ZBORNIK
PRAVNOG FAKULTETA U ZAGREBU

GOD. 38 - BROJ 6

ZAGREB
1988.

DATA PROTECTION AND NEW TECHNOLOGIES IN PUBLIC ADMINISTRATION

Dr STEVAN LILIĆ
University of Beograd

UDK 342.7:681.5:35
Original Scientific Paper

In modern society, collecting, processing and transmitting information can be regarded as a principle public function of government and public agencies on all community levels. This view of the public administration as processor of recorded information can be illustrated with many examples from different areas of public activity. The tremendous growth of the "computer environment" unquestionably challenges the traditional legal interpretation in such areas as contracts, property, patents and copyright protection, public records, data security and privacy. The privacy issue, incorporating data protection and computer security questions, has surged - both conceptually and practically into the focus of legislative, judicial and administrative legal interest. It is within the scope of a today's computer society, the "assault on privacy" and with it data protection have become the quint essential privacy issue. Most developed nations have established some kind of expert body to analyze and study the question of data protection and privacy in the public and private sector and have proposed and applied various types of legal regulatory and protection mechanisms. An overview of data protection and computer systems security is given for the following countries: Sweden, France, The Federal Republic of Germany, United Kingdom, United States, Japan and, particularly Yugoslavia.

The last decades have been characterized by the expanding growth in the technology of collecting, processing and transmitting data and information.

As the growth of information sources multiply, not only in the field of science and technology, but in other areas of social and individual activity - from economy and education to public services and law, this phenomenon is often described in terms of an "information explosion".

Information has always been an important factor in governing public affairs. It is the image of files and records, of protocols and dossiers containing information on a particular matter or person that symbolize government and public agencies at work.

In modern society, collecting, processing and transmitting information can be regarded as a principle public function of government and public agencies on all community levels. The task of government and public service can be seen as a general need to carry out administrative and social functions in an efficient, economic and legal manner. This view of the public administration as processor of recorded information can be illustrated with many examples from different areas of public activity - from tax

collecting to population census statistics. The accumulated data is processed, transmitted and evaluated electronically by the mighty technological potential of today's "computer state".

"The enormous benefits provided by this technology offer another kind of camouflage. The comfort and conveniences of the computer, make thinking about its potentially negative effects something of an exercise in self-denial".[1]

Parallel with the development of information processing technology, the last decades also witness a tremendous development in electronic surveillance technology. Advances in electronics and related technologies have greatly increased the technical possibilities of surveillance activities used to monitor various aspects of individual behavior. Existing legal frameworks - from the legislature to the judiciary, usually cannot keep up with the pace of technological innovations to adequately cover these applications. In resolving legal issues of this nature an interactive balance must be found between the rights and liberties of the individual and the need of monitoring individual behavior by electronic surveillance devices for the purpose of law enforcement by the authorities in fighting crime and securing social order.

> "[Until recently] electronic surveillance was limited primarily to audio surveillance devices [...], now, however, technological developments have significantly expanded the range of electronic surveillance options. These include miniaturized transmitters for audio surveillance, light-weight compact television cameras for video surveillance, improved night vision cameras and viewing devices, and a rapidly growing array of computer-based surveillance techniques..."[2]

As modern industrial and social systems grow more complex, government regulatory and administrative functions increase. On the other hand, the large governmental and administrative bureaucratic organizational systems become models for industrial enterprises and public service institutions.

In such social and administrative environments, most individuals usually leave a "record trail" behind their actions in communicating with various government offices, public agencies and private institutions (birth certificates, school and medical records etc). Before the wide-spread use of computer information processing, collecting and linking particular bits of information into integrated patterns was technically very difficult, if not altogether impossible.

The reason for this was the nature of the data media paper. Finding and matching paper files presented not only a physical and organizational problem, but a financial one as well. In addition, the time needed for these operations often greatly diminished the value of the action itself.

Today, however, computer-based record systems and electronic communications networks, make it possible to overcome the time and cost barriers. Computer information technology permits instant communication linkage - integrated data processing, of a large number of record systems (for instance, on individuals) literally in seconds. Within this general context, the whole complexity and contradiction of a number of legal issues come into focus.[3]

---

1 David Burnham: "The Rise of The Computer State", New York, 1979, p. 7.

2 Congress of The United States, Office of Technology Assessment: "Electronic Surveillance and Civil Liberties", Washington, D.C., (20510) 1985, pages 9-13.

3 Selected references:
Colin Campbell (Ed):

1. Computer and law developments

Since the early 1950's, when electronic digital computers were introduced, new technological innovations have been rapidly multiplying. In the early days of the computer, the complexity and expense of electronic data processing equipment limited their use mainly to scientific and military experimental research.

Since then, however, inoformation processing technology, has been dramatically improved and advanced. Developing around the computer, new fields of legal information processing technology, particularly in public administration and services (census, health, tax, education, urban planning etc) have been developed. From "user-friendly" individual personal computer systems in offices and homes[4], to complex, national and international, legal information retrieval systems (CREDOC, QUIC/LAW, IRETIJ, JURIS, ITALGIURE, EUROLEX, LEXIS, WESTLAW, EURONET, INTERDOC, PRAVO-1 etc.)[5] Today, advanced research is being done in the field of highly sophisticated legal expert systems using the "artificial intelligence" (AI) techniques and processing capacities of the fifth generation super computers.[6]

2. The legal challenge of new technologies

The tremendous growth of the "computer environment" unquestionably challenges the traditional legal interpretation in such areas as contracts, property, patents and copyright protection, public records, data security and privacy. Of the many challenging aspects of the computer impact on legal questions, two issues top the list: transborder data flow ("TDF") and the privacy issue.[7]

The question of transborder data flow has evolved into a major issue related to the transaction of business, scientific and cultural information across national borders. In

---

"Data Processing and The Law", London 1984.
Andre Flory & Herve Croze:
"Informatique Juridique", Paris, 1984.
Nimmer Raymond:
"The Law of Computer Technology", Boston, 1985.
Jon Bing & Knut Selmer:
"A Decade of Computers and Law", Oslo, 1980.
Herman Seegers & Fritjof Haft:
"Rechtsinformatik in den achchziger Jahren, "München, 1984.
Peter Seipel:
"Computing Law", Stockholm, 1977.
Ettore Giannantonio:
"Italian Legal Information Retrieval", Milano, 1984.
Hubert Rodingen:
"Die Rechts- und Verwaltungsinformatik in der Sowjetunionen", Berlin, 1980.

4 Stewwart Schneider & Charles Bowen:
"Microcomputers for Lawyers", Blue Ridge Summit, PA, 1983.

5 Jon Bing:
"Handbook of Legal Information Retrieval",
Amsterdam-New York-Oxford, 1984.

6 Anne Gamer:
"Overview of Artificial Intelligence Approach to Legal Reasoning" in "Computing Power and Legal Reasoning", Edited by Charles Walter, West Publishing Co, St. Paul, 1986, p. 247-274.

7 Stuart Wolk & William Luddy:
"Legal Aspects of Computer Use", Engelwood Cliffs, NJ, 1986.

addition to the economy, transborder data flow is equally important to other international activities, such as education and agriculture, banking, transportation, insurance, law enforcement etc.

> "Every government function from security and national defense to weather prediction and disaster relief continues to be increasingly dependent upon computer and telecommunications technology. These uses necessarily require the transmission of data across national borders and the creation of data banks for the storage of information".[8]

On the other hand, the privacy issue, incorporating data protection and computer security questions, has surged - both conceptually and practically into the focus of legislative, judicial and administrative legal interest. It is on this matter that attention will be focused on this occasion. The privacy issue challenge is legally and socio-psychologically complex.

> "[The challenge] seems to stem above all from the uneasy feeling that the computer necessarily implies a loss of control over ones's affairs [...] earlier innovations were less traumatic than the computer, because they were designed to carry out rather specific functions and impinged rather less upon traditional working methods. Above all, the user remained manifestly in control of those earlier innovations - at least he could read and see something! [...] Computers can store information and (like the human mind) do it invisibly. That makes them powerful, mysterious, possibly devious, and certainly dangerous. [...] It is the ability of the computer to reproduce information in a flash in an infinite variety of forms and places which really poses the challenge."[9]

New technologies open legal questions of both "technical" (e.g. identifying the source of a legal document created and transmitted by "electronic mail" devices)[10], and "conceptual" nature (e.g. modeling legal reasoning[11] or "sentencing by computer"[12]).

3. Privacy and the Public Interest

The multi-dimensional nature of the privacy, issue directly reflects on the legal concept of privacy, making it a multi-disciplinary issue. The privacy issue is both complicated and complex, not only because of the difficulties in establishing a precise formal legal definition of "the right to privacy", but also because of the contradictions of modern legal systems, as well.

---

8 Richard McGuire:
"The Information Age - An Introduction to Transborder Data Flow", Jurimetrics Journal, Vol. 20, No. 1, 1979, p. 2.

9 David Andrews:
"The Legal Challenge Posed by The New Technology", Jurimetrics Journal, Volume 24, No. 1, Fall 1983, pages 43-44.

10 Richard Lettieri:
"How to Develop and Use In-House Legal Systems", American Bar Assocation, Chicago, 1985.

11 Philip Leight:
"Logic, Formal Models and Legal Reasoning",
Jurimetics Journal, Volume 24, No. 4, 1984.

12 Richard V. de Mulder & Helen M. Gubby:
"Sentencing by Computer: A Step Forward?", Law/Technology, Volume 17, No. 1, 1984, page 15.

"It is one of the greatest anomalies of our time that law, which exists as a public guide to conduct, has become such a recondite mystery, that it is incomprehensible to the public and scarcely intelligible to its own votaries."[13]

Despite numerous attempts of formulating a general (legal) conceptual definition of privacy, the concept is still being discussed. It is not rarely argued that, as early forms of information technology (telegraph, telephone etc) came into use, that the modern concept of "the right to privacy" (as the right to be left alone), was invented in the United States by Samuel Warren and Louis Brandais.[14] Today, however, this concept of privacy as "non-interference" has been seriously criticized and is steadily loosing ground.

"Despite the incurable vagueness of this formulation, there is something very seductive about attempts to equate privacy with non-interference, or being let alone - what philosophers call 'negative liberty'. [...] To equate them is mistaken and potentially confusing".[15]

Recent alternative approaches to privacy, focus on "information control" rather than on non-interference.

"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[16]

It is argued that, unlike the non-interference concept, the information control concept of privacy corresponds to real social and individual interaction, enabling, thus clear identification of the interest involved when people resist surveillance or monitoring of their affairs. In this manner, the issue of privacy can be approached from the "interest" point of view, a notion that can be legally identified and utilized.[17]

It is, essentially, for this reason that such an approach has been adopted for practical puposes by, for instance, a panel on Privacy and Behavioral Reserach reporting to the US President's Office of Science and Technology.

"The right to privacy is the right of the individual to decide for himself how much he will share with others - his thoughts, his feelings, and the facts of his personal life..."[18]

a) Data protection

Even though the term "privacy" has been in legal circulation for a hundred or so years, the issue "exploded" with the development of electronic data processing technology and computerized information systems - and with it, all aspect of the data protection problem. Storing vast amounts of data on computer media and retrieving it for various

---

13 Lee Loevinger:
"Jurimetrics – The Next Step Forward", Minnesota Law Review, Volume 33, No. 5, 1949, p. 455.

14 This concept was presented in the now famous Harvard Law Review article "The Right to Privacy" by Samuel Warren and Louis Brandais, published in 1890.

15 Arthur Schafer:
"Privacy: A Philosophical Overview", Aspects of Privacy Law - Edited by Dale Gibson, Toronto, 1980, page 6-7.

16 Alan Westin:
"Privacy and Freedom", New York, 1967, p. 7.

17 Schafer (supra), page 9.

18 See G. L. Simons (supra), page 15.

purposes is no technical problem. Yet, it is within the scope of today's computer society, that the "assault on privacy" and with it data protection have become the quint essential privacy issue.[19]

> "On first impression data protection is apparently an essential 'private law' issue - the protection of privacy from invasion or abuse of modern information technology. This is a wholly misleading impression, however, because (it) involves a number of public law issues."[20]

Data protection issues related to public administration and public services vary. They range from questions of a functional nature - restricting availability of certain classes of information, informal exchange of information, information disclosure from private institutions to public authorities, to questions of an organizational nature, such as creating public authority bodies and institutions (commissions, boards, registers etc) entrusted with the implementations of data protection legislature.

Generally speaking, the nature and degree of legal protection is determined by the degree of political significance of privacy and data protection (as a human rights) issue, which in itself is determined by the general level of technological and cultural development.

> "[Government] attitudes to these topics determine with what commitment legislative and other measures are introduced in this field... [it is, therefore] ... necessary to define legitimate claims of government and other bodies within the framework of appropriate legislative and institutional safeguards...".[21]

Most developed nations have established some kind of expert panel or commission to analyze and study the question of data protection and privacy in the public and private sector and have proposed and applied various types of regulatory and legal protection mechanisms. Legislation may vary, depending on the "point of view" - if the legal protection mechanism is mostly "private law oriented", the result is usually a Privacy Act (United States, Canada). On the other hand, if the legal protection mechanism is "publiclaw oriented", the result is a Data Protection Act (United Kingdom, West Germany).

There are various ways and methods - for the better or for the worse - that individual freedom is constrained and limited on account of the interest of the community and the spontaneous human need not to be molested is penetrated by organized social groups (political and social organizations, governments agencies and public services) in need to secure law enforcement, tax administration, medical protection, educational programs etc. All these circumstances emphasize the relevance of the privacy issue, of data protection and the physical and legal security of the information systems in which data is stored.

---

19 Selected references:
Arthur Miller:
"The Assault on Privacy - Computers, Data Banks and Dossiers", Ann Arbor, MI, 1971.
David Flaherty:
"Privacy and Data Protection" – An International Bibliography, London, 1984.
Alfred Büllesbach:
"Informationstechnologie und Datenschutz", München, 85.
Tom Riley:
"Data Protection Today and Some Trends", Law/Technology, Vol. 17, No. 1, 1984.

20 R. C. Austin:
"The Data Protection Act – Public Law Implications", Public Law, Winter 1984, p. 619.

21 Simons, supra, page 15-16.

b) Computer system security

There is a wide variety of hardware and software methods that can be used to safeguard security and integrity of computers as technological systems. Among them, professional standards of the staff responsible for their operation, as well as "regular operation procedures" are considered of vital importance.[22]

> "Computer security [...] is an umbrella that protects the organization's hardware and software, as well as the data and information processed by the computer against abuse, fraud, embezzlement, sabotage, and intentional or accidental damage, or natural disaster."[23]

The weakest link in any computer system is most likely to be the "human factor" i.e the staff, as they have both the skills and opportunities to misuse the system. It is general practice that access to computer files is possible only from designated terminals and by authorized users who are required to identify themselves by means of a special "password". The password system, as is the case of any safeguard program, cannot guarantee that the files will not be reached. Control of access can also include special programs where one user cannot penetrate the field of another, and so on.

Technical safeguards can include various "early warning" systems (personal identification, sound and light alarms, automatic shut-off devices, etc) and "post-facto" analysis of recorded material (video recordings of activity in the computer center, automatic back-up recordings of processing operations, etc), depending on the security level of the system.

Particularly in the area of public administration, adoption of a "sound administrative practice code" would greatly diminish the treat of system misuse.

> "The implementation in public undertakings of a code of good practice designed to ensure security and privacy of stored data would be a most useful step. (The code) would specify the qualifications of the staff required to operate and maintain a computer center and would lay down minimum acceptable standards of technological protection".[24]

4. Comparative legislation overview

In the 1970's certain West European and North American countries began passing laws and regulations on data protection of personal privacy. The State of Hesse, one of the federal units of the Federal Republic of Germany, enacted the first data protection legislation in 1970. The first national data protection law, however, was Sweden's Data Act of 1973; the United States Privacy Act in 1974 - other countries, followed.

---

22 Selected references:
Dom Parker:
"Fighting Computer Crime", New York, 1981.
Norman Lyons:
"Understanding Computer Crime", Sherman Oaks, CA, 1984.
Daniel Brooks & Susan Nycum:
"Computer Crime - Prevention, Detection, Prosecution", New York, 1983.
Jack Bologna:
"Computer Crime - The Wave of The Future", San Francisco, 1981.

23 J. A. Van Duyn:
"The Human Factor In Computer Crime", Los Angles, 1985, p. 4.

24 G. B. F. Niblett:
"Digital information and The Privacy Problem", OECD, Paris, 1971, p. 26-27.

Sweden - Sweden was the first country to pass a national protection law - The Data Act (Datalag) of 1973. The Act requires the licensing of all personal registers in both public and private sectors and compliance with a set of strict standards to prevent unwarranted invasion of privacy. The Data Inspection Board is headed by the Director General.[25]

The Federal Republic of Germany - The Federal Data Protection Act (Bundesdatenschutzgesetz), enacted in January 1977, provides detailed principles for data protection in the public sector and a coordinated system of implementation for the federal and state level, as well as the creation of a Data Protection Commission (Bundesbeauftragte für den Datenschutz). The Data Protection Commissioner is independent in performing his functions, and oversees that the provisions of the Act are implemented in the federal public sector. Although, his power is advisory, he can submit complaints to the relevant authority, and can receive complaints from individuals.[26]

France - The French Law on Information Processing and Freedoms (Loi No. 78-17 Relative à l'informatique aux fichiers et aux libertés), of 1976, is extensive and innovative. It created an independent authority with regulatory powers - The National Commission on Data Processing and Freedoms (La Commission Nationale de l'informatique et des Libertés). The Commission, among other functions, gives authorization of particular personal information systems as well as expert legislative advise on data protection and freedom to the government.[27]

United Kingdom – The Data Protection Act of the United Kingdom of 1984, is structured along the continental data protection legislation in order to conform with the Council of Europe's Convention of the Protection of Individuals with the regard with the Automatic Processing of Personal Data - of which the main effect is the establishment of an independent Data Protection Registrar for both public and private users of personal information systems. The Act emphasizes simple registration, rather than detailed licensing (as in Sweden or France). Data subjects have the right to be informed what data about them is being collected and can sue for damages. A decision of the Registrarr can be appealed to the newly established Data Protection Tribunal and in last instance to the regular courts.[28]

Canada - The federal Privacy Act of 1982, supplemented and elaborated privacy protection provisions of the Human Rights Act of 1977 (Part IV), regulating the collection, retention, disposal, protection and disclosure of personal information by the federal government. Complaints can be filed to the Privacy Commissioner, request denials for information access can be appealed to the Federal Court. The province of **Quebec** has enacted Law No. 65 (1982) on data protection in the public sector, that applies to personal information systems of all public bodies, including schools, universities, municipalities, health and social services. The law establishes an independent Information Acces Commission (Commission d'accés à l'information), that has significant supervisory and inspection authority, as well as authority to respond to complaints and conduct investigation, to issue binding orders, etc.[29]

United States - The Privacy Act of 1974 provides regulation of information processing activities of the federal government. The Privacy Act had a major initial

---

25 David Flaherty:
"Privacy and Data Protection" – An International Biography, London, 1984.

26 Ibidem.

27 Ibidem.

28 Ibidem.

29 Ibidem.

impact. Unlike the large majority of other countries, the United States have not established any kind of data protection institution (e.g. commission) with independent authority - the argument being that it is not in the Common Law tradition. In absence of such a federal institution, the task of monitoring the implementation of the Privacy Act is with the US Office of Management and Budget (Office of Information and Regulatory Affairs), which - by virtue of its competence, does not have the political motive for active involvement, not to mention that it is overburdened with other responsibilities as well. The dependence on law suits of individual citizens for data protection has proven to be relatively fruitless, because of the costs of the litigation and the legal and technical problems of establishing "privacy" damages. Still, it would be misleading not to acknowledge the strength of the data protection and privacy system in the US.[30]

Japan - A 1975 government report focused on the issue of protecting the privacy rights of individuals, recuiring that attention should be paid to "harmonization and adjustment" between individual rights and public interests. On basis of this report, Rules for the Protection and Management of Computer-Processed Data (1976) were laid down as guidelines for measures each ministry should adopt in the data protection of data under its jurisdiction. In 1984 The Committee on the Protection of Data Privacy was established with the purpose of studying the necessary measures, including legislative.[31]

Yugoslavia - Taking advantage of the occasion, we would like to briefly inform on the current state of affairs regarding data protection in Yugoslavia. In Yugoslavia there is no integral piece of data protection legislation, neither on the federal, nor state level. Nevertheless, the Federal Government introduced a Draft amending the existing "Basis of the Social System of Informing and the Information System of the Federation Act"[32] adding a whole new section on the protection of data and information in the "social information system". Interesting features of the proposed draft deal with the right of self-management organizations and communities to regulate the measures and procedures of data protection by "their own self-management general acts", in other words, that these subjects independently prescribe the data protection standards. The draft, further proposes various hardware security measures, as well as a firm stand on data collecting. Practically, the central data protection provision is article 24-h: "Data and information [...] may be collected only where there exists a legal basis for it, or with the consent of the subject.." [...] "The data and information [...] can be used only for purposes for which they have been collected. The purpose must be defined before the collection [...] A person can request the correction of inaccurate data [...] as well as the deletion of data about himself which cannot be proved correct or data that has been collected in a manner not permitted". The draft does not propose a data protection body or commission. On the other hand, strong arguments for an independent piece of legislation on data protection and privacy, particularly in general view of the forthcoming constitutional changes, have been heard from the academic and practicing legal community.

It is interesting to point out thought, that as far as data protection related to public administration is concerned, it is our opinion that some amended provisions (1986) of the General Administrative Procedure Code can be applied, particularly the ones regarding the

---

30 Ibidem.

31 "Protection of the Right to Privacy and the Issue of Making Government Information Public in Japan", The Local Authorities Systems Development Center, Special UN Program for Senior Government Officials, Stockholm, Sweden, Oct.,1985.

32 Predlog za donošenje Zakona o izmenama i dopunama Zakona o osnovama sistema društvenog informisanja i o informacionom sistemu Federacije, Savezni sekretarijat za informacije i Savezni sekretarijat za pravosuđe i organizaciju savezne uprave, Beograd, mart 1987.

81

issuing, correcting and use of public documents. For instance, the Code provides that "(A government agency or public body) document can be issued in a form that can be electronically processed..."(Art. 164), further, it regulates the procedure of issuing such documentsand certificates (Art. 171) and provides specific and general legal remedies - appeals to higher instances (žalba), and administrative judiciary protection (upravni spor).[33]

Data protection activity on the international level was initiated by The International Commission of Jurists in Stockholm (1967), concluding that [Individuals should have the right to be protected against]:

> 1. interference with the individual's private life, family or home life; 2. interference with one's physical or mental integrity or one's moral or intellectual freedom; 3. attacks on one's honor and reputation; 4. being placed in a false light; 5. the disclosure of irrelevant embarrassing facts relating to ones private life; 6. spying, prying, watching and besetting; 7. interference with correspondence; 8. misuse of private correspondence, written or oral, and 9. disclosure of information given or received by the individual in circumstances of professional confidence.[34]

International activity on the privacy issue is very intensive, but limited space permits only a summary overview of the most significant international conventions:[35]

– **United Nations**, "Human Rights and Scientific and Technological Development - The uses of electronics which may affect the rights of a person and the limits which should be placed on such uses in a democratic society".

– **The Council of Europe,** "Convention For The Protection of The Individual With Regard to Automatic Processing of Personal Data".

– **OECD:** The Organization for European Cooperation and Development, "Guidelines for the Protection of Privacy and Transborder Data Flow of Personal Data".

Instead of a Conclusion

Instead of concluding, we propose that it would be most useful that expert bodies study the matter thoroughly in regard to the general trends in new technologies and international law development, and to propose the implementation of specific legislative measures and legal mechanisms for data protection and system security. On the other hand, a new legal disciplines (e.g. "Information Law") could relate to the research needs of the legal challenge of new technologies in law generally, and public administration in particular. Information Law could integrate legal questions regarding the application of data and information processing technologies with the realization of fundamental human rights in modern complex societies and to try to reach the optimal balance between the information collecting and processing needs of public and general social interests, on one side, and the freedoms of the individual citizen, on the other.

---

33 General Administrative Procedure Code (Zakon o opštem upravnom postupku – 1986), and the Administrative Suits Code (Zakon o upravnim sporovima – 1977).

34 See Simons, supra, page 15.

35 Report of the Secretary-General of the United Nations, E/CN. 4/1142, Jan. 1973. Council of Europe, Strasbourg, 1980. OECD, Paris, 1981.

SELECTED BIBLIOGRAPHY

G. L. Simons: "Privacy in the Computer Age", Manchester, 1982.
Arthur R. Miller: "The Assault on Privacy – Computers, Data Banks and Dossiers", The University of Michigan Press, Ann Arbor, 1971.
Arthur Schafer: "Privacy: A Philosophical Overview", Aspects of Privacy Law – Edited by Dale Gibson, Toronto, 1980.
David Burnham: "The Rise of The Computer State, New York, 1979.
Alan Westin: "Privacy and Freedom", New York, 1967.
David Flaherty: "Privacy and Data Protection – An International Bibliography", London, 1984.
Stuart Wolk & William Luddy: "Legal Aspects of Computer Use", Engelwood Cliffs, N. J., 1986.
Jon Bing: "Handbook of Legal Information Retrieval", Amsterdam - New York-Oxford, 1984.
David Andrews: "The Legal Challenge Posed by The New Technology", Jurimetrics Journal, Volume 24, No. 1, Fall 1983.
Lee Loevinger: "Jurimetrics – The Next Step Forward", Minnesota Law Review, Volume 33, No. 5, 1949.
Hubert Rodingen: "Die Rechts- und Verwaltungsinformatik in der Sowjetunionen", Berlin, 1980.
Throne McCarthy: "Intelligent Legal Information Systems-Problems and Prospects", Rutgers Computer & Technology Law Journal, Volume 9, No. 2, 1983.
Cary de Bessonet: "An Automated Intelligent System Based on a Model of a Legal System", Rutgers Computer & Technology Law Journal, Volume 10, No. 1, 1983.
Anne Garner: "Overview of Artificial Intelligence Approach to Legal Reasoning" in "Computing Power and Legal Reasoning" Edited by Charles Walter, West Publishing Co, St. Paul. 1986.
Richard Immel: "The Automated Office – Myth Versus Reality", Popular Computing, May, 1983.
Stewart Schneider & Charles Bowen: "Microcomputers for Lawyers", Blue Ridge Summit, PA, 1983.
Richard Lettieri: "How to Develop and Use In-House Legal Systems – A Corporate Council's Computer Guide", American Bar Association, Chicago, 1985.
Philip Leight: "Logic, Formal Models and Legal Reasoning", Jurimetrics Journal, Volume 24, No. 4, 1984.
Richard V. de Mulder & Helen M. Gubby: "Sentencing by Computer: A Step Forward?", Law/Technology, Volume 17, No. 1, 1984.

Sažetak

Prof. dr. Stevan Lilić: Zaštita podataka i nove tehnologije u javnoj upravi

Posljednje decenije dvadesetog stoljeća obilježava brz rast tehnologija prikupljanja, obrade i prenošenja podataka i informacija. Taj proces ne ostavlja po strani ni javnu upravu, štoviše, u modernom društvu takvi zadaci postaju osnovna djelatnost javnih službi. Suvremenu državu ("computer state") karakterizira i mijenja upravo narasla mogućnost prikupljanja i upotrebe podataka, razvitak tehnologija elektronskog nadzora (electronic surveillance), napuštanje pismenog bilježenja te ubrzanje poslovanja i snižavanje troškova. Računarska tehnologija dozvoljava trenutno informacijsko povezivanje, obradu podataka doslovno u sekundama te povezivanje u velike informacijske mreže.

Paralelno s tehnološkim napretkom dolazi i do dramatične promjene u pravnom reguliranju te problematike. Predmet regulacije nisu samo postupci s računalima već čitava tehnologija obrade pravnih informacija (legal information processing technology), od korisnicima prilagođenih osobnih računala (user-friendly) dostupnih u uredima ili kućama pa do složenih nacionalnih i internacionalnih mreža primjene pravnih informacijskih sistema (CREDOC, QUIC/LAW, IRETIJ, JURIS, ITALGUIRE,

EUROLEX, LEXIS, WESTLAW, etc.). U novije vrijeme osobit je napredak postignut na stvaranju ekspertnih sistema (expert systems) koji se služe tehnikama umjetne inteligencije.

Takva je promjena izazov i za pravnu teoriju i doktrinu na području ugovora, vlasništva, patentnog i autorskog prava, javnih isprava, zaštite i sigurnosti podataka.

Posebno se naglašava pitanje prenošenja podataka preko nacionalnih granica, bilo da se radi o poslovnim podacima, znanstvenoj ili kulturnoj djelatnosti.

U okvirima tako označene mreže problema autor bira pitanje zaštite privatnosti ističući da se ne radi o pukim tehničkim i pravnim problemima (elektronska pošta i sl.), već o pitanju koje dira u samu konceptualnu osnovu pravne znanosti (model pravnog zaključivanja).

Prije svega treba razgraničiti pojmove zaštita privatnosti, zaštita podataka i zaštita računarskog sistema.

Iako postoje različiti pokušaji određenja pojma privatnosti, ne postoji opće slaganje o njegovu značenje. U ranijim razdobljima razvitka računarskih tehnologija privatnost se pretežno određivala kao "pravo na privatnost", pravo na nesmetanje, pravo na "negativnu slobodu". Tako definiran pojam (prema S. Warrenu i L. Brandaisu) u novije se vrijeme sve više napušta u korist tumačenja po kojem je pravo privatnosti prije svega pravo na kontrolu informacija, a potom i pravo na nesmetan život. Takvo određenje koje naglašava zaštitu interesa pojedinca nazire se i u jednoj novijoj definiciji koju citira autor: "Pravo na privatnost je pravo pojedinca da odlučuje koliko će s drugima dijeliti svoje misli, svoje osjećaje i podatke o svom osobnom življenju..."

Zaštita podataka klasičan je problem javne uprave. Obuhvaća pitanja funkcioniranja organizacije (od pristupačnosti pojedinim klasama informacija, razmjeni informacija, zatvorenosti informacija i sl.) odnosno strukturnih problema kao što su stvaranje posebnih tijela i institucija zaduženih za primjenu zakona o zaštiti podataka. Zaštita podataka ne može se odvojiti od pitanja privatnosti, naročito ako potonju odredimo u modernijem, širem značenju. Dakle radi se o političkom pitanju, za koje postoji cijela skala različitih pravnih rješenja. Razvijenije nacije osnovale su posebna tijela ili komisije koje se bave zaštitom privatnosti i zaštitom podataka u privatnom i javnom sektoru, predlažu pravna rješenja ili se snagom autoriteta pravne znanosti brinu o provedbi zakona.

Zaštita računarskih sistema (computer system security) pojam je koji se odnosi na cijelu skalu različitih problema - funkcionalnih (ograničenje pribavljanja određenih skupina informacija, neformalna razmjena informacija) i organizacijskih (kao što je stvaranje javnih tijela i institucija ovlaštenih za primjenu legislature o zaštiti podataka). Općenito, priroda i stupanj zaštite podataka određeni su političkim značenjem zaštite privatnosti i podataka, a ono opet općom razinom tehnološkog i kulturnog razvoja.

Razvijenije nacije su ustanovile razne vrste ekspertnih komisija zaduženih za analizu pitanja zaštite podataka i privatnosti te predlaganje i izvršavanje različite pravne regulative na tom području. Pravna regulativa ovisi o tome da li je sistem pretežno orijentiran "privatnopravno" - tada je rezultat zakon o zaštiti privatnosti (Privacy Act - USA, Kanada), odnosno da li je "javnopravno" orijentiran - tada se izražava zakonima o zaštiti podataka (Data Protection Act - Velika Britanija, SR Njemačka).

Nakon kratke analize tehničkih i pravnih okvira zaštite računala autor sažeto prikazuje zakonodavstva pojedinih zemalja:

Švedska - prva zemlja koja je uredila zaštitu privatnosti (Datalag, 1973). Zakon zahtijeva dobivanje dozvole za vođenje osobnih registara uz stroge standarde koji sprečavaju zloupotrebu podataka.

Savezna Republika Njemačka. U siječnju 1977. proglašen je Bundesdatenschutzgesetz koji podrobno uređuje načela zaštite podataka. Istodobno je osnovana i komisija zadužena za praćenje primjene zakona. Ovlaštenja komisije ograničena su njenom savjetodavnom ulogom, no nema sumnje da se radi o tijelu kojem građani mogu podnositi svoje prigovore a koje snagom svog stručnog autoriteta inicira djelovanje drugih organa.

Francuska. Od 1976. i Francuska ima poseban zakon o zaštiti obrade informacija i zaštiti sloboda. Tim zakonom formirana je nacionalna komisija za informatiku i slobode. Zadatak je komisije da daje suglasnost pri stvaranju informatičkih sistema, a ona je ujedno i tijelo koje daje pravne savjete vladi u slučajevima koji se tiču zaštite privatnosti i podataka.

Velika Britanija također ima nov zakon (Data Protection Act, 1984) koji slijedi logiku evropske legislative na tom području. Istina, ne zahtijeva se suglasnost za uvođenje sistema obrade osobnih podataka, no postoji obveza registracije. Osnovan je i poseban sud (Data Protection Tribunal) koji u žalbenom postupku odlučuje o zahtjevima stranaka.

Autor nadalje izlaže sažeto zakonska rješenja kakva postoje u Kanadi, Japanu i Sjedinjenim Državama, a i neka rješenja međunarodnog prava. U pogledu Jugoslavije konstatira da ne postoji specifičan zakon o zaštiti podataka i privatnosti, no informira o rješenjima koja se predlažu nacrtom odgovarajućeg zakona i o mogućnostima da se za određene slučajeve koriste i pojedine odredbe ZUP-a.

Zaključujući, autor upozorava na značenje praćenja općih trendova u razvoju novih tehnologija, a posebno novih pravnih rješenja vezanih za zaštitu podataka i privatnosti. Posebnu važnost u tome imale bi i nove pravne discipline kao npr. informatičko pravo. Zadatak pravne znanosti je pronaći pravu ravnotežu s jedne strane između potrebe da se u društvenom interesu obrađuju i prikupljaju osobni podaci te vrijednog političkog cilja zaštite osobnih prava i sloboda s druge strane.