their protection.[3] Discounting the reference to the controllability of correspondence and telephone conversations, no reference is made to the legitimacy of restricting informational self-determination.

Health care provision for convicts is regulated by special rules.[4] Convicts and persons in preliminary apprehension are to undergo an examination of health. This begins with an examination in public health and epidemiological terms, which is conducted by a qualified health care employee and is followed within seventy two hours after admission by an examination by the physician of the penitential establishment who records the data of their previous health history, mapping their general state of health and physical condition and ranking them in terms of capability for work. The convict or detainee is not in the position to refuse to submit to the examinations[5] and other members employed in the penitential facility's staff (including the guard[6]) may be present at it (and later examinations during detainment or imprisonment). This may be undeniably necessary in the interest of the security of imprisonment or detainment, and we must accept that the guard may then have access to certain medical data simply as a result of being present when they are recorded. There are no rules on a duty of confidentiality on the guard's part, however. During their detainment or imprisonment convicts or detainees may have to undergo several screening examinations. When admitted, they

3 Decree on the Execution of Punishments, Paragraph 2, Section (2) c).
4 Ministry of Justice Decree 5/1998. (III.6.) on the Health Care Provision for Convicts.
5 Act on Health Care Provision for Convicts, Paragraph 1, Section (3), Paragraph 4 Section (3) and Act on the Execution of Punishment Paragraph 33, Section (2) f).
6 Act XLVII./1997. on the Handling and Protection of Health Information and Related Personal Data, Paragraph 14, Section (1), c).

have to undergo HIV screening but are not then lung X-rayed or screened for Hepatitis.[7] Health care provision for convicts has to be conducted within the health care framework of penitential establishments, so convicts are taken to external civil health care establishments when the required health care intervention cannot be secured in any other way.[8] If a convict needs protracted medical care which cannot be rendered within the penitential institutional system, the execution of the imprisonment may be interrupted or postponed.

The Act on the Execution of Punishment contains no provisions which envisage more substantial restriction of the right of convicts to informational self-determination than would be possible under the normal circumstances of civil life. Interpreted together with other rules pertaining to health care provision for convicts however, they do amount to a limitation of this fundamental right, or at least interpretations which allow such restriction are near at hand.

The presence of the guard at the above-mentioned examinations certainly leads to the result that someone other than the physician gets to know the medical data of the person examined. The person concerned is not in the position to influence this transmission of data since he/she cannot refuse to cooperate in the medical examination so he/she reveals the data to the guard, whether either of them wish to tell or to be told, or not. At this point, then, the Act limits the right of convicts or detainees to the protection of personal data while giving no guarantees to counterbalance the limitation thus imposed. The guard of course is not entitled to pass information thus acquired on to anyone without a law prescribing just that, but he/she is not under a duty of confidentiality arising out of a legal rule such as the professional

7 Act on the Health Care Provision for Convicts, Paragraph 8.
8 Ibid, Paragraph 1, Sections (3)-(5).

duty of confidentiality with reference to which he/she is entitled to refuse to bear testimony . There are two persons involved in addition to the detainee or convict: the physician, who is under a duty of confidentiality, and the professional member of the professional staff of the penitential facility, who may be obligated to disclose what he/she has heard at the examination. It would be reasonable to change this situation by supplementing the relevant provisions of the Act on the Execution of Punishments to the effect that the guard present on such occasions should be under a duty of secrecy. Even if the duty of confidentiality is once anchored in a legal rule, efforts should be made to create and establish routines which minimize the chances of a guard being exposed to health-related information in such situations (e.g. to make arrangements such that the guard will not see the medical findings, the physician tells the person examined in a low voice, etc.). Besides lending greater effect to the right to the protection of personal data, such an arrangement would also promote greater cooperation on the part of the patient, since undoubtedly anyone (including a convict) is more likely to reveal medical data in a confidential environment.

Information about drug consumption is to be treated as data of special sensitivity, since this health problem may form the legal ground for additional criminal proceedings. According to the Criminal Code[9] the physician employed at a penitential establishment[10], if a member of the professionally employed staff, is an official person even when he is examining the convict's state of health. What is not clear is the extent to which he is obligated to report a suspicion of drug consumption, since

9 Act IV./1978. Paragraph 137, 1.i): a person of authority is a person in service at an institution of state administration whose activity is involved in the functioning of the institution for the purpose it is designed to serve.

10 According to Act CVII./1995 on the Organization of the Execution of Punishment a physician employed at a penitential establishment is a public servant.

he is also bound by the duty of medical confidentiality, and he is handling medical data. In addition, the legal rule on the service relationship in the execution of punishment allows for data related to drug consumption to be registered, and to be made available to prosecuting institutions. Although the relevant rules are in harmony with the Data Protection Act, when the request is made "for the purpose of some lawful task prescribed by law", it remains an open question whether penitential institutions are under a duty to report the fact of drug consumption when there have been no proceedings against the inmate.

If the convict's behavior during the medical examination in the course of admission reveals signs of possible drug consumption, further examination may be ordered.[11] The patient (convict) has the right to adequate medical care, but since the physician is mostly an official person, further criminal proceedings may be started against the convict on account of drug consumption. The same holds of drug consumption revealed in the course of a medical examination after admission. Whatever examinations are conducted in addition to the compulsory examination, it is important that the convict should have exclusive control over the data which result from them. It is desirable that this should be declared unambiguously in a legal rule.

One among the general provisions of the Act on the Execution of Punishments provides that, according to the provisions of another legal rule (obviously the Act on the Protection of Medical Data), the convict should be secured access to his/her medical data which are produced during imprisonment or detainment.[12] According to a rule earlier in the Decree the convict is to be given a copy of his/her final hospital bulletin when he/she is released as

11 According to the Act on the Execution of Punishment Paragraph 30 the treatment is to be carried out in the health care establishment of the penitential institution.

12 Act on the Execution of Punishment, Paragraph 4, Section (2).

well as copies of the medical findings which are essential for a correct assessment of his/her state of health, or such as he/she demands.[13] This provision may be interpreted to the effect that before release the convict is not entitled to receive copies of health documents, being entitled to exercise his/her right to being informed about his/her medical data when he/she is released. This cannot have been the legislative intention, yet the practice of penitential institutions reveals that this interpretation is widespread: the convict is not given these copies during his imprisonment. In the most recent example a convict at the penitential establishment in Tököl has recently been denied access to his data which resulted from the health care he had received in connection with his drug problem. He was told that in such matters his legal representative was to contact the penitential institution in writing. Regrettably enough, it has also happened that the legal representative's letter has not been answered. The Health Care Act in general secures the right to have access to medical files, and the provisions of a law cannot be overridden by a ministerial decree. The rule, then, is to be interpreted to the effect that the patient-convict has the right to have access to medical files according to the Health Care Act, but he/she is also to be asked at the time of release from the penitential institution which documents he/she wants a copy of, and copies requested must be available to him/her already during imprisonment.

The legal regulation of the handling of convicts' data is open to criticism in general. The Act on the Execution of Punishments, the fundamental legal document on the execution of punishments, contains no provisions on data handling. Rules for the registration of convicts can be found in Chapter V. of Act CVII./1995 on the Organization of the Execution of Punishment.

13 Act on the Execution of Punishments, Paragraph 35, Section (1).

These provisions regulate the content of the data in the registers, the disclosure of data from the registers and the right of data subjects to get to know their data, but, undoubtedly, penitential facilities handle a much broader range of personal data than those contained in the registers, including the medical data of the convicts. Legal rules on the execution of punishments fall behind modern expectations in many ways which are not discussed here. It is desirable that the Act should be replaced by a new one. As long as this is not done, specific guarantees for the protection of personal and special data could be provided in the form of modifications.

QUESTIONS RELATED TO DATA PROTECTION IN THE POLICE ACT

Balázs Dénes

1. DATA HANDLING CONNECTED WITH THE FULFILLMENT OF THE DUTY TO RENDER HELP

In cases involving the duty to render help police become data processors in the interest of the assertion of a third party's right rather than "in their own right". The classic case of the kind I am thinking of is the situation in which a ticket controller of the public transport company asks a police officer to help him/her in getting the data of a passenger who has failed to validate his/her ticket. Rules for such cases of data-handling are contained in Paragraph 24, Section (4) of the Police Act[1], which gives the following prescription: the person asking for help presents proof of his/her personal identity and provides a plausible reason to believe that he/she has a rightful interest in checking the person's identity. If after proving identity the person asking for another's identity gives reliable proof of his/her rightful entitlement to have the data available, police will pass on to him/her the data of the person whose identity has been checked. If he/she does not do so within eight days from the day of the identity check, the data have to be deleted. The person whose identity has been checked is to be informed of the disclosure of his/her data in writing and the reason given by the person claiming to have them must also be indicated. At the request of the person checked for identity police will also communicate the personal identifiers of the person claiming the

1 Act XXXIV/1994 on the Police, henceforward "Police Act".

former's data. These regulations offer an acceptable guarantee for the person whose identity is checked. One could conceivably raise the question that perhaps the request for the data by the person asking for the identity check should have to be made in writing, as the present regulations do not give any guidance on that score.

There is no doubt, however, that according to the Police Act the person asking for the identity check may only be provided with the data of the person checked for identity if he/she has given officially acceptable proof of a rightful title to the data within 8 days after the identity check. This rule is contradicted by Paragraph 32, Section (4) of Ministry of the Interior Decree 3/1995.(III.11.) on the Rules of Service of the Police: "If an identity check is asked for by a person fulfilling some public task within the legitimate scope of his/her legitimate activity, the data of the person checked for identity may be disclosed to him/her on the spot. As regards the data of the person asking for an identity check he/she may only give his/her name and workplace." In view of the hierarchy of legal instruments (law vs. ministerial decree) in this case the stricter rules laid down in the Act are to take precedence in application in every case even if the identity check is being asked for by a person performing a public task. One has reason to suspect however, that police officers on duty are following the prescriptions of the Rules of Service which provide weaker guarantees.

Another problem, also one to do with identity checks, is the following: while according to the Police Act the data of the person checked for identity may be legitimately stored only if there is a need for "recording the data for the prevention of a crime or offence"[2] the Rules of Service, which are couched in a different terminology, provide for the legitimacy of recording

2 Paragraph 84. item p) of the Police Act

data obtained in the course of an identity check when "they are necessary for further measures or procedures or are justified by further circumstances".[3] It is not acceptable that the lower-order legal instrument should give much broader justifying reasons for data recording than the law – "other circumstances" is open to a range of interpretations which is too broad.

2. MAKING PICTURES AND RECORDING SOUND

"(1)In the course of taking police measures Police may take pictures and make sound recordings of the person affected by the measures, the environment, details and objects of relevance to the measures taken. Police may set up photographic and video equipment in public places in the interest of public safety in such a manner that it is evident to citizens. The population are to be notified of the placement and operation of the photographic or video equipment. Pictures, video and audio recordings and the personal data thus recorded may only be used in the course of court proceedings started on account of some criminal act or misdemeanor committed on the particular spot or for identifying a person wanted by police.

(2) If no proceedings have been started on account of some criminal act or misdemeanor which has been recorded on the spot, and if the data recorded there carry no lasting value, the recordings have to be destroyed within six months from the date of the incident"[4].

According to the above regulations, rules relating to recordings made in the course of police measures and those relating to

3 Paragraph 12, Section (2) of Ministry of the Interior Decree 3/1995.(III.11.) on the Rules of Service of the Police

4 Paragraph 42, Section (1)-(2) of the Police Act

photographic recordings made by the public safety equipment are regulated in the same paragraph. The terminologies of the two passages quoted are also divergent to some extent. Section (1) speaks of "police measures" and recordings made in the course of police measures. Later in the same section video recorders installed in public places for public safety (which are a kind of space monitoring system) are mentioned. This is then followed – still in the same section – by another occurrence of the category of an "incident" (which is another reference to police action). The term "incident" is used again in Section (2), thus the rule admits, under several interpretative approaches, of the conclusion that rules for storing, using and destroying audio and video recordings apply in the same way to video or photographic recordings made in the course of police measures and made by recorders placed in public places.

It is not acceptable to regulate in the same way two significantly different kinds of recordings. In the first kind of case records are made in the course of actual police measures and there may be legitimate interests in the storing of the records taken. In one of the cases indicated in the law the recordings may be needed for use in the proceedings started in connection with a criminal act or misdemeanor, but it is perfectly conceivable that the recordings should be needed for a follow-up examination of the legality of police measures.

The case of recordings made by public safety recorders set up in public places is different. Anyone may be recorded on the tapes running in such equipment as a result of simply walking across or staying in the public area. In view of the declared aim of installing such equipment, namely to improve safety conditions in public places, these systems are run in an acceptable way if appropriately authorized police officers are monitoring the

pictures broadcast by these systems and take measures if they perceive any act of crime or misdemeanor. There may be a reason against instantly destroying the recordings as a matter of course but the six months of storage time may be too long. The six months are too long even in the case of recordings made of police measures. If the recordings are needed – because they record evidence of some crime, for instance – the six months' deadline does not apply to their destruction, so there is no reason for police to store unnecessary recordings as in some kind of "data base".

The expression "of lasting value" in Section (2) of the Paragraph quoted gives rise to another problem connected with audio and video recordings. The regulation being unified, this formulation again applies both to recordings made in the course of public surveillance and police measures. According to this, if the recordings have "lasting value", they may not be erased. This vague and broad formulation cannot be accepted, however. Who is entitled to decide what gives "lasting value" to a person or a detail recorded?

The way police may identify the wanted person mentioned in Section (1) while observing the constitutional norms relating to data protection is less than clear. In its present formulation the law is so broad that it would not prevent police from using the tapes recorded by public watching systems with a system for face recognition and examine the persons who appear in public places at certain times.

In view of the above it would be necessary to settle the regulation of using, storing and destroying photographic recordings made in the course of police measures and by watching systems set up in public places.

The legal instrument quoted also prescribes that recording systems installed in public places are to be placed in such a way

as to make their presence evident to citizens, and the inhabitants are to be informed about the placement and operation of public recorders. One might wonder as to the extent to which these requirements are actually met in practice. Ideally, one should be informed of the working of public recorders without having to make special effort to get information about them e.g. by signs put up in public places

3. SECRET COLLECTION OF INFORMATION

Secret information may be acquired in two ways: one is conditional on a leave of court, the other is not. Sections (1)-(5) of Paragraph 63 of the Police Act contain provisions about the secret collection of information:

"(1) Police are entitled to collect information in a secret manner regulated by law for purposes of preventing, detecting or interrupting criminal acts, identifying or seizing a perpetrator, seeking out a wanted person, identifying a wanted person's place of stay, acquiring evidence and in the protection of persons participating in criminal proceedings and members of the authority conducting proceedings and persons cooperating with the administration of justice.

(2) Data acquired secretly until their use as evidence in criminal proceedings, the identity of persons cooperating with the Police and covered detectives, the fact of information acquisition and its technical details qualify as a state secret .

(3) Measures taken on the basis of Sections (1)-(2), the data of the natural and corporate persons therein involved and of organizations without legal personality may not be published."

There is an equivocation between Section (1), which makes secret acquisition of information possible in a broad area and for several reasons (including e.g. the acquisition of evidence) and Section (3), which prohibits, without exemption, the data of natural and artificial persons from being published. It is not clear how this rule can be followed since the data indicated in Section (3) inevitably become public when they are used as evidence at the public court trial.

A further contradiction results from the fact that the new Code of Criminal Procedure, to be introduced as of June 1, 2003 specifies, in contrast to the Police Act, the kinds of criminal acts against the suspects of which secret acquisition of information, of both kinds, is legitimate. In view of the secret acquisition of information creating ample opportunity to get to know citizens' personal data, two interpretations of the same question cannot be accepted.

3.1. SECRET ACQUISITION OF INFORMATION NOT CONDITIONAL ON LEAVE OF COURT

"For the purpose of fulfilling its tasks of criminal prosecution defined in Paragraph 63, Section (1) Police may

b) acquire information and check data by covering up the aim of proceedings or by relying on the covered detective."[5]

In the passage quoted the definition of acquisition of data is unacceptably broad. It fails to define either the range of data which may be acquired or the persons who may have access to them, or the time during which they may be accessed, or the time when they are to be erased.

5 Paragraph 64, Section (1) of the Police Act

Such a broad-sweeping definition cannot be accepted as Paragraph 69, which gives directions for acquisition of data conditional on leave of court, strictly defines the ways in which information may be acquired for the purpose of prosecuting a serious crime, while not even a serious crime is given as a precondition of acquisition of information not made conditional on leave of court.

3.2. SECRET ACQUISITION OF INFORMATION CONDITIONAL ON LEAVE OF COURT

"(1) With a leave of court and for the purposes of prosecuting crime defined in Paragraph 63, Section (1) in cases of serious crime Police may

a) secretly search private flats (secret search) and record findings with some kind of technical equipment;

b) watch or record happenings in private flats with the help of technical equipment;

c) get to know and technically record the content of letters and other parcels, messages transmitted via the telephone cable or other means of transmission;

d) get to know and use data and information arising from correspondence on the Internet or other computational correspondence (E-mail);

(2) Data acquired through the use of means defined in items c)-d) of Section (1) relating to persons obviously not involved in the procedure underlying the secret acquisition of data

(3) Police may apply the means and methods of secret information acquisition listed in Section (1) (henceforward: 'special means') according to the provisions set out there for the purpose of seeking out a wanted person suspected of a crime."[6]

6 Paragraph 69, Section (1)-(3) of the Police Act

It is not clear under what conditions secret means and methods may be used for the purpose of finding wanted persons: exclusively in connection with those wanted for a serious crime or in connection with those wanted on the suspicions for any category of suspected criminal act, because Section (1) speaks of a "serious crime" while Section (3) mentions "a person wanted on account of the suspicion of having committed some criminal act".

According to Section (2) data about persons clearly not involved in proceedings aimed at the acquisition of information are to be erased without delay and may not be subsequently used. The rule however makes this dependent on the condition that secret acquisition of information should be conducted in the manner specified in Items c)-d) of Section (1), i.e. via watching letters and other parcels, tapping telephone conversations, checking communication through the Internet and other computational instruments of communication. Thus if data are gathered about someone by applying the methods indicated in Items a)-b) (searching private flats or other ways of acquiring information in private flats) it will not be possible to destroy them even when the person turns out not be involved in the proceedings aimed at acquiring information. Another consideration that bears on our view of the problem is that according to Section (7) of the Paragraph the private flat indicated in a)-b) is to be interpreted very liberally as rooms and areas other than public or open to the public qualify as private flats in the technical sense.

4. REQUESTS FOR DATA

"(1) The head of the investigating branch empowered to engage in secret acquisition of information may, with the state attorney's approval, request data related to the matter under investigation, from the revenue authorities and, for the purpose of detecting contemplated crime subject to two years imprisonment or a heavier sanction, a telecommunications organization, health care establishment or its data handling organization, as well as organizations handling data which qualify as a business secret in general and banking, stocks or cash secret. The investigating institution may set a deadline for the performance of data provision. The supplying of data is free of charge and may not be denied. The information acquired in this way may only be used for the purpose given.

(2) In situations which require urgent action , in which delay involves danger, and the matter is connected with drug trafficking, terrorism, illegal arms traffic, money laundering or organized crime, data may be requested without the state attorney's prior permission and the request has to be complied with without delay. In such cases the request has to be marked as an "urgent measure". The state attorney's approval is to be requested along with the request. If the state attorney declines to give his approval, Police are to erase the data thus acquired without delay." [7]

Enacted into the Police Act by Act LXXV./ 1999 and taking effect on September 1, 1999, the passage quoted forms part of a body of regulations which result in the controversial situation that provided certain criminal acts have occurred or certain sanctions

7 Paragraph 68, Section (1)-(3) of the Police Act

have been imposed, police may request data of practically any personal or special kind about practically anyone, even when the person concerned is not suspected of any crime. Requests for data motivated by urgent measures (if delay involves danger) and requests connected with certain types of crime listed do not even require prior approval by the state attorney.

In view of the fact that the provision quoted allows acquisition of data about persons not yet suspected of a crime, it is contrary to the constitutional right to the protection of personal data. In conformity with the sustained practice of the Constitutional Court, such rights may be restricted only if such restriction is absolutely inevitable, only with reference to another constitutional fundamental right or constitutionally acknowledged fundamental interest, to the necessary extent and within certain limits of proportionality. By contrast, the passage quoted allows

- police to acquire data about patients prior to the commencement of criminal proceedings with the aim of collecting general information prior to criminal investigation;
- police to acquire, in the course of criminal proceedings, specially protected data about persons whom police have no well-founded ground to suspect of a crime;
- it makes no distinction between sensitive data (such as medical data) and other kinds of data;
- does not guarantee that police will get to know only such data as are necessary for conducting the proceedings;
- control by the state attorney in itself provides no guarantee against constitutionally unacceptable use of data.

The paragraph quoted also allows requests to be made for data transmitted via telecommunications systems, which in

practice boils down to lists of calls made from mobile phones. In October 2000 the Data Protection Commissioner called the attention of the National Chief of Police's deputy for the criminal branch to the unlawful practice of police claiming such data from telecommunications services in the course of police investigations with reference to the passages of the Code of Criminal Procedure on seizure rather than with reference to the above-quoted paragraph of the Police Act.[8] This practice goes back to Measure 63/1996. issued by the National Police Chief's Deputy for the Criminal Branch on the Ways of Acquiring Data from Telecommunications Service Organizations. This order features express directions to the effect that data needed for the conduct of investigations should be acquired in the manner outlined in the Code of Criminal Procedure's provisions on seizure[9] rather than on the basis of requests for data prescribed in the Police Act. As was expounded by the Data Protection Commissioner, this procedure is unlawful, being subservient to the obvious purpose that police should not have to acquire the state attorney's approval for such "acquisition of data" – requests for data under the Police Act being conditional upon the state attorney's approval while no such permission is needed for seizure as set out in the Code of Criminal Procedure. In his letter the Commissioner argued "Police are to apply the Police Act even when they proceed according to the Code of Criminal Procedure. In other words, proceeding according to the Code of Criminal Procedure does not exclude other legal instruments from being effective. Therefore in cases where the Police Act provides a special rule for some procedural action undertaken by police (such as the acquisition of data from telecommunications service

8 File number 533/A/1999.
9 Paragraph 10, Section (1), Item a) of Act I/1973. Effective at the time of the Commissioner's comments.

organizations in the present case) the general rule (Code of Criminal Procedure) is to be applied with appropriate differences asprescribed by the more specific rule (Police Act)."

5. DATA HANDLING BY POLICE

The law distinguishes between two kinds of data processing by police. On the one hand, police handle data for the purpose of performing its tasks in the prosecution of crime (including prevention)[10], and, on the other, they handle data in the area of their tasks in administration, public security and control of misdemeanor.[11] Data belonging to these two systems of activity are to be kept and treated apart, may not be combined in one unified data base.[12]

The legislator is likely to have been lead by the aim that data acquired for the purpose of the prosecution of crime should be allowed to be used for the purpose envisaged. This is confirmed by the prescription that data acquired for different purposes should be handled separately. At the same time, Paragraph 77 makes an equivocal statement about the question:

"Personal data acquired and stored by Police for the purpose of the prosecution of crime may only be used for police purposes and in the prosecution of crime, unless otherwise provided by law."[13]

The problem is that although the Act prescribes separate data processing, the above passage still does not remove the

10 Paragraphs 84-89 of the Police Act
11 Paragraph 90-91. of the Police Act
12 Paragraph 76, Section (4) of the Police Act
13 Paragraph 77, Section (1) of the Police Act

possibility of police using data acquired for the purpose of the prosecution of crime for administrative purposes, since data handling by police includes administrative data processing. Indeed, in certain cases there is even an opportunity to place data treated separately in one system:

"(1) In the interest of performing its task of prosecuting crime defined in the Act, the Police may – if conditions of data protection are met – conduct individual data handling by combining its criminal prosecution system with its administration system in the course of investigating a given criminal case. Data arising as a result of such data handling not used in the course of criminal proceedings are to be erased.

(2) In the interest of performing its task in the prosecution of crime the Police may – if conditions of data protection obtain – engage in individual data handling by combining its systems of data handling for criminal prosecution with the data handling systems of other public security institutions or investigating authorities in the course of investigating a given criminal case. Data arising as a result of such data handling not used in the course of criminal proceedings are to be erased."[14]

According to this law other organizations or persons may request data from Police data handling systems if they can substantiate their claim to the data. The Act specifies the kinds of organizations that are allowed to request data from criminal prosecution systems, yet the general formulation is much too broad.

It is a serious problem that the law specifies no exact time for the erasing of data, and without such a specification it is

14 Paragraph 88, Section (1) of the Police Act

difficult to check whether or not data are handled to the extent required and for the length of time specified as necessary to achieve the aim.

"In addition to those specified in Section (1) the following may request supply of data for purposes expressly indicated, in the interest of performing their tasks defined in law:

a) investigating authorities
b) courts
c) the state attorney's office
d) national defense services
e) competent body of the frontier guard
f) competent body of the Foreign Ministry
g) competent body of the national defense administration
h) other organizations specified in the law"[15]

In a question of such great importance as the identity of those entitled to request data from the criminal prosecution data base a detailed list of specific persons and bodies would be necessary. The law appears to do just that in the above passage, but Section (3) still extends the range of possible claimants toward the general definition of those able to produce some title to the request for data, which is a serious concession.

"(3) The data handling department of Police may supply with data organizations or persons not mentioned in Sections (1) and (2) – in cases defined by law – if they are able to justify their entitlement to claim the data in question, from its base of data kept for the purpose of prosecuting crime."

15 Paragraph 86, Section (2) of the Police Act

Paragraph 84 defines a number of details including the length of time for which data handled for the purpose of prosecuting crime may be stored. The formulation of this passage is again not free of equivocation. The passage is about the length of time during which data may be stored, on the one hand, but the same stretch of time is given as the time during which police are entitled to make data available to other organizations entitled to handle data, on the other.

According to the definition of Item j) the criminalistically important features of data about persons suspected of drug-related criminal acts and their contacts are to be stored for twenty years and during this period police are entitled to take over relevant data from other data handlers. In view of the fact that the law speaks merely of "drug-related criminal acts", offences of mere consumption fall in this category, and twenty years' storage is difficult to justify for such minor offences.

Without further specification or reference to other legal instruments the term "contact" itself is much too broad, providing an opportunity for biased legal judgment, and it thus comes up against the requirement of security in the law. The consequence that police may process data about "their contacts", i.e. persons not involved in criminal proceedings under Item j) of Paragraph 84, conflicts with the requirement set out in Paragraph 80 that special data must be handled only if they relate to persons suspected of a crime.

Similarly, Paragraph 84 provides that data recorded in the course of identity checks for the purpose of the prevention of crime and misdemeanor are to be stored for two years. It is not entirely clear what cases this passage is valid for. Considering that police's entitlement to conduct identity checks is entirely general and is not conditional on the aim of preventing crime or

misdemeanor it may be questionable whether only data recorded in the course of identity checks for the prevention of crime or misdemeanor are stored for two years, and whether data recorded in the course of "routine" identity checks are erased immediately.

When calls are received on the general emergency hotline, a law prescribes that the caller's phone number and the conversation are to be recorded and stored for a year. In other words, if someone calls an ambulance to a relative who is lying unconscious, the data will be stored by police for a year. False or forged medical prescriptions for medicaments with a drug content exposed as such in the course of police checks as well as all data recorded on such prescriptions are to be stored for five years, for the purpose of the prevention of crime. Such data will typically include the patient's name, age, domicile, social security identity number, identity-establishing data of the physician or institution who, or which, wrote the prescription, data related to the medicament, the identifiers of the pharmacy, the signature and identity card number of the person buying the medicament. This kind of data handling is authorized by law when no criminal proceedings are started as a result of the identification of the false receipts or prescriptions in the course of a police check. Since however the cases mentioned at this stage (e.g. forging a prescription) are criminal acts, and thus have to be followed by the initiation of criminal proceedings (in conformity with the principle of proceeding in the line of duties) one might wonder why the law speaks of 'no criminal proceedings' in the main rule, It remains an open question why data are to be stored for such a long time (five years).

No doubt uniquely, the Police Act secures that personal data should be stored by police without a time limit. A variety of data may be stored in the interest of the prosecution of crime for a

variety of periods defined in Paragraph 84. The detailed list is followed by the words 'unless otherwise ordered by law, personal data handled for the purpose of the prosecution of crime are to be corrected and erased in such a way as to leave the original data recognizable'.[16] Obviously, in some cases such as when correcting registration errors of a simple kind, it is more expedient to preserve the old, erroneous data, and this in no way violates any fundamental rights. The Police Act gives no guarantees, however, that data will be preserved only in such innocuous cases. There is no "unless otherwise provided" clause to counterbalance the controversial provision just quoted, so the personal data may be stored beyond the time defined for registering. The rule in effect defines 'erasure' as something that is impossible to carry out. When the time defined in the rule rolls by, the data are "erased", but they remain recognizable in the system.

Finally, a question about data handling performed for the purpose of public administration: one might wonder why it is necessary to store data about persons and organizations which have exercised their constitutional right of assembly for two years.[17] Data on those exercising the right of assembly (e.g. data about the organizers of a public meeting or event) are to be stored under all circumstances even when the event does not fall under compulsory registration but is legally required to be held in the presence of a security police force, and even when the event falls under the law of assembly. It is difficult to justify the inclusion of this kind of data in the pool of those that are handled for the purpose of public administration.

16 Paragraph 85, Section (2) of the Police Act
17 Paragraph 90, Section (1) h) of the Police Act

DATA PROTECTION AT SCHOOLS

Dániel Máté Szabó

The subject of this study is the processing of students' personal data in public education establishments. The right to the protection of personal data forms part of the protection of privacy, which enjoys the most elaborate effective protection in the present Hungarian legal system and thus serves as the foundation for the protection of the private sphere. Participation in the activities of public education, as will be described below, places students and teachers in a very special situation. The present study focuses on the point where these areas, sensitive in their own unique ways – data protection and education – intersect.

This study is also intended to be a starting point for a discussion. This is reflected in its structure, form and tone, all of which are meant to serve that purpose. Problem areas relevant to the topic will be presented in a unified framework reflecting the structure and terminology of data protection law, highlighting within that frame realistic life situations which arise naturally in the course of the everyday practice of education which deserve the attention of the analyst interested in assessing them in terms of data protection. Besides getting clear about the conceptual foundations and applying them to the realities of public education, the article also aims at presenting real-life situations which are problematic in terms of the right to informational self-determination by putting forward proposals for practice and, where appropriate, for legislation. Some of the proposals to be put forward happily coincide with plans which are being entertained by the Ministry of Education, as is revealed by the draft completed in early 2003 in preparation for a modification to the Act on Public Education. If

the draft gets parliamentary acceptance, it will be a major advance in data processing at schools.

At the end of the paper I turn to examining a few typical instances of data processing within schools. Throughout the paper I will develop my theme in an idiom accessible to both the legal profession and participants in the educational sphere.

1. THE DATA SUBJECT

Educational institutions handle data on persons in different positions. This study focuses exclusively on the personal data of students for the reason that students in schools are in a rather special situation on account of their age and dependent position. To a large extent, students are exposed to the influences of their school environment in many ways including the processing of personal data by their superiors, so the protection of their rights requires greater than average attention on the part both of legislators and the personnel of public education institutions. With many students spending the whole day in the school, what goes on at school greatly influences the quality of students' everyday lives. Rather than just providing useful knowledge and skills, the school is also an institution which educates them; it is their "second home" in which they reveal a great part of their private selves. Thus the data subjects here are mostly children who have adults placed above them and making decisions about them above their heads, so to speak. To put it in legal terms, students are defined as entirely lacking legal capacity, as incompetent in this role. Their self-determination cannot be effectively practised unless certain conditions obtain. The situation of students as data subjects is also special in another way, namely that the processing

of their data almost invariably affects their families, parents, brothers and sisters. This is a result not only of the fact that the parent as a legal representative becomes involved in these legal relationships but also of the further fact that through the student the school inevitably acquires data on the family members and enters them in the school data records.

2. THE DATA PROCESSOR

A data processor is any natural person, corporate person or organization without legal personality who or which handles, i.e. takes, records, stores, registers, processes, transmits, publishes or erases data, i.e. anyone other than the data subject who does anything to personal data.[1] The next question then is: who handles students' data: the institution, the head of the institution or particular teachers, or anyone else within the school who has access to them? This is by no means a question of merely theoretical interest: we have to define the obligations that are incumbent upon the data processor under the Data Protection Act and the subject of those obligations.

2.1. THE INSTITUTION OF PUBLIC EDUCATION

There is no doubt that the institution is a data processor. At this point we could acquiesce in the simplicity of the answer – as the Public Education Act does[2] – treating the educational institution as a black box, examining as far as data protection is

1 Paragraph 2, Section 4.a) and 7.a) of the Act LXIII./1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest (henceforward 'Data Protection Act'). We do not discuss the technicalities of data processing.

2 Act LXXLX./1993 on Public Education (henceforward 'Public Education Act').

concerned only such questions as what sorts of data get to the institution and under what circumstances from the data subject and other data processors and what sorts of data the school discloses to third parties and under what conditions. This could lead to a schematic map of data disclosure routes. This however would leave out of consideration a number of data processing processes going on inside the school which may be of special importance from our point of view. One thing is certain: it is the educational institution that is treated as a data processor by the Public Education Act which prescribes that institutions of public education handle data, thus it is the institution that collects, registers and discloses personal data on the basis of legal authorization or consent from the data subject. The Act does not deal with the persons who carry out these operations in real life. It is up to the distribution of tasks and responsibilities within the institution which data are to be recorded, registered or transmitted by which particular person. It is thus the institution that is responsible to the data subject and it is the institution that is to be called to account in cases of unlawful data processing, according to the Data Protection Act, and the institution in turn may, of course, call to account its employees whose conduct has lead to unlawful data processing. In terms of criminal law, however, the institution is elusive: you cannot indict corporate persons on criminal charges. At the same time Paragraph 177/A of the Penal Code[3] states that only the data processor may be regarded as a perpetrator. Consequently, if we regarded only the institution as a data processor, no one would be liable under criminal law for unlawful data processing at schools (or at the police, court, health care institutions, for that matter, where employees handle data instead of their employer, not personally

3 Act IV./1978 on the Penal Code (henceforward 'Penal Code').

in their own right). This is just another reason why it would be unreasonable to exclude from the range of data processors those natural persons who actually carry out the processing of personal data and make decisions about data processing. In what follows I will treat these natural persons as data processors.

2.2. THE HEAD OF THE INSTITUTION

The head of the institution is responsible for the lawful running of the institution which of course includes lawful data processing. According to the law the head is accountable for the actual performance of obligatory data processing, for defining the orderly routines of data processing within the institution, has the task of taking the organizational and technical measures and laying down the procedural rules which are necessary for meeting data security requirements and is also entitled to call to account employees for unlawful data processing. It is one of the head's tasks to perform legally legitimate disclosures of data to other institutions and persons, therefore only the head or his/her deputy or other employee entrusted by him/her is entitled to disclose personal data to external organizations or persons according to the order established within the institution. It is the head of the institution that is expected to know the relevant legal instruments, notably rules of procedure, which are requisite for judging whether a given request for data is lawful.[4] With the growth of data processing tasks (obligatory data processing, dealing with requests for disclosure of data from authorities and

4 The proposal submitted by the Ministry of Education for modifications to the Public Education Act would make this clear: "The head of the educational institution and – within the limits of the proxy warrant – other leaders senior officials or employees proxied are entitled to disclose data." htp:/www.om.hu/letolt/kozokt/kozokt-mod/20021219doc.

others) it would be expedient for schools to entrust data protection tasks to a person who monitors data processing performed at the school under this specific aspect, preparing or (with delegated powers) making, decisions on data disclosure, informs employees about data protection requirements and monitors changes in relevant legal instruments. This would amount to a task we may call that of the person responsible for data protection, which would not amount to a separate job but would be subsidiary to the person's main job, though by no means a minor part of it. Preparing and controlling the implementation of the data protection regulations applied to the specific circumstance of the local work environment on the basis of data protection rules is another task for which a particular employee could assume responsibility. There is no legal rule at present that would mandatorily prescribe that educational institutions should appoint an official responsible for data protection, but the distribution of tasks within the school may make it reasonable to appoint one, so institutions are free to decide to establish such a job, indeed it would be reasonable to encourage them to do so.

The question of an obligation of the head of the institution to report to prosecuting authorities, including the police, is a very special one. The school director, e.g., may be considered under Paragraph 137. k) of the Penal Code as an official person[5] (in discharging his/her obligation of issuing a student's identity card or a school report), and under Paragraph 122, Section (2) of the Act on Criminal Procedure an authority and an official person informed of a crime in the sphere of their official activity have an obligation to make a report to prosecuting authorities.[6] The head of the institution is thus under an obligation to report one of

5 B.H. (Court Decisions) 1995, 199.

6 Act I./1973 on Criminal Procedure (henceforward 'Act on Criminal Procedure').Paragraph 171, Section (2) of the new Act on Criminal Procedure (Act XIX./1998), which is to become effective in 2003, makes the same provision.

his/her students if he/she has committed a crime which the head has been informed of within the purview of his/her competence. Legal interpretations of what it is that a head is informed of within the purview of his/her competence diverge widely. The question may arise e.g. whether something heard at a teachers' meeting counts as such information. Majority opinion says 'no' to that question (i.e. the official powers of the head of the institution are seen as restricted to his/her issuing of official deeds) and that is the view of the matter that comes closest to the requirements of legal interpretation conforming to the constitution which conduces to the greatest possible effectivity of fundamental rights. Yet the question is far from being beyond dispute. What would bring this problem to a solution is a legal settlement of the duty of confidentiality in the profession[7] and a clarification of the relation between the duty of confidentiality and the duty to report incumbent upon the head as a person in authority.

2.3. THE TEACHER

Of all the school staff, the teacher has the closest contact with the students. In the sphere of his/her teaching activity he/she gets to know details of students' lives outside the school. It is teachers who talk to them, who decide what questions they ask them, and who decide what they do in the course of teaching them with the information they have come to know. Ideally, a special relationship of trust evolves between teachers and students, a relationship in which the student may share even such problems and questions as are not closely related to their education with the more experienced adult whom they may occasionally even ask for help.

7 See 2.3.

At the same time this relationship is also one between data subject and data processor: the teacher inevitably handles the student's personal data. The teacher acquires most of the data and enters them in the institutional register and he/she can also be seen as a creator of certain data (such as those relating to students' conduct at school and their achievement in the subjects) in so far as assessment partly depends on his/her judgment. The most important register, the logbook is run by the teacher who is entitled to enter personal data in it. The teacher can be seen as a special data processor in the further respect that data which are not personal to others may become personal in the teacher's mind, so to speak. A teacher who knows his/her students' handwriting, vocabulary and is intimately acquainted with the students' personality manifestations may be able to identify examples of these with particular students, This enables the teacher to recover, in many cases, the correct connection between particular data and particular students.[8] A questionnaire filled out in anonymity conveys no personal data to someone who does not know the students or only knows them casually, while the teacher may know from the handwriting or the answers given which questionnaire was filled in by which student.

Despite all these important facts the law provides no rules for the activity of the teacher as a data processor. This is at its most striking in the lack of any regulations on teachers' duty of confidentiality. The duty of confidentiality in one's profession springs from the relationship of trust between a person and the subject of the duty in which the party under duty comes, as a natural consequence of his/her profession, to know information which does not become known to others. It is generally accepted that a physician, a priest or a pastor is under a duty of

8 Cf. the last sentence in Paragraph 2, Section (1), of the Data Protection Act.

confidentiality. The physician's duty of confidentiality is declared in law, while the priest's or pastor's is not expressly anchored in legal instruments. In view of the nature of the relationship of trust between teacher and student the teacher should also be subject to the duty of confidentiality vis-à-vis the students. Without a duty of confidentiality the relationship of trust is vulnerable and without it the teacher's work would often be without effect. Paragraph 122, Section (1) of the Act on Criminal Procedure entitles anyone to make a report of a crime to the police. In theory, this entitles the teacher to report his/her student when his/her suspicion is founded on confidential communications from the student made in the spirit of respect for the teacher or with a view to asking for help. If there are criminal proceedings against a student, the teacher is under a duty to bear testimony as a witness according to Paragraphs 62 and 66 of the Act on Criminal Procedure.[9] This would be ruled out, or practically ruled out, if the teacher were under a duty of confidentiality. The relationship of trust which could serve for such a duty is very similar in nature to the relationship of trust arising from the nature of the profession of a physician or a priest or pastor which underlies their duty of confidentiality, so a sense of such a duty is clearly felt to be involved in the teacher's role. Yet while the physician's duty of confidentiality is secured in law and the pastor's is generally acknowledged, neither of these statements can be made about the teacher's duty of confidentiality. The duty of keeping secrets one has come to know in the course of doing one's profession does not necessarily have to be laid down in a legal instrument, but when it is not, its existence should be a matter of course to both the duty subject and the applier of the law. If this is not the case, it will be necessary to anchor the duty in a legal rule. That is why the

9 Paragraph 79,Section (2) in the new Act on Criminal Procedure.

Parliamentary Commissioner of Civil Rights and the Data Protection Commissioner prepared a recommendation for the Minister of Education in preparation for a supplement to the Public Education Act that would settle teachers' duty of confidentiality. (The then Minister did not accept the recommendation, finding it impossible to interpret.)[10] The relevant rules could be laid down among the teacher's duties in the Public Education Act.[11]

School staff comprises not only teachers but also other employees helping in teaching and education such as officials responsible for child and youth protection, school psychologists and school physicians. What we have discussed in connection with teachers may apply equally to them, namely that they have regular contact with the students, know them personally and have some knowledge about their lives outside the school. As a result the relationship between these members of school staff and students may also acquire a quality of trust which may even be stronger than with teachers. Therefore it is reasonable to create legal foundations for the duty of confidentiality with respect to them, even if the question can be regarded as settled with respect to some of these jobs, although via regulations not specifically related to the school.[12]

10 File number 171/H/2000.

11 According to the draft of a modification to the Public Education Act mentioned above at note 4. "teachers and employees directly involved in teaching and education are under a duty of confidentiality with regard to all data related to children and students which they come to know in the course of their work. This duty is independent of the existence of the legal relationship of employment and does not expire after its termination. The duty of confidentiality does not apply if the child or student or a minor's parent has absolved the teacher or employee. The duty of confidentiality does not extend to data that are open to processing and disclosure under the present law." Such a rule would present a solution to the problem discussed here.

12 According to the regulations quoted in the previous footnote the duty of confidentiality would also hold for persons in these jobs.

3. THE LEGAL GROUND OF DATA PROCESSING

The legal ground for processing students' data may be provided by the data subject's (student's or his/her legal representative's) consent or authorization conferred by a legal instrument (primarily the Public Education Act).[13] The Constitutional Court defined the content of this right secured by Paragraph 59 of the Constitution in a way which made it different from traditional protective rights when the Court took its active component into consideration and interpreted it as a right to informational self-determination [Constitutional Court Decision 15/1991. (IV.13.)] Accordingly the purport of this right is not simply that data are to be protected from unlawful access, use, publication, change and destruction, but also, or rather primarily, that every person is entitled to decide about what is to happen to his/her personal data, whether he/she will allow others to record, store, disclose, in one word: process them. The essential ingredient of this right is consent: the data subject exerts his/her right by deciding whether to consent to the processing of his/her data. Consent may be given in several ways, but the important point is that the data subject should know without any doubt what he/she is consenting to, and that he/she should be allowed to decide freely, without any influence (the principle of explicit, informed and voluntary consent). The Data Protection Act does not contain these words literally, but they can be derived from the content of the right to self-determination. According to the individual's right to self-determination every autonomous person has the right to decide and act freely and according to his/her own values and life plans, and this right is limited only by the similar rights of others. Accordingly, consent provides an appropriate

13 Paragraph 3 of the Data Protection Act.

legal ground for the processing of personal data when it is the voluntary, explicit and informed expression of the wish of the person concerned.[14] The Data Protection Act also lays down an important formal requirement with respect to certain data: consent to the processing of sensitive data has to be given in written form[15].

The right to informational self-determination may be lawfully restricted if the data processing is not made conditional on the data subject's consent. According to the Data Protection Act this is allowed when there is a law or a local authority decree (usually of restricted scope, on the basis of, and strictly in accordance with, authorization by law) which gives orders for data processing. Sensitive data may be processed only if such processing is ordered by a law, and certain sensitive data[16] may be processed only under circumstances defined in the Data Protection Act (e.g. being required by an international convention, or being instrumental in giving effect to a fundamental right secured in the Constitution, or serving some interest connected with national security, prevention or prosecution of crime).

3.1. THE DATA SUBJECT'S CONSENT

3.1.1. COMPETENCE TO CONSENT

The right to informational self-determination can be exercised by giving or withholding consent. In so doing, the person concerned exercises a fundamental right. In order for him/her to

14 Voluntary, explicit and informed consent is an internationally accepted principle of data protection, see e.g. Guideline 95/46/EK Section 2 (h) of the European Parliament and Council of Europe on the Protection of the Person with regard to the Processing of Personal Data and on the Free Flow of these Data.
15 See Paragraph 2 of the Data Protection Act.
16 See Paragraph 2, Section (2), a) of the Data Protection Act.

be able to do so – for the consent to be valid, in the present example –, it is necessary for him/her to be competent according to the constitutionally established sense of the term. In Paragraph 56, the Constitution defines all persons as having legal capacity but it does not give any provisions on competence. The Constitutional Court expounded its view on the extent to which the exercise of this fundamental right may be legitimately restricted with reference to the person's age, in Constitutional Court Decision 21/1996. (V.17.)[17] The Constitutional Court laid down no specific age as a condition of competence to exercise a fundamental right. Whether competence to exercise a fundamental right obtains is a matter for weighing in particular cases, which is to be based on such considerations as the child's discretion, which will primarily depend on age, and the particular risk threatening the child's development. As can be seen from these facts, there are no exact criteria for competence to exercise a fundamental right pinned down exactly in a rule. The criteria of competence as provided by civil law are just one among those applicable in the context of the exercise of a fundamental right, and they do not always provide an adequate solution. They are therefore not to be applied across the board. It is undoubtedly practical to borrow criteria of competence from civil law (there being no other system of criteria of similar elaborateness), but

17 The Court was examining the question in the context of children's right to association. Children's exercise of their right to association may be legitimately restricted according to Paragraph 67, Section (1) of the Constitution: children's right to receive from the state the protection and care that is necessary for their physical, intellectual and moral growth, establishes a constitutional duty on the state to protect children's development. It is this obligation to protect that serves as a constitutional foundation for the legislator or the court to limit children's exercise of the relevant right. According to Paragraph 67 of the Constitution the state has to protect children not only from influences harmful to their development but also from taking risks such that the child is unable to realize or assess either the available options or the consequences of each for his/her personality, later life and social integration as a result of his/her age (and the level of physical, intellectual and moral maturity assumed from his/her age).

their adequacy is disputable. Legal statements in the civil law sense of the term are statements made to effect arrangements concerning relations between persons and property and the criteria of competence are defined by the Civil Code[18] with such matters in mind. Legislators perceive differences in discretion arising from age in other human relationships and, accordingly, devise different sets of criteria for other branches of law (one might think of the age limit to criminal liability or to employment) or resort to the notion of competence under civil law (one might think of competence for suits as defined by the Act on Civil Procedure[19]), but these provisions are made in the form of legal rules. As regards the exercise of the fundamental right to informational self-determination, the legislator chose neither the first, nor the second of the above-mentioned notions. It is therefore disputable whether the civil law rules of competence are correctly and rightfully applied – as subsidiary rules, as it were – for the only reason that they are the ones most frequently invoked. The Data Protection Act regulates relationships that are seen as belonging to the realm of constitutional rather than civil law,(see the Preamble), it is therefore an at least questionable move, if not to be completely ruled out of court, to borrow the system of criteria applied in civil law. Nevertheless, this is the line consistently adopted by the Data Protection Commissioner concerning the question of children's consent to data processing.[20] The reasons in support of such a line are disputable.

According to the Constitutional Court's decision on constitutional interpretation referred to above, whether competence to exercise a fundamental right obtains in a given

18 Act IV./1959 on the Civil Code (henceforward 'Civil Code').
19 Paragraph 49, Section (1) of the Act III./1952 on Civil Procedure,.
20 See e.g. the Data Protection Commissioner's recommendation concerning the data collection through questionnaires performed by the "Xénia Láz" Association. (450/A/1996).

case is a matter for consideration, so unless legislators lay down specific rules for certain situations in life, the teacher may have to make decisions of this kind several times during an average weekday. In a social sphere such as public education, in which young people of limited discretion find themselves in a situation that requires decisions on a variety of important practical questions, there is a clear need for legislators to lay down a set of conditions within which the rights may be exercised. Such a set of conditions could rest on the civil law rules of legal competence, but it may as well be different, milder or stricter, as is appropriate to the case under consideration. In certain situations for instance the teacher or the head of the institution might take responsibility by giving his/her consent to the decision of a young student. Such issues need to be settled in positive law.

With reservations as to the justification and practicability of applying civil law standards in this area, let us now review the Data Protection Commissioner's recommendations for the ways in which students may consent to the processing of their data within the system of criteria of competence provided by civil law. Students tend to lack full competence, but this is just a generalization: in any actual public education institution there are students who are not competent, students who have limited competence, and students who have full competence. They should not be treated according to the same standards. Consent for an incompetent person may be given by his/her legal representative. In order for the consent given by a person with limited competence to be valid, consent or subsequent approval from his/her legal representative is required.[21] What this comes to in practice is that consent for students below fourteen years of age is given by their parents, and parents' approval is

21 Paragraph 12/A, Section (2) and Paragraph 12/C, Section (1)of the Civil Code.

required for consent given by students between fourteen and eighteen to be valid.

Public education institutions do not always realize that consent by a parent or a legal representative is necessary. They usually ask for it only when there is a legal rule specifically prescribing for the case under consideration that parents' consent should be obtained (e.g. in cases of application for admission to a school) or when the parent's consent serves the interests of the school as data processor by e.g. diverting responsibility (as with parents' permission for the child to go on a class excursion, or concerning the management of class funds), and also when the formalities attaching to an act make it obvious to the lay person that it is a legal statement (e.g. signing a document). When, however, the significance or form of some instance of consent does not reveal its nature as a legal statement to the lay person, institutions tend to be oblivious to the fact that the student's consent is, or may be, insufficient in itself. This is especially so in cases where the processing of data clearly serves some interest of the student's, or when data processing without the appropriate consent does not seem to be an instance of the restriction of some right (e.g. the publication of a class photograph – i.e. the students' portraits – on the school's homepage, i.e. the publication of their personal data). It sometimes happens that while school staff realize that they have to do with a case of a legal statement, and the student alone may not give valid consent, school staff still think they, being adults, may take the responsibility of deciding for the students, who are not adults. Asking the students in these cases is often merely a gesture. To take an example, at a national athletic and football competition organized for students with disabilities, one of the conditions a student had to meet in filing an application for participation was attaching the document recording the decision

of an expert committee charged with certifying the fact of disability in particular cases. According to the Data Protection Act, such a document, containing as it did data of the student's state of health, could only be passed on with the written consent of those concerned. The application form sent out by the institution announcing the competition instructed applicants to have it "validated" by the school director's signature without asking for the parents' consent to the disclosure of data. In his statement the Commissioner argued that the parents' consent could not be ignored and therefore schools were not allowed to enter students as they pleased if entering them would involve the disclosure of sensitive data.[22] If the invitation had gone through as originally planned, it would have lead to a pool of medical data acquired from students with disabilities which could have been organized into a national data base in which data are handled with the students themselves and their legal representatives completely ignorant of where their medical data were processed and by whom. Apparently innocuous disclosure of data may involve risks such as these.

The question of consent to be given by students of limited competence to the processing of their personal data is thus in need of settling in the form of legal rules. As for the exact way in which this should be done, one might propose a solution based on the civil law notion of competence with due attention paid to the special features of data processing at schools. It should be laid down as a main rule that the consent of an incompetent student may be given by his/her legal representative, while students with limited competence may give their consent themselves to the processing of their personal data with at least subsequent approval from their parents as a condition of validity. The student

22 File number 457/A/2001.

may consent personally to data processing in the sphere of the school's everyday activities which do not put him/her at any kind of disadvantage (such as posting his/her name on the school board in a context favorable to him/her), but even in such cases the school is under a duty to inform parents about the student's decision, who, in turn, may protest to the data processing. No right must be conferred on the institution which would entitle it to handle students' data. If this were the case, the institution would itself "consent" to its own processing of data, and not even a right conferred on students or the parents to subsequent protest could provide an appropriate guarantee against such an arrangement, as students and parents have traditionally been anxious to avoid taking a stand against their child's school on which they consider themselves as "depending".

3.1.2. Voluntary Consent

In the area of data processing based on consent, the voluntary consent of the student (or parent or legal representative) forms a precondition of the validity of consent. A public education institution is a community of people with a structure that uniquely amalgamates legal relationships based on legal rules for public education and labor relations, and, together with the sociological characteristics of the community (age differences, obligatory participation in a closed community of members mutually depending on each other), these give rise to a special relationship between data subjects and data processors. In the school there is an unequal relationship between the positions of the leadership of the institution and the teachers on the one hand and between students and the staff, on the other. Students are dependent on

school management and teachers in many ways. Only voluntary consent can create an appropriate ground for data processing, and if the data subject has no choice (is not asked whether he/shewill consent, or can only choose from alternatives each of which involves consent to data processing) or if he/she decides under some degree of duress, it is as if there had been no voluntary consent at all. A student (parent, legal representative) who has reason to fear that refusal to consent to data processing may lead to indirect expression of disapproval or retaliation (e.g. a failing mark, disciplinary proceedings, exposure to humiliation before the class, falling into disfavor with the teacher, unfavorably biased assessment of learning achievement etc.) is not acting free of duress. The Data Protection Commissioner has dealt with a complaint in which a parent reported that he/she had to fill in a marketing questionnaire distributed by a private firm and send it back with a statement of consent signed unless he/she wanted his/her child to get a one (the lowest mark).[23] There are many more different forms of pressure. In all cases where such pressure has influence on the decision whether or not to give consent, the data processing based on such a decision will be devoid of a legal foundation, and contrary to the law. As a result of the dependence detailed above, students tend to have reason to fear something unpleasant happening to them, if they decline to comply with a request, and this fear alone is enough to deprive the decision of its voluntary character even if no one intends to cause any disadvantage. As a result data processing on the basis of consent is confined within a very narrow range at the school with its complex relationships of dependence, and therefore there are only a few situations in which we can speak of full-blown consent as a legal ground. Legislators may consider in advance the kinds of

23 File number 850/A/1998.

data processing that cannot be dispensed with if the school is to be capable of functioning, and legal authorizations have to be created for such data processing. In the school setting voluntary consent should be made a condition only for unforeseeable situations which cannot be provided for in legal instruments due to the inevitable limits of legislative foresight. If there is no legal authorization for data processing, decisions whether or not consent may create an appropriate legal ground are to be made with great circumspection and attention to the features of the particular environment. The teacher has to weigh all possible disadvantages before asking even a seemingly innocent question. If, for instance, a teacher asks students in one of the classes in early January about their Christmas presents, he/she may embarrass a student (by making him/her reveal his/her religious identity) who can only truthfully say that they had no Christmas because they have different celebrations. I am not saying that such questions must not be put to students. I am only suggesting that they have to be put with great circumspection and tact.

3.1.3. The Problem of Collective and Negative Consent

More often than not, schools do not seek individual consent, i.e. a series of statements made separately by every one of those concerned. "Collective" consent is routinely treated as an appropriate legal ground in cases e.g. when the class cast a vote to decide whether they agree to data processing (e.g. deciding on such questions as whether the class will take part in a children's program broadcast by a television company) or when some body of students give their consent to data processing. To take an example, one school argued for the rightfulness of its processing

of data with reference to the "rules of the house" (inner school regulations) which had been accepted by the students' self governing body which represents all students. Another inappropriate form of requesting consent is to make the request in negative form, i.e. to give students only the right to protest by relying on the pressure of the collectivity. A question put to a class of pupils such as "Would you mind it if two men came into the next class with a camera and record the way children were giving clever answers to the questions?" is an example.

3.2. AUTHORIZATION BY A LEGAL RULE – LEGAL REGULATIONS ON DATA PROCESSING

Paragraph 40, Sections (4) and (5) as well as Supplement 2. to the Public Education Act define the kinds of students' personal data which are to be registered and handled and those of them that may be disclosed to other institutions, which, again, are defined by the Act. Data outside the scope of those defined in the Act may only be processed and disclosed to other institutions with the data subject's consent, unless otherwise provided by some law.

3.2.1. Minimalism

The provisions of the Public Education Act on data processing are rather poor. The few rules it contains for this area amount to no more than the prescription that schools are to register and handle the data indicated in the Supplement[24] and registers prescribed in other legal rules are to be kept and data are to be

24 Paragraph 40, Section (4) of the Public Education Act,.

supplied to parties such as are defined in the national statistics project and defined in the decree on local authorities. There are also a number of provisions relating to the processing of data about accidents happening to students and children.[25] Supplement 2 to the Act lists the kinds of data which may be kept in registers, and defines the range of persons or institutions to whom data may be disclosed. These provisions are open to criticism on several counts. First of all, they deal with much fewer questions than one could reasonably expect of a body of regulations minimally required to deal with the problem of data processing. Despite the extraordinarily broad range of data listed in Item 1. of the Supplement and the special character of the situation, there are no guarantees for data processing at schools. There is only a legal authorization to process and disclose data, and even this is done in such a way that the lists are left open at several points. It would be a task for the head of the institution to lay down intra-institutional rules for data processing. The Act provides no point of reference for this task. The Act should say something at least about the conditions under which data may be passed on, and the range of tasks for which the institutions listed may legitimately request data. There is no rule at present to indicate what sorts of request for data may be denied (see what has been said about teachers' duty of confidentiality). Nor is there a rule that would state that only the head of the institution (or a person with a right delegated by the head) has the powers to disclose data, not other employees within the institution. What these poor regulations result in is an unlimited restriction of the right to informational self-determination, providing an authorization to handle data while giving no guarantees for the protection of the rights of data subjects. The fact that appliers of

25 Paragraph 40, Section (5) of the Public Education Act,.

the law within the institution cannot be expected to apply the Public Education Act with the restrictions imposed on them by the Data Protection Act or in accordance with the general principles of data protection only serves to underscore the need for such rules as would address these issues in specific terms. It is exactly in such cases that sectorial data protection rules have to be more specific and detailed. In response to a recommendation written by the Data Protection Commissioner outlining the above problem and proposing a modification to the Act, the Minister of Education responded in 2000 by opining that there was no good reason to make the provisions of the Public Education Act on data protection more precise, for the reason that the Data Protection Act contained satisfactory rules to settle those matters. The Minister argued that heads of educational institutions were supposed to know the legal rules which define the functioning of the institution.[26] In actual experience however, there is a great deal of insecurity and infringements of valid rules are frequent. Not even the most competent head can be realistically expected to know all rules relating to legitimate addressees of data disclosure,(e.g. the Police Act, the Act on Criminal Procedure and the Act on Misdemeanor), their functioning and procedures. The head of the institution has to know the rules which relate to the functioning of the institution, and that is exactly why the Public Education Act, which is intended to be a fundamental legal code book for regulating the operation of educational institutions, must contain rules which regulate data processing by public education institutions.

Hungarian data protection law – in keeping with the European trend – follows the regulational model of general law/sectorial law in which we find the most important principles of data

26 File number 171/H/2000.

protection, the conditions of limiting the right to the protection of personal data and the guarantees for its protection in what is called the general law. This law does not normally contain express authorizations for data processing. Provisions on kinds of data and data processors and their authorizations for data processing are found in the sectorial laws. Without such laws, the content of the general laws cannot become appropriately effective, what is expressed in them at the level of principles can become real only to a minimal extent. Sectorial regulation is thus necessary primarily with respect to data processors entitled to handle especially sensitive data and data processors who handle the data of a great number of subjects, and data processors who handle the data of subjects who are in a dependent position in relation to them. This is true of public education institutions.[27]

3.2.2. Data Types

The types of data which are to be registered, including several kinds of sensitive data, are listed in item 1. of Supplement 2 to the Public Education Act Such a list is required for the reason that according to Paragraph 3, Section (1) Item b) of the Data Protection Act, personal data may be handled without the data subject's consent only if this is authorized by law. When the law prescribes that certain data should be processed, it restricts the scope of the right to informational self-determination since in such cases data are handled not according to the subject's orders

27 The above-mentioned legislative draft proposal would add a new title to the Public Education Act. We would find under the title 'Data Processing in Institutions of Public Education' we would find very important provisions which we do not find fin the law as it is at present. In this part of the proposed bill contains rules on teachers' duty of confidentiality, clarify the aim of data processing by institutions and make data processing of students' data dependent on the obtainment of one of those aims. It would indicate who is entitled to disclose data and it would prescribe that an order ordered mechanism data processing should be established in institutions.

but according to the legislator's decision. It is therefore required that the legislator should also define the class of data that are to be handled. The list provided in the Supplement has therefore to be examined in terms of how precise is the class of data available for processing, whether it is open or closed, whether, in other words, the law allows practically all sorts of data to be registered or it does not. If the law did make virtually all data available for registration, that would amount to an unlimited restriction of the right, i.e. to its deprivation of any content. Arranged in items, the Supplement suggests that there is an underlying taxonomical order to it. With respect to personal identifiers, domicile, addresses and phone numbers, the list is also rather precise.[28] The other kinds of data are much less precisely delimited. The expression 'related to' allows room for personal interpretations. The principle of taxonomy-based listing is also contradicted by such formulations as "especially".[29] When this expression is used, in the text of the law, any data related to the student relationship may be handled and is to be handled, and "especially" is followed by a mere list of examples of data that the legislator thinks must be available for processing in any case.

It would be unrealistic, however, to expect the legislator to give a strictly closed and precise list of data that are available for processing and data that are to be handled. It would be naive to think the legislator is able to anticipate all the sorts of data that may be needed in public education situations as precisely as is otherwise possible in other situations of life. The expression "data related to" the student's development, disciplinary and compensatory matters etc. is not to be criticized too severely, because one cannot know which personal data may belong to this class in a particular situation. In its present formulation Item d)

28 See 1)a) and b) of the Supplement.
29 See 1)d) of Supplement 2.

with "thus especially" added opens the class of data to be handled too wide, so the expression should be left out and classes of data that might be reasonably listed but not indicated in the paragraphs beginning with a dash ("–") could be indicated at the same level of exactitude and in the same style.

What usually gives food for thought is the need to decide whether some particular data may be registered or not. To make that decision, it is necessary to examine whether the kind of data may be included in one of the data classes listed in the Supplement. The fact that a student is a drug user (which is sensitive data related to addiction) cannot be handled in the public education institution of course. If, however, drug use counts as a breach of discipline under the rules of the house, then this data may also be handled by the school, as in such cases the data is the student's data related to his/her disciplinary problem.[30] This authorization does not create a legal ground for collecting data on the students' drug consumption (through regular or random checks). It creates such a ground only for processing data that come to the institution's notice in the course of disciplinary proceedings. Within classes of data which have been delimited with insufficient exactitude (such as the present one) the principle of appropriacy to the aim may be used by the institution as a guideline in determining which particular data are legitimately available for processing. In sum, data may be handled if they serve the original aim of the legal authorization valid for the given class of data.[31]

30 See the third Paragraph beginning with a dash of 1.d) in Supplement 2.

31 If the legislative draft of the Ministry of Education is accepted, the Act will unambiguously define the aim of the data processing: "Institutions of education may handle the personal data of children and students only for purposes of teaching and education, purposes required for the performance of pedagogic tasks of habilitation and rehabilitation, for child and youth protection, school health care, the keeping of registers defined in this Act, the purpose of detecting crime and misdemeanor, judging the degree of punishability and liability, to the extent required by the aim.

3.2.3. The Legal Ground for Data Disclosure

Item 2 of Supplement 2 to the Public Education Act addresses the question of legitimate disclosure of data by providing a list of legitimate addressees and data available for transmission. In the last four of the five Paragraphs beginning with a dash ("–") that make up the list of the classes of data available for transmission is precisely delimited and aim dependence seems to be secured with respect to the addressees of the data transmission. In formulating these items the legislator obviously took such great care in delimiting the class of legitimate addressees that he indicated the data subject's school class among the possible addressees of disclosures of data relating to the student's assessment.[32] The aim of data transmission, however, is not indicated. Legal authorization for the disclosure of personal data presupposes the satisfaction, by the data processor, of a number of requirements such as indicating the class of data, the addressee and a specific aim. Authorized disclosure amounts to a restriction of a fundamental right, and the extent and conditions of such restriction have to be defined exactly. Therefore the law must unambiguously reveal what can be legitimately done to the data. A legal rule merely circumscribing what may be legitimately done with data undermines the principle of security in the law. This shortcoming is at its gravest in the first Paragraph beginning with a dash, where the class of personal data available for disclosure is not satisfactorily delimited and, as a result, all data are communicable. (We have just seen that "all data" may mean practically any data of any kind.)[33] Nor is the addressee exactly indicated here: the maintainer, the court, the police, the state attorney's office and the local authority are precise definitions, but

32 Second Paragraph beginning with a dash.
33 See 3.2.2.

"administrative body" makes the class of legitimate addressees limitless. This is an authorization for data processing without a precise indication of either the class of data, or the aim of disclosure, or its addressees. This authorization could be used by the Ministry of Finances to support a request for students' school reports at the Training College of Finances to get information about students' level of proficiency graduating in the near future, or the Ministry of Defense could acquire the health-related data of young students in their fourth year at secondary school to find out about the physical fitness of young men coming up for conscription. This is not to be tolerated. No fundamental right should be allowed to be restricted through imprecision. The Data Protection Commissioner does not consider the first Paragraph beginning with a dash in item 2 of Supplement 2 to the Public Education Act a legal authorization for data disclosure. In a statement he argued that the above-mentioned provision of the Supplement does not represent a general and freely applicable authorization.[34] In another statement he argued that the Public Education Act authorizes the administrative body only in principle to receive data. This authorization is not a sufficient legal ground for having data disclosed. When requesting data, the institution making the request has to indicate the legal provision which authorizes the given administrative body to request and handle the data for the given purpose. (As for the particular case in which the Commissioner had given his opinion, it was a request made by a district office of the Surgeon General's Office to the school for the names and addresses of students who had been punished for breaking the prohibition against smoking which was accepted as part of the school regulations approved by the students' body.)[35] This authorization is merely general. It is addressed to a class of

34 File number 861/A/1999.
35 File number 104/A/2002.

bodies which are authorized to take over personal data from public education institution registers, but within certain restrictions only, on some legal ground and for the achievement of some aim.[36] The view one can infer from the statements of the Data Protection Commissioner is that data processing requires a precise legal authorization. If there is no clear legal authorization, the Public Education Act alone does not provide an appropriate legal ground for data processing. This being so, the first Paragraph beginning with a dash in item 2 in Supplement 2 to the Act is not only superfluous but positively harmful, as it provides an apparent legal ground, deluding the heads of public education institutions into thinking that the Public Education Act authorizes them to disclose any data to any official body. This provision misleads rather than regulates, so it is in need of such supplementation as will reveal that data processing needs to take account of a further legal rule which defines the range of data available for disclosure, the addressees and the aim of disclosure. In 2000 the Minister of Education stated that "it is impossible to determine centrally – especially at the level of laws! – what are the sorts of personal data that may and can be disclosed in a given case".[37] In light of the set of conditions restrictions of fundamental rights are to meet and on the basis of the Data Protection Act, precise definition at the level of laws is a strict requirement, and it does not seem unfeasible in other areas of sectorial laws.[38]

An especially sensitive area within data disclosures is those data that are disclosed at the request of police. Police's interest

36 File number 171/H/2000.

37 The Minister of Education's letter in response to case 171/H/2000.

38 See e.g. Act XXXI./1997 on Children's Protection and the Guardianship Administration (henceforward the Children's Protection Act), in which data, addressees and the aims albeit in a sophisticated language are appropriately defined. This shortcoming of the Public Education Act would not be overcome by the legislative draft prepared by the Ministry of Education which I have mentioned several times. Instead of narrowing the range of legitimate data disclosures in Supplement 2 to the Act, it would extend them, allowing for a range of further kinds of data disclosure.

in data registered at public education institutions is understandable, since a school knows a lot about its students and almost all the students' families are represented in one way or another in the school registers, so the information possessed by a school may be a good starting point for an investigation. Police often request data from schools not only when a student is involved as suspect or aggrieved, but also when the investigating authority wishes to find out something about a member of the family. The Public Education Act and the Police Act[39] together give sufficient authorization for the disclosure of data kept in school registers. All data may be disclosed to the police[40]:in performing his/her task, a police officer may ask information from anyone, and no one is entitled to refuse to give information at the request of a police officer unless this is specially provided by a legal rule. In performing their task of prosecuting crime, police have access to personal data handled by other bodies. Data processors, unless exempted by the law, are obligated to comply with police's request for data.[41]

The conditions of data disclosure are appropriately determinate in the two Acts: both the public education institution and the police have an appropriate legal ground secured in law for processing data within the bounds set by the principle of aim dependence. Of course, we do find shortcomings here. The most conspicuous of these shortcomings is the lack of a duty of confidentiality on the teacher's part. According to the last sentence of Paragraph 32 of the Police Act if a police officer asks about facts which the teacher knows on the basis of a confidential conversation with a student, the teacher may not refuse to give an answer unless otherwise provided by law. The Public

39 Act XXXIV./1994. On the Police (henceforward 'Police Act').
40 Public Education Act Supplement 2, Item 2, first Paragraph beginning with a dash.
41 Paragraph 32, Section (2) and Paragraph 82 of the Police Act.

Education Act is the law that should "provide otherwise" for such life situations by laying a duty of confidentiality on the teacher.[42]

The public education institution is part of the child protection indicating system[43] which is to be established according to the Act on Child Protection. This is a system of data transmission with several points of input. The Child Protection Act contains very precise rules for data disclosure determining the purposes for which, the bodies to which, and the kinds of data that may be disclosed. By contrast, data disclosures within the indicating system are absolutely unregulated. The idea underlying the child protection indicating system is that bodies and persons performing child protection tasks (such as nurses, police, the state attorney's office, social organizations, churches) and public education institutions have an obligation to give an indication to the child welfare service whenever a child is endangered and to initiate an official procedure when there are strong reasons to do so.[44] The suspicion that a child is endangered is often based on inferences which are not immune from error and misunderstanding. This may give rise to disclosures that may cause a great deal of harm even when the teacher gives a well-meaning indication in the child's interest. For instance, if the student often draws wine bottles in drawing classes, the teacher may draw the conclusion, perhaps fallacious, that the student's parents are alcoholics, possibly letting their child drink alcohol, so he/she initiates police measures through the system against the family in question.

42 See 2.3. We will come to speak of the problem of joint data processing by police and schools.

43 Paragraph 17, Section (1), Item c) of the Child Protection Act,.

44 Paragraph 17, Section (1), Item c) of the Child protection Act

4. TYPICAL CASES OF DATA PROCESSING WITHIN SCHOOLS

4.1. CIGARETTES, ALCOHOLIC DRINKS, DRUGS

The staff of public education institutions often feel they have to assume a role in curbing students' consumption of cigarettes, alcohol and drugs – this last being perhaps the most sensitive problem area. Schools often do not stop at prevention through information and education but feel called on to deploy other means such as sanctioning smoking and alcohol consumption within their own competence, while in trying to counteract drug consumption they try adapting the methods employed by police in prosecuting crime. In trying to stop these problems as far as possible, they often go beyond an examination of particular cases to punishing them and finally get to the stage of general preventive checks. This transformation of the methods employed by public education institutions involves increasingly intense intervention in the students' private sphere. How do schools create the legal ground for such measures? By adopting appropriate rules as part of school regulations, the consumption of cigarettes, alcohol and drugs can be made into a breach of school discipline. (School regulations cannot in principle be valid for conduct outside the school, but being under the influence of alcohol and drugs may become a breach of school discipline even if they have not been consumed within the school walls.) Schools do have competence and a set of appropriate measures for investigating and sanctioning breaches of discipline. He who exercises the disciplinary powers may act against cigarette alcohol and drug consumption and at least with apparent legality may interfere much more profoundly with students' privacy than

would be permissible for an institution of tuition and education. Experience shows that public education institutions extend methods of proof to the extreme in the disciplinary proceedings, engaging in quasi investigative action, but the employment of such methods may even come to be detached from the conduct of disciplinary procedure. The legal rule does not expressly prohibit such quasi-investigative action. We may rightly protest to the use of such means in this kind of context, arguing that such tasks and means are reserved by law for other bodies and authorities, and are regulated by procedures which provide appropriate guarantees to shield personal liberty. Such an argument, however, is difficult to assert in practice because schools tend to regard the fight against smoking, alcohol and drugs – often in agreement with parents – as a noble aim, and the argument rests on principles rather than specific legal provisions.

Positive law offers only one single means for the protection of privacy: the regulations which protect personal data, and these regulations protect data relating to smoking, alcohol and drug consumption as sensitive data. Schools as we have mentioned, employ preventive checks. Examples include teachers examining students' clothing and bags for prohibited substances, or the school conducting drug testing, whether by its own employees or by requiring students to present medical certificates proving their freedom from drugs. According to the data protection rules the institution is processing sensitive data in these cases and such data may be processed.

Only on authorization by a legal rule or with the data subject's consent. Such steps lack a legal ground, however: there is no authorization by legal rules, while voluntary consent – voluntariness being a precondition of the validity of consent – is excluded since in the kinds of cases under consideration

students always risk some disadvantage if they do not cooperate. Nor do school regulations create an appropriate legal ground, because of the lack of collective approval. By contrast, disciplinary proceedings against breaches of discipline of this kind must be judged differently in legal terms. The school may handle students' data related to disciplinary matters, so the law provides authorization for the processing of these sensitive data.[45] As the acquisition of data qualifies as data processing, it is a different question how such data may be acquired without legal provisions on proof. The lack of such legal provisions, i.e. of regulations for such a procedure, amounts to a lack of guarantees, which opens up the way for abuses and arbitrary restrictions of the fundamental right, which, in turn, places the students completely at the mercy of school staff.

Another reason why schools make efforts to handle investigations of drug consumption and disciplinary proceedings within their walls is that rumours of such problems are likely to be detrimental to their public image. However, recording and registering data relating to drug consumption becomes instrumental in getting the information outside the school walls since police may seize the records of drug screening at any time and may use them as grounds for indicting students. No school has an interest in involving its students in criminal proceedings. Many schools are not aware that not only the recording of information in writing but mere testing for drugs qualifies as data processing.

45 Supplement 2. to the Public Education Act, Paragraph 3 beginning with a dash, 1.d).

4.2. CORRESPONDENCE IN CLASS

Students often "correspond", i.e. send little written messages to each other, in class. When teachers take these messages from students, they are in effect, intruding into students' privacy. Paragraph 59, Section (1) of the Constitution provides protection for privacy including the confidentiality of letters, which is confirmed, albeit with some imprecision, by the Public Education Act.[46] Paragraph 178 states the content of, and the guarantees for, the protection of the confidentiality of letters, when it provides that anyone who obtains, opens or passes on to someone without appropriate authorization a closed parcel containing a message addressed to someone other than either of those involved, is to be punished. Letters sent by students during class are not the kinds of closed parcel intended by the Criminal Code, so the teacher's measure taken against them is not prohibited by the Criminal Code. When, however, a teacher seizes an informal letter of this kind, looks at it, perhaps reads it out before class for educational purposes, he/she may gravely intrude into students' privacy.

Sending messages during class, being disruptive of orderly teaching activity, qualifies as a breach of obligation on the part of the student. The teacher has both a right and an obligation to give classes so we cannot deny him/her the right to stop correspondence during class. The measure chosen to do this however must be the mildest possible. It may occasionally go as far as seizing the student's letter. This measure may of course be combined with some sanction, disciplinary step or punishment against the student who has reneged on his/her obligation. The

46 Paragraph 10, Section (3) e) of the Public Education Act states that a student is a subject of personality rights, of the right to privacy, and thus of the right to the confidentiality of letters, which is included in the more general entitlements. Paragraph 11, Section (1)) states the right to correspondence, a legal category which is difficult to interpret in terms of school life, but we may suppose that it is closely associated with the idea of protecting the confidentiality of letters.

two kinds of legal consequence cannot be conflated however: the student must not be punished by violating his/her human dignity, personality rights and his/her right to the confidentiality of letters, and thus the student's conduct must not be sanctioned by destroying the letter, reading it silently or out to the class. As we have just seen, the law provides no express protection for the student, it is yet again the legal rules of data protection that provide positive legal protection for students' rights. If the teacher reads such a message, or reveals its content to others by reading it out publicly, or destroys it, he/she is processing, disclosing or erasing data. This amounts to unlawful data processing because the student's breach of obligation does not create a sufficient legal ground for these steps.

4.3. DATA DISCLOSURE AND PUBLICATION FOR PURPOSES OF SANCTIONING AND EDUCATION

Supplement 2 to the Public Education Act provides that data relating to the assessment of students' conduct, diligence and skills may be disclosed within the class to which the students belong. This provision, as is easy to see, serves the purpose of securing reasonable conditions for delivering assessments by e.g. announcing aloud the mark given before the class. The presence of the class may also assume the function of a guarantee. The Public Education Act, however, – as we have seen – does not define the purpose of data disclosure so the school staff – on a literal interpretation in default of a better one – may easily come to the conclusion that it is lawful to disclose assessment data before the class for the purpose of humiliating a student, or for the purpose of providing encouragement, which has humiliating side

effects. This misunderstanding can only be removed by a more circumspect definition of the legal ground for data disclosure.

The occasional practice of disclosing data relating to students' conduct, diligence and skills not only to the class community concerned but also to a wider circle of persons, e.g. the entire school community is a different question. Examples include posting documents relating to disciplinary measures taken by the school or punishments on the school information board, or reading them out in the school radio. The school may do this only with authorization by a legal rule or on an appropriate legal ground for data disclosure. Disclosing data about a student which are seen as favorable by the processor but may be seen as less favorable by the data subject (e.g. announcing a particular student's having come third at a school contest) are to be judged in the same legal terms. Such data being positive or negative to the student depending on the way he/she perceives them, it is up to the student to decide whether he/she wishes to make them public. That is how the right to the protection of personal data is a right to self-determination: data may be handled or disclosed with the subject's consent. With data which are viewed as negative by the subject the condition of voluntariness is unlikely to be met, and when the disclosure of data serves the purpose of sanctioning, the student's human dignity may be offended.

For similar reasons, it is not lawful, without legal authorization, for teachers to disclose assessments publicly at the parents' meeting. In so doing, they may disclose these data to parents who have no entitlement to know them. The words in the fourth Paragraph beginning with a dash under 2. of Supplement 2., according to which data relating to conduct, diligence and progress, may be disclosed to parents should not obviously be understood to refer to all parents.

4.5. THE POLICE OFFICER IN THE SCHOOL

Police officers are legally entitled to act in schools as in any other public places. This together with police practice as it is at present may put students and parents at policemen's mercy and may lead to severe infringements of rights. The Police Act does not prescribe that a police officer should behave differently toward a child than toward a person of age. A police officer may take measures in a school in the same way as he/she may do at a place of entertainment, with the only restriction that the place being a place which does not qualify as a private apartment he/she is supposed to act with due respect for the institution's own regulations, if possible.

When seen in light of the priority of the protection of students' rights, it will not seem sufficient for police to act in accordance with the principle of aim dependence and with the principle of respect for the working order of the institution: it must be held that police may take measures in schools only under exceptional circumstances. The mere demand for information is no reason in support of information acquisition within a school. The orderly functioning of teaching and education is necessarily disrupted by the presence of a police officer taking measures. It is therefore to be allowed only in cases where police have no other means to resort to.[47] If, for instance, a student is to be interrogated by police, serious harm may result from police contacting the student in the school. Imagine a police officer turning up in the school, the student being called to the director's office, then carried away in a police car before the eyes of all the other students watching through the window. Whenever this happens, the student's rights are violated as a result of the scene chosen for the police action.

47 Andrea Pelle, School and Police, Working Paper prepared by HCLU.

There is therefore a need for a rule which would make it clear that police may take action in schools only under exceptional circumstances, a rule that would make police action in schools conditional on a clear need to avert direct and present danger in the school building or to investigate crime committed in the context of the institution's ordinary functioning. This would be further constrained by limiting police action during teaching time to cases in which delay would involve disproportionate harm.

Most of the real problems arise at the level of practice rather than of legal regulation. The school is a good field for police investigation, but the practical problems arising out of this form part of the question of the legality or otherwise of police proceedings rather than data processing at school. Police often wish to resort to the method of total data collecting, seizing all logbooks with all the students' data, or check the identity of all students. Such proceedings are to be prevented by regulations relating to the work of the police or a change in police attitudes rather than by the public education institution or regulations pertaining to it. As long as police proceedings are viewed as an area outside all procedural law, the Police Act makes no distinctions in terms of the age of the persons involved or the scene of the proceedings. As long as the only restriction placed on police proceedings remains the principle of proportionality, police may easily slip into the error of subordinating the rights of the persons involved to considerations of convenience.

ISBN: 963 206 619 7

Layout by Pál László

Copies are available from HCLU's office

H-1114 Budapest

Eszék utca 8/B. fszt.2.

Tel-Fax: (361) 209 0046

tasz@tasz.hu

www.tasz.hu