

INFORMATION MANAGEMENT: LEGAL AND SECURITY ISSUES

Andrzej Adamski

1. Introduction

This section discusses the legal protection of information and the security issues of computer data and electronic information systems and is organised into four parts: First, it focuses briefly on the basic conceptual distinction between information and data, providing a basis of understanding of the primary object of legal and technical means of protection. Second, access to Government information will be discussed. Third, protection of personal data in the administration of criminal justice will be presented. Finally, security of data and network communications will be explored.

2. Information and Data: Legal Protection of Information and Data

2.1 Information and Data

Data is a formal representation of concepts, facts or instructions. Information is the meaning that data has for human beings. Data has, therefore, two different aspects: as potential information for human beings or as instructions meant for a computer.

Information is not material, but a process or relationship that occurs between a person's mind and some sort of stimulus. Information, therefore, is a subjective notion that can be drawn from its objective representation which we call data.

Different information may be received from the same data. As in the various natural languages the same word may have different meanings, so in computer programming the same byte or set of digits (e.g. 01100010) may serve as a carrier of different content.

2.2 Legal Protection of Information and Data

The new legal doctrine of information law and law on information technology recognises information as a third fundamental factor besides matter and energy. This concept realises that modern information technology alters the characteristics of information, especially by strengthening its importance and by treating it as an active factor that works without human intervention in automatic processing systems. In this new approach, it is obvious that the legal evaluation of corporeal and incorporeal (information) objects differs considerably.

Information, being an intangible and an entity that can be possessed, shared and reproduced by many, is not capable of being property as most corporeal objects do. Unlike corporeal objects, which are more exclusively attributed to certain persons, information is rather a public good. As such it must principally flow freely in a free society. This basic principle of free flow of information is essential for the economic and political system, as indispensable for the government's accountability and the maintenance of a democratic order.

A second difference between the legal regime of tangibles and intangibles is that the protection of information has not only to consider the economic interests of its proprietor or holder, but at the same time must preserve the interests of those, who are concerned with the contents of information - an aspect resulting in new issues of privacy protection.

A third difference originates from the vulnerability of data for manipulation, interception and erasure - proprieties that constitute a major concern of computer security, and the criminal law provisions on computer crime.

3. Access to Government Information

3.1 From Secrecy to Openness

In most countries, the disclosure of government documents is largely discretionary. Government agencies, at both the central and the local level, are rarely forthcoming with information unless it is in their interest. There are no general laws that provided a mechanism for public access.

Generally, access to government information can be defined as the availability for inspection or copying of both records and recordings, possessed or controlled by a public authority. This mechanism came, for the first time in history, in the eighteenth century Sweden with the passage of the Act on Freedom of the Press (1766). After 1945 this regulatory approach was followed in other Scandinavian countries, in the United States (since 1996, when the Freedom of Information Act was enacted), and in several other countries. Among these are Australia, Canada, France, the Netherlands, and New Zealand. Some other countries have constitutional clauses relating to a right of access, but not always transformative legislation¹.

The route by which the promotion of the rights of access to official information has become a strong political issue is varied. Initially, the public's right to government information had been found to be closely related to the concept of human rights. Because of its importance for democratic society, the public's right to information was even acknowledged to constitute a third generation of human rights, after the civil and political rights of the eighteenth century, and the economic and social rights of the first half of the twentieth century. As it was stressed in the Council of Europe Recommendation on "Access by the Public to Government Records and Freedom of Information": "A parliamentary democracy can function adequately only if people in general and their elected representatives are fully informed"².

The most recent emphasis, however, is on the commercial rather than human rights aspect of public sector information. There is now a widespread recognition by the private sector of the commercial value of much government information. Large data sets, as land registers, company registers, demographic statistics, and topographic information (maps) are routinely produced as a by-product of the day-to-day functioning of public administration. Information is not an end in itself. Sound and comprehensive information is needed if government is to frame workable public policies, plan effective services and distribute resources fairly and equitably. Government information, therefore, constitutes a resource of considerable importance. The potential of such data for exploitation via the digital network was noted and encouraged.

3.2 Impact of Computerisation

Over the 1970s and 1980s, when computerisation of public sector information systems in the most developed countries was in its infancy, there were fears that government agencies would use computerisation as a technology of secrecy rather than a technology of freedom.

¹ Constitutional provisions relating to a general right of public access to official information are to be found in Austria, Belgium, Estonia, Finland, Hungary, the Netherlands, Portugal, Romania and Spain.

² Council of Europe, Recommendation on "Access by the Public to Government Records and Freedom of Information", 1 February 1979, No.854 (1979).

In fact, in some countries computerisation of government information had a strong impact on the way the right of public access has been interpreted by the authorities. For example, when new programming was necessary to extract information from computer systems, agencies and courts have sometimes held that such programming is analogous to record creation, and is therefore not required under the freedom of information laws, which only oblige to search for available records³. There is a common feature of these laws to grant access only to information which is available or can be made available through reasonable effort.

As electronic records became more common, the freedom of information laws proved to be less useful in the new environment. Because the wording of these laws usually provide access to paper records, an authority was not obliged to accommodate a requester's preference for access in an electronic form, for example a copy on computer tape or disk. There are well known, especially in the United States, cases of the Government's agency refusal of making computerised records available to the party concerned in their access⁴.

Today, in the United States these definitional problems have successfully been solved. With the adoption of the Amendments Act on Electronic Freedom of Information of 1996, the Government information maintained in electronic format has become accessible to the public on an equal footing with paper-based documents. Though, there are still some national legislations that do not allow requesters to obtain data in machine-readable format⁵, the process of commercialisation of the public sector information is a present development both in the United States and most countries of Western Europe. Moreover, due to the traditional concept of the right of access, as a right to request the handing out of identified documents, the right to search for documents has so far not been a recognised part of the principle of public domain.

In view of the fast growing information networks, the powerful search engines, and, generally speaking, the retrieval possibilities of electronic information increase the significance of search rights as an integrated element of the traditional right of access.

New developments in hardware and software technology, as relational databases and hypertext, not only enhance computer flexibility and responsiveness to unanticipated form of requests, but also make it easy to compile and format information for network access. The cost in money and effort to share information is much lower. As a result, public access to government information can be enhanced.

The most recent event illustrating the tendency of making legal text databases freely available to citizens is a decision of the Swedish parliament to make its on-line legal information service (Rixlex) available to the public on a free of charge basis via the Internet.

³ "The Freedom of Information Act in the Electronic Age: The Statute is Not User Friendly", J.A. Grodsky. *Jurimetrics Journal*, 19, 1990

⁴

_In the case *National Security Archive v. CIA*, a public interest research group requested an index of previously released records by the CIA under FOIA. The plaintiff group asked for the data on a computer tape or disk so that the information could be scanned electronically more quickly than on paper. The agency refused, and instead it produced a 5,000 page print-out that made a stack three and a half feet, or about a meter, high. While the group argued that the size of the print-out made analysis practically impossible, the court held that the CIA had provided the information in a reasonably accessible form, and dismissed the complaint.

⁵

_The Swedish Act on Freedom of the Press states that an authority shall be under no obligation to make a recording for electronic data processing available in any form other than transcript, a paper print-out. The official reason for this restriction is to prevent the provided electronic copies from being used for any unauthorised data registration that leads to an invasion of personal integrity.

To facilitate this tendency, government information should be exempted from the copyright protection. For instance, the United States Copyright Act of 1976 explicitly provides that copyright protection is not available for any work of the United States Government⁶. Article 4 of the Polish Copyright Act of 1994 excludes legislative acts, their official drafts, and other official documents and materials from the copyright protection. A number of other countries have adopted similar regulations⁷. The significance of the limitation on copyright for government information policy was not always appreciated, but its importance became clearer in recent years as digital data became commonplace. It simply implies that government information is public domain. Anyone may reprint a government document in any way and at any price. Any government data made public also may be used in any on-line information service without restriction.

3.3 Openness vs. Secrecy

Public access to official information does not prevent the Government from protecting information from disclosure for their legitimate aims as stipulated by legal provisions.

In the United States, nine exemptions permit the withholding of records to protect legitimate government or private interests. Thus, national security information, trade secrets, law enforcement investigative files, personal data, pre-decisional documents, and other categories of government records can lawfully be denied to a FOIA requester. The early experience under the Act on Freedom of Information shows some negative consequences of this legislation for effective law enforcement. It was estimated that only 7 percent of the 30,000 FOIA requests received annually by the Department of Justice came from media and other researchers. Many requests came from persons who were obviously seeking improper personal advantage, including convicted offenders, organised crime people, drug traffickers, and persons in litigation with the United States who are attempting to use the FOIA to circumvent the rules of discovery contained in the rules of criminal or civil procedure. Consequently, the ability of the federal, state, and local governments to combat crime was thought to be affected, mainly by a decline in the number of informants⁸.

A highly detailed Swedish Secrecy Act contains 16 chapters and more than a hundred articles. They provide a specific requirements of damage to the interest concerned, as well as a maximum period of time during which secrecy applies. For example, where the protection of personal circumstances of individuals is concerned, usually a term of 50 or 70 years is applicable. With regard to secret information on matters of national defence or foreign relations a maximum period of 40 years has been established. In principle the restrictions laid down in the Secrecy Act are mandatory in nature, i.e. if a restriction applies the authority involved must refuse access.

The legal nature of the restrictions based on secrecy interests differs among the various jurisdictions. In the United States of America, Denmark and France for example the limitations are not mandatory as is the case in Sweden and the Netherlands but are discretionary in nature. This means that if a restriction is applicable, the public authority concerned is under no obligation to give access to the information, but is nevertheless entitled to do so. Under

6

United States Copyright Act, §105 (1994). The prohibition on copyright protection for United States Government works is not intended to limit protection abroad. Thus, under the Copyright Act, the Federal Government can seek copyright for its information of other countries.

⁷ In Germany and Switzerland, for instance, legislation and jurisprudence is not copyrighted. The Italian law explicitly bars statutes, regulations, rulings and the like from being copyrighted by Italian Government, local authorities or a foreign one. In Turkey, legislation and jurisprudence are not copyrighted as far as they are published officially (Law on Intellectual and Artistic Works, No. 5846, art. 31). Speeches are not copyrighted in the scope of mass communications, otherwise they are copyrighted (art. 32). All other governmental works, such as reports, plans, maps, drawings etc. are copyrighted.

8

Report of Attorney General's Task Force on Violent Crime of 17 August 1981. United States Department of Justice.

the Canadian Act on Access to Information the general rule is that exemptions are discretionary. There are, however, five mandatory exemptions in the Act that require the public authority involved to claim an exemption for certain types of records. The mandatory exemptions relate to information that was obtained in confidence from the government of a foreign state or from an international organisation of states, personal information as defined in the Privacy Act, trade secrets of a third party, financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party, and information the disclosure of which is restricted by or pursuant to specific other statutes.

The mandatory nature of these exemptions is set aside in certain circumstances, in which the public authority may disclose the information. First, this applies if the organisation from which the information was obtained or the person to whom the information relates consents to the disclosure. Secondly, personal information under the control of a government institution may be disclosed even without the consent of the individual to whom it relates if the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure. Thirdly, financial, commercial, scientific and technical information that is confidential, may be disclosed if such disclosure would be in the public interest as it relates to public health, public safety or the protection of the environment and, if such public interest in disclosure clearly outweighs in importance any financial loss or gain to, prejudice to the competitive position of or interference with contractual or other negotiations of a third party. The exemptions concerning international affairs, defence and national security, law enforcement and investigations, safety of individuals, economic interests of Canada, and deliberative documents are discretionary.

From the above review it becomes clear that the right to access public information remains in conflict with other social values and interests such as the efficiency in Government and the right to privacy. The reconciliation of these opposing values and interest should be provided by the legal instruments and can take different procedural forms, depending on the legal and constitutional system of the country concerned. Among legal tools available to protect private interests in confidentiality there are data protection laws that appeared in most western legal systems in response to new challenges to privacy caused by expanded possibilities for personal data processing by new technologies.

4. Data Protection in Computerisation in Criminal Justice

Computerisation of criminal justice has far-reaching implications for human values that are involved in the automatic processing of personal data. The fears that computerisation of criminal justice is able to induce are mainly related to the potentials for over-control of individuals, including the possible breaches of their privacy through misuse of sensitive data about them recorded in computer files:

1. An application of increasingly sophisticated information gathering devices for surveillance activities may reduce the individual's sense of security and liberty;
- I Accumulation of personal data in various databases connected throughout computer networks would make possible the creation of personality profiles or so-called computer shadows of the data subject;
- I Susceptibility of computerised information systems for an unauthorised access to data stored and their possible abuses have constituted another cause of concern;
- I Use of information provided by centralised computer systems on large sectors of the population who have no opportunity to inspect the accuracy of the information held, may also affect the legal position of the data subject in a way being harmful for their civil liberties.

4.1 Data Protection Legislation and International Standards

With information technology an individual may become transparent for the data controllers. To prevent such a possibility data protection legislation has been initiated in several countries. For the first time in Sweden (1973), and subsequently in over 20 other countries of Western Europe, North America and Australia. The underlying idea of protection of personal data is to reverse the above tendency and make it possible for the individual to exercise control over the one's own data that is collected and used by others. There is a positive feedback between the national legislation

in privacy and protection of personal data and the number of international and regional instruments in this field⁹. A recent document, that has addressed these issues to the entire international community, is the 1990 United Nations General Assembly resolution 45/95 on Guidelines for the Regulation of Computerised Personal Data Files.

The Guidelines contain eight principles which apply to handling those files, and constitute the minimum standards to be provided in national legislations:

- I Principle of lawfulness and fairness,
- I Principle of accuracy,
- I Principle of purpose-specification,
- I Principle of interested-person access,
- I Principle of non-discrimination,
- I Principle of security,
- I Principle on sanctions and supervision of the observance of the above principles,
- I Principle on transborder data flows.

— The following section seeks to explain as how the above principles may apply to the operations of the criminal justice authorities.

4.2 Data Protection Principles in the Administration of Justice

4.2.1 Principle of Lawfulness and Fairness

The principle of lawfulness and fairness in the collection and processing of personal data for criminal justice purposes implies that data must be obtained in a lawful way, i.e. in compliance with procedural rules which define the limits of permissible intrusion by agents of the state against private interest of the citizen.

It is not easy to comply with this requirement in the information age. Legal provisions on the inviolability of telephone communications may not provide sufficient basis for the protection of confidentiality of an e-mail and other forms of electronic communications. The rise of electronic surveillance and the use of computers to data matching and sort, for instance, conversation intercepts have developed so fast, that the legal system may not be able to respond adequately to situations created by these new techniques.

⁹ The right to privacy has been recognised by the United Nations Universal Declaration of Human Rights (art. 12), the European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 8), and the International Covenant on Civil and Political Rights (art. 17). Privacy protection by means of data protection is dealt with, at the international level, by: Recommendation with Guidelines on the protection of privacy and transborder flows of personal data adopted by the Council of the Organisation for Economic Co-operation and Development on 23 September 1980; Council of Europe Convention No. 108 for the protection of individuals with regard to automatic processing of personal data, adopted 28 January 1981; Directive 95/46/EC of the European Parliament and of the Council of Europe 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 (EU-Data Protection-Directive); General Agreement on Trade in Services, stating in Article XIV that Member States are not prevented by this world wide agreement to adopt or enforce regulations relating to the protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

Nevertheless, the encroachment on privacy which these investigative methods and procedures involve and the possibilities for abuse inherent in their use require that they be closely defined.

As to telephone tapping, or other forms of electronic monitoring, the balance between the interest of criminal justice and the privacy protection of individuals requires that the use of technical surveillance should be explicitly provided by law:

- I As an exceptional measure, employed in certain restricted, most serious crimes;
- I Targeted only on the person who is suspected, on reasonable grounds, of having taken part in a crime;
- I. Provided that the monitoring has been duly authorised by the court or an organ of judicial investigation.

Specific provisions should also govern the duration of monitoring, the manner it is carried out, and the processing of the information obtained.

A detailed regulation of conditions on the use of surveillance provides necessary grounds for the subsequent supervision over the police undercover activities. In several democratic states such a supervision is carried out by an independent public body (e.g. special parliamentary commission), appropriately empowered to check, in any case involving monitoring, whether the police is acting in a lawful way. This, however, requires that the police be obliged to report regularly on such cases to the supervisory authority, which should also be entitled to look into the cases at its own initiative or at the request of individuals who believe they are under surveillance.

Once monitoring is over, and unless this would not prejudice the outcome of the investigation, the person concerned should be informed that monitoring has taken place. Then, he or she should be given an opportunity to examine the recordings made without his or her knowledge as well as to take legal action thereupon.

The report on the monitoring and recording should be destroyed if irrelevant, or no longer relevant, to the investigation.

4.2.2 Principle of the Purpose-Specification

4.2.2.1 General observations

The principle of purpose specification impose two kinds of limits on processing of personal data:

- I. It prohibits the collection and processing of data for undefined purposes;
- I. It permits to keep only personal data files that concern the legitimate objective of activity of the data controller.

It also implies that the purpose justifying the creation of a file should not only be specified before it is set up, but also made known to the supervisory authority (Personal Data Inspector/Commissioner) in order to enable him registration of the file.

A notification of supervisory authority should concern so-called permanent files (databases), which are used by the police for their routine purposes. This notification may not apply to ad-hoc files set up for the purpose of particular investigations. The supervisory authority should be informed by the police agency about the nature of each file declared, the body responsible for its processing, its purposes, the type of data contained in the file and the persons to whom the data are communicated.

The notification procedure makes it possible, at any time, to check, whether:

- I. The collected and recorded data are in keeping with the purpose sought;
- I. The data are not used for a purpose other than for which the file was set up;
- I. The data are held on file no longer than is normally required for the purpose for which they were collected.

4.2.2.2 Restrictions of data collection

Crime data constitute a highly sensitive category of personal information. For this reason, their collection and processing by any private or public body other than the criminal justice agency of the State is usually prohibited in those countries who have adopted data protection laws. Exceptions are only made, if it can be shown that there are special or extraordinary reasons for gathering data about persons who have committed crimes (e.g. for the purpose of scientific research). This implies, inter-alia, that any authorisation may not be given to private investigators or trade companies for setting up data banks on lawbreakers or shoplifters, since the maintenance of such registers outside the criminal justice system has no legal reasoning.

4.2.2.3 Data matching

According to the principle of purpose specification, the use or disclosure of personal data for purposes other than originally specified is not allowed unless the data subject consents. This requirement reflects the essence of the right to self-determination. It may, however, be exempted in the public interest, such as the prevention and investigation of crime. As the United States Guidelines stress, such departures should be „expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards” (guideline 6).

Consequently, the police on-line access to personal databases set up in other sectors of public administration should meet this condition. This is the case in some Western European countries (e.g. Denmark, Germany, the Netherlands) where the integration of police files into a network and their combination with existing files of public institutions is expressly permitted by the law. Moreover, in most of these countries police investigation by computer-screening is subject to supervision and approval of administrative (e.g. Denmark) or judicial (e.g. Germany) authorities¹⁰.

4.2.2.4 Third party access to criminal records

A disclosure of personal data to the third party - not embraced by the original purpose of the data controller - is an important issue in the context of third party access to criminal records¹¹. The criminal record system is not only intended to assist the judicial authorities in decision-making in individual cases, but also provide information for statistical and research purposes. Furthermore, it may serve as a source of useful information for other parties. The press, professional organisations, licensing authorities and employers are among those parties who most frequently seek to take advantage of information contained in this record. In a number of countries all of these parties are entitled to ask to be given extracts from criminal records, while in other countries only few of them are authorised to do so.

With a strong emphasis upon rehabilitation of offenders in the modern criminal policy, a visible tendency towards limiting the access of the third parties to the criminal records has occurred in many legal systems. The disabilities flowing from a record of conviction or arrest have been well documented by criminological research. A social stigma involved in these records makes it difficult for the convicted or arrested person to find a job, and this in turn prevents rehabilitation and may lead to recidivism.

¹⁰ See: "Special Methods of Investigation for Combating Organised Crime", W. Gropp. European Journal of Crime, Criminal Law and Criminal Justice, no.1, 1995.

¹¹

By the criminal records is meant any register of criminal decisions made in individual cases in the course of criminal proceedings, irrespective of what criminal justice authority is responsible for keeping it.

Accordingly, the principle of restriction of the use of criminal records has been set forth at the international level¹². This principle states that information in criminal records should only be communicated in the form of extracts and contain data indispensable for the legitimate interest of the recipients. However, application of this rule is recommended only to public organisations and employers. As to the private employers and other recipients outside the public sector, their access to the criminal record (even in an abbreviated form) should be restricted to the utmost. The same can be said about the communication of decisions relating to minors. As the United Nations Standard Minimum Rules for the Administration of Juvenile Justice state: "Records of juvenile offenders shall be kept strictly confidential and closed to third parties. Access to such records shall be limited to persons directly concerned with the disposition of the case at hand or other duly authorised person" (rule 21).

However, recent developments in making criminal history record information available to third parties are less restrictive for them. In the United States, for instance, some professional groups when applying for job are obliged to submit fingerprints in order to check whether they have been arrested or convicted for crimes that might make them unfit for a given employment¹³.

4.2.3 Principle of Non-Discrimination

The collection of specific categories of data about persons dealt with by the police shall be severely restricted, even prohibited in so far as they may have discriminatory effects for civil liberties of data subject in the legal and sociological context of the country concerned. According to Western European standards, even the police should not be allowed to collect data on individuals solely on the basis that they have a particular racial origin, particular religious belief, sexual behaviour, or political opinions or belong to particular movements and organisations which are not proscribed by law¹⁴. Police authorities should neither set up any personal indexes based on these factors nor record data relating to them on permanent files. Insofar as this highly sensitive data are absolutely necessary for the purposes of particular inquiry, they may only be recorded in ad-hoc files.

4.2.4 Principle of Accuracy

Poor criminal justice data quality leads to two problems:

- I. First, individual rights may be violated by the use and dissemination of inaccurate data;
- I. Secondly the effectiveness of criminal justice administration may be diminished.

Errors in automatic data processing may also have cumulative effects, and may spread to other information systems through the links that exist between them.

The interest of an individual requires that all data concerning him which are based on judgements, assumptions or personal assessments should be distinguished from hard or factual data and kept separate from the main file, so as to prevent the former category from dissemination. In the event of communication, such data should be checked at source

¹²

— Recommendation of the Committee of Ministers of the Council of Europe No. R(84) 10 on the Criminal Record and Rehabilitation of Convicted Persons, (in:) The criminal record and rehabilitation of convicted persons, European Committee on Crime Problems, Strasbourg 1984.

¹³ "Change at the Speed of Light: Doing Justice in the Information Age" J.D. Coldren. Computerisation in the Management of the Criminal Justice System: Proceedings of the Workshop and the Symposium on Computerisation of Criminal Justice Information at the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Cairo, Egypt, 29 April - 8 May 1995 (R. Scherpenzeel, ed.). HEUNI Publication Series No. 30, Helsinki/The Hague, April 1996.

—

¹⁴ Council of Europe Recommendation No. R (87) 15 of 17 September 1987 regulating the use of personal data in the police sector.

—

and their degree of accuracy or reliability indicated.

Once computerised, information is particularly vulnerable to a long term storage: inputting is swiftly, whereas updating and selective erasure may be time consuming. Even so, it is desirable that all records in a file should be updated regularly.

As a general rule, data should not be stored in a form permitting identification of the data subject for longer period than necessary to accomplish the purpose for which they were recorded. Data processing techniques may facilitate the compliance with this requirement through the automatically deleting of outdated entries from the computer records.

On the other hand, the storage of data in the police permanent files insist upon regulations similar that govern deletion of criminal records. The advantages that the use of permanent automated files may have for the effective law enforcement are undeniable. Nevertheless, the data contained there cannot be held forever and must be open to the verification and erasure. Therefore, these data should also be open to the data subject.

4.2.5 Principle of Individual's Access

4.2.5.1 General observations

The right of access of the interested person to his or her files constitutes one of the central requirements of any data protection law. This right is composed of several elements:

- I. The right to know the existence of the file;
- I. The right to know the information;
- I. The right to rectification and erasure of wrongly stored data;
- I. The right to a judicial remedy if any of the aforementioned rights are infringed).

The right of individual access is perhaps the most difficult right to implement and secure. Especially in those sectors of public administration as the administration of justice, where the balance between openness in government and the government's responsibility to protect citizens from crime is delicate and unlikely to be accomplished once and for all. Even so, the harmful effects that inappropriate or inaccurate crime-related data may have on data subjects, require that their right of access to personal information be granted and its upholding stringently be monitored. According to the European standards, departures from this rule may apply to the police files, but are inadmissible with regard to criminal record information.

4.2.5.2 Access to the police files

In the Council of Europe recommendation No. R (87) 15 of 17 September 1987 regulating the use of personal data in the police sector, three general exceptions from the right of access are specified. The access may be denied, if it is likely to be prejudicial to the performance of a legal task of the police, the protection of the data subject's own interests or the rights and freedoms of others.

All the information that is given as confidential by a third party should be treated as such and not made accessible to the person concerned without the consent of the individual or agency supplying the information. Police authority should in particular be entitled to deny access whenever this would involve revealing the identity of their informants. The right of access should also be denied if the file contains information about health or development of the personality of the data subject that would negatively affect him.

4.2.5.3 Access to the criminal record

As oppose to police files, access of the person concerned to his/her criminal records should not be restricted in any form. Any person, proving his identity may be shown, by applying to the appropriate judicial authority, a list of all entries concerning him in the criminal records. However, no copy of such a list should be issued, so as to prevent the possible pressure on an individual which employers or other private persons not entitled to obtain extracts from the criminal record would exert on him in order to obtain it through the person concerned¹⁵.

¹⁵ As the Recommendation No. R(84) 10 of the Council of Europe put it: „ to avoid written communication of the record, in order to prevent any

4.2.6 Principle on Supervision and Sanctions of the Observance of the Above Principles

Data protection can be guaranteed only as long as the conduct of those who process data can be adequately supervised. Based on this assumption, two control mechanisms contribute to any scheme designed to afford individual's rights protection in this area:

- I. A supervisory authority, a largely independent public body, responsible for ensuring respect for the data protection principles;
- I. Appropriate sanctions and remedies for violation of these principles.

The main tasks of a supervisory authority (e.g. data protection ombudsmen/ commissioner or data inspection board), established outside the criminal justice system, usually include:

- I. Maintenance of a public register of automated personal data files and their inspection;
- I. Regular announcement (e.g. once a year in the government gazette) of the existence of all permanent automated files held by the police as well of their ad hoc files, where appropriate;
- I. Promotion of the public awareness of its rights in regard to these files;
- I. Investigation of complaints from individuals whose rights to access, obtain rectification and/or erasure of one's own data were denied by the police authority.

Both criminal sanctions and civil remedies are employed by the national data protection laws for violation of their basic principles. Improper handling of personal data by its user (e.g. without registration of a file or the permission of person concerned for a disclosure of data) frequently constitutes a criminal offence. If a data user refuses to permit access, the data subject is usually entitled to take judicial action and apply for a disclosure or rectification of his/her personal data to a court. A claim for compensation for data inaccuracy and related damage is another civil law remedy.

4.2.7 Principle on Transborder Data Flows

The United Nations Guidelines provide that „...when the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitation on such circulation may not be imposed unduly and only in so far as the protection of privacy demands”.

The very similar recommendation provides the data protection directive of the European Union of 25 October 1995¹⁶ stating that personal data could be transferred only if the third country „ensures an adequate level of protection”. The third country provision illustrates the difficulty of maintaining personal data protections when other jurisdictions do not have similar laws or practices. A term sometimes applied to the third country that deliberately avoids having privacy regulations is a data haven. If personal data from a country with privacy regulations can be freely transferred to a data haven with no privacy rules, the legal protections available in the source country may be lost. The controller in the data haven may have no legal obligations or restrictions on use, and the data subject may have no enforceable rights.

None of the international privacy instruments directly recognises current computer network technology. The Guidelines of the Organisation for Economic Cooperation and Development and the Convention of the Council of Europe were adopted long before computer networks were commonplace. The United Nations Guidelines and the European Union data protection directives are more recent, but they too fail to address network issues. Technology simply overwhelmed some traditional approaches to privacy protection and some legal assumption upon which the approaches rely.

Data protection on the Internet is even a more complex issue. Sensitive personal data can be communicated from sites located in countries without any privacy legislation where they can be accessed from all over the world by a simple mouse click. Even a casual connection through a World Wide Web page can produce a remote record of an inquirer's electronic mail address and the subject of the inquiry¹⁷. The use of the Internet for the publication of search warrants by the police or lists of wanted suspects (as it is practised by the United States Federal Bureau of Investigation) has already faced criticism due to the deficiencies in the authentication procedure and the easy manipulation of pictures in Cyberspace¹⁸. There is, however, one thing to be clear: the Internet does not exist in a legal vacuum. Therefore, providing information on the Internet is subject to the national data protection laws and regulations.

5. Security of Data and Computer Network Communication

Below some basic aspects of computer security in networked environment are outlined¹⁹. Main topics addressed are the threats for confidentiality, integrity, and availability of network communications and their countermeasures.

5.1 Trends: The Growing Potential for System Abuse

¹⁶ European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data of 25 October 1995.

—

¹⁷

— Most servers log every access. The log usually includes the IP address and/or host name, the time of the download, the user's name (if known by user identification), the URL requested, the status of the request, and the size of the data transmitted.

¹⁸

— See: "Data Protection on the Internet, Report and Guidance", "Budapest Draft", International Working Group on Data Protection in Telecommunications, 21 May 1996. Journal of Information, Law and Technology (JILT), issue 3, 1996. <<http://lrc.law.warwick.ac.uk/elj/jilt/consult/iwgdp/default.htm>>.

¹⁹

— A comprehensive overview of computer security measures is provided by the United Nations Manual on the Prevention and Control of Computer-Related Crime, „International Review of Criminal Policy”, Nos .43 and 44, United Nations, New York, 1994, which is also available in an electronic format from the United Nations Crime and Justice Information Network <<http://www.ifs.univie.ac.at/~uncjin/uncjin.html>>.

With respect to computer security, the past is not a good predictor for the future. An enormous pace of the information technology development is a challenge not only for the law makers but to even a greater degree for the computer security specialists. Several trends underlie this assessment:

- I. In the past data was stored on floppy disks that could be locked up if necessary, and information stored in volatile memory disappeared once the machine was turned off. Thus the operating system contained no features to ensure the protection of data stores in the computer.
- I. The introduction of hard disks, which can store large amounts of potentially sensitive information in the computer, introduced new vulnerabilities: whoever turns on the PC can have access to the data and programs stored on the hard disk.
- I. Use of passwords and removable hard disks diminishes such potentials but do not eliminate the corruption of data from a virus or malfunctioning program while the machine is running.
- I. The most damaging change in the operating assumption underlying the PC was the advent of network attachment. External connection via networks has created the potential for broader access to a computer and the data it stores. So long as the computer is turned on, the network connection can be exercised by a remote attacker to penetrate the computer. Computer systems are becoming more open, connected to other systems, or available to authorised users through telephone connections that use dedicated lines or the general public telephone system. Although passwords or other devices can control who can use the computer system, the greater the openness, the greater the vulnerability.
- II. The Internet has the potential to become an even greater threat to computer security than dial-up telephone modems. An Internet connection is unlike those available with dial-up modems, which give one outsider one point of entry into an organisation's computers. With a direct Internet connection, computers in a local network are tied to the Internet, allowing access at any time without resorting to modems. Outsiders, in turn, only need an organisation's Internet address to communicate with its computers. Consequently, an access control has become an increasingly important aspect.
- I. Having the freedom of large, open networks comes at a cost: an inherent lack of communication security. Messages pass through numerous machines on the way to their destination. Currently, sending electronic mail is the equivalent of sending a typewritten postcard in the mail. It theoretically can be read by anyone in the computer link between the author and the recipient and there is also no method to conclusively verify the identity of the message originator.

5.2 Network Communication Security Issues

Data security is commonly held to consist of three properties: confidentiality, integrity, and availability, of which confidentiality is controlling who gets to read information, integrity assures that data and programs are changed only in a specified and authorised manner, and availability assures that authorised users have continued access and resources.

These three requirements may be emphasised differently in various applications. For a national defence system, management concern may be ensuring the confidentiality of classified information, whereas a funds transfer system may require strong integrity controls. The requirements for applications that are connected to external systems will differ from those for applications without such interconnection. Thus the specific requirements and controls for information security can vary.

The availability of the means of storage, processing and transfer of data and these data themselves (including software) is prerequisite for taking advantage from computerisation at large. The importance of uninterrupted access to computer systems increases in proportion to the degree of dependence of a society on information technology. The availability of means and data may be jeopardised by such factors as accidents, power failures or human error, but also by deliberate acts of malevolence such as sabotage, damage, destruction or removal of media and data, or the obstruction or interruption of data communications.

The availability of resources may also be undermined by unauthorised users overloading of the system to such an extent that legitimate users encounter difficulties or are completely prevented from working. This is a form of denial of usage of the media. Denial of usage of data and software can also occur if these are made inaccessible to

legitimate users. An example here would be the unauthorised alteration of passwords giving access to the computer system. Availability has to be effected by procedural measures, such as regular back-ups, recourse to stand-by computer facilities, or regular computer virus checks. In terms of network security, suitable access control checks must supplement this set of measures.

Table 1: Some Basic Aspects of Data and Network Security

Security Attribute to be Protected	Type of Attack	Actual or Potential Damage
Availability	Sabotage, Modification of Data or Programs: introduction of worms and viruses	Denial of Service: preventing authorised access to data and systems, (alteration of passwords) malicious overloading of the system (spamming, electronic mail bomb)
Integrity	Break-in to the System (masquerading, IP spoofing) Reconfiguration (Trojan horses)	Introduction of Incorrect Data, Alterations, Additions
Confidentiality	Unauthorised Access, wiretapping, eavesdropping, interception Unauthorised Copying of Data	Theft of Information, Breach of Secrecy, Privacy, Copyrights Infringements

Confidentiality and integrity play important roles in data transmission and storage. Confidentiality means that no unauthorised person has access to the data. This property is also called exclusivity. Integrity is the certainty that data are unimpaired, i.e. that no one has altered, deleted or added to the data. It is often taken to include authenticity, i.e. certainty about the identity of the sender. Trojan horses, viruses and worms are the most typical attacks on the integrity of data that is stored in systems and communicated across networks. In case of hacking or unauthorised access, integrity of the whole system is at risk. Such events as potentially damaging for all attributes of data security should be prevented by all available means of access control. Three of them: passwords, firewall technology and encryption constitute the first level of defence.

5.3 Passwords

Passwords are the most common means of computer system access control. To be effective in the performance of their function, passwords should be:

- I. Issued to an individual and kept secret;
- I. Separate from the user ID;
- I. Chosen by the user, but restricted to the following format:
 - Alphanumeric and;
 - At least six characters long;
- I. Changed regularly, at least every 30 days;
- I. Removed immediately an employee leaves employment or gives notice of leaving the organisation's employ²⁰.

²⁰ See: "Basic Security Methods", Computer Crime Unit of New Scotland Yard, October 1992.

In view of the ease of tapping transmission lines, or monitoring the local network traffic, one has to recognise that the classical protection with static passwords is in several cases no longer adequate. A clear example is so-called password sniffing, a relatively new type of attack on the Internet which puts at risk even the most carefully chosen passwords. Password sniffers are programs that simply collect the first 128 or more bytes of each network connection on that network that's being monitored. When a user types in a user name and a password, as required when using common Internet services, the sniffer collects that information. Additional programs sift through the collected information, pull out the important pieces, e.g. user names and passwords, and cover up the existence of the sniffers in an automated way²¹. Detection of running sniffers is difficult and for some Unix-systems even hardly possible.

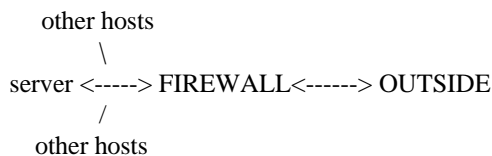
Sniffing attacks can be stopped by the use of one-time passwords or encrypted passwords. One time password technology is card systems where each user gets a card that generates a new password every minute. The use of software that allows encryption between connections make the data captured by the intruder useless²².

5.4 Firewall Technology

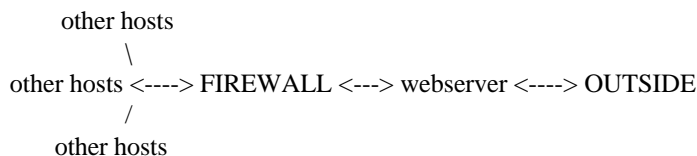
A firewall is one of several methods of protecting one's network from another mistrusted network. It is deemed as absolutely indispensable for the Internet users who are running their own Internet World Wide Web site. The hardware and software that makes up the firewall screens all traffic. The firewall can be thought of as a pair of mechanisms: one which blocks traffic, and one which permits traffic. Some firewalls permit only e-mail traffic through them, thereby protecting the network against attacks other than attacks against the e-mail service. Other firewalls provide less strict protection, and block services that are known to be problems.

Generally, firewalls are configured to protect against unauthenticated interactive log-ins from the outside world. This, more than anything, helps prevent vandals from logging into computers on the network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside.

The most straightforward way of use of a firewall is to create a so-called internal site, one that is accessible only to computers within one's own local network. Then, all what needs to be done is to place the server inside the firewall:



As to the web-servers connected to the Internet, they need to place it somewhere outside the firewall. From the point of security of an organisation as a whole, the safest place to put it is outside the local network:



This is called a sacrificial lamb configuration. The server is at risk of being broken in, but at least when it's broken in it does not breach the security of the inner network. On the other hand, web pages at the server are vulnerable for an unauthorised alteration and other forms of vandalism.

²¹ " Computer Crime: A Crimefighter's Handbook", D. Iovine, K. Seger, W. von Stroch. O'Reilly & Associates, Inc., Sebastopol, 1995.

—

²² Further details available from: Sniffer FAQ <http://www.iss.net/sec_info/addsec.html>

—

There are a number of variations on this basic set-up, including architectures that use paired inner and outer servers to give the world access to public information while giving the internal network access to private documents²³. However, the system with the really secret data should be isolated from the rest of the corporate network, and should not be hooked up to the Internet at all.

5.5 Encryption

Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. For example, one may wish to encrypt files on a hard disk to prevent an intruder from reading them. Encryption can also be used to protect e-mail messages and to verify the identity of the sending part

The combination of advanced mathematical techniques with the enormous growth of the possibilities for automatic data processing has resulted in very strong cryptographic systems, that are almost impossible to break. In the open and unsecured networks like the Internet, strong encryption has become one of the main tools for the protection of privacy, trust, access control and corporate security, to name only basic possible application of so-called public-private key encryption systems.

— Under a more traditional single key system, the same key is used both for encrypting and decrypting the message. Although this is reasonably secure, there is a risk that this key will be intercepted when parties involved exchange keys. A public key system, however, does not necessitate the exchange of a secret key in the transmission of messages. The sender encrypts the message with the recipient's freely-disclosed, unique public key. The recipient, in turn, uses his unique private key to decrypt the message. It is also possible to encrypt messages with the sender's private key, allowing anyone who knows the sender's public key to decrypt the message. This process is crucial to creating digital signature that provides verification of the identity of the message sender.

— Currently, the two main cryptographic systems providing for secure e-mail are Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM). Despite export restrictions, PGP is widely available outside the United States in different versions, becoming de facto international standard²⁴. It is available for most computers and can be easily configured to work in several different languages, including Spanish, French and German.

²³ See : The World Wide Web Security FAQ <<http://www.genome.wi.mit.edu/WWW/faqs/uwusf.html>>

—

²⁴ Details available from: EFH Pretty Good Privacy Workshop <<http://www.efh.org/pgp/pgpwork.html>>

—

— To-day, an acute and mostly unresolved conflict exists, however, between the private interests in protection of secrecy of information by means of encryption, and the interests of the investigating authorities to obtain timely access to the content of sized or intercepted data. To minimise the negative effects of the use of cryptography on the investigation of criminal offences two different approaches have been developed at national level. The legislation of France and the Russian Federation prohibits the use, distribution, development and export of any cryptographic tool without a license granted by a special government agency. An alternative approach, supported by a number of the most developed countries and some international organisations as the Organisation for Economic Cooperation and Development, the Council of Europe, the European Commission and the International Chamber of Commerce have proposed the key-escrow scheme, based on the cooperation of one or more trusted third parties who will hold keys and be required to hand them over to law enforcement authorities under certain conditions²⁵.

Encryption is often recommended as the solution to all security problems. Unfortunately, this is not the case. Encryption does nothing to protect against many common methods of attack including those that exploit bad default settings or vulnerabilities in network protocols or software. Information security requires much more than just encryption. Authentication, configuration management, good design, access controls, firewalls, auditing, security practices, and security awareness training are a few of the other techniques needed.

²⁵ See also: "Crypto Law Survey" <<http://cwis.kub.nl/~frw/people/koops/lawsurvey.htm>>

—