ISSN 2029-1701

Mokslinių straipsnių rinkinys
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2011 (6) Scientific articles

THE RIGHT TO PRIVACY IN THE CONTEXT OF INFORMATION TECHNOLOGY DEVELOPMENT

Birutė Pranevičienė

Mykolas Romeris University Faculty of Public Security Department of Law
V. Putvinskio 70, LT-44211 Kaunas, Lithuania
Telephone (+370 37) 303655
E-mail: praneviciene@mruni.eu

Abstract. The right to privacy is considered as one of fundamental, inalienable human rights, which should be protected in civilized society. However, changes in societies, growing of computer technologies raised new challenges to the system of ensuring the right to privacy.

Some problematic issues, related to the right to privacy and legitimate expectation of the protection of the right to privacy, are presented in the article. The article consists of two parts. First part is devoted to discuss about the peculiarity of the right to privacy and emerging threats to privacy, which arise by using information technologies. There are different concepts of privacy and emerging main threats to individual privacy presented in the article. Second part of the article presents the need of legal protection of privacy in using informational technologies, especially in cyberspace, and analyzes international legal documents ensuring right to privacy. It was made a conclusion that during last decades, privacy has been one of the most problematical social issues related to development of digital electronic information technologies. A specific part of human lives has moved to cyberspace, individuals began to use digital technologies in many areas of life, especially in communication and commerce. This situation has created new threats to human privacy. Therefore privacy became legally protected value. The right to privacy has been embedded into the main laws of many states – constitutions, international agreements, etc. International agreements oblige countries to keep the same high standard of ensuring individual's right to privacy. However, development of new technologies simultaneously raised not only new threats for privacy, but also formulated a need for such legal regulation, which limits the right to privacy. Therefore EU Directives not only established the standards and principles of the protection of personal data and safe use of informational technologies, but also legitimized data retention in the field of Electronic Communications.

Keywords: right to privacy, human rights, cyberspace, information technologies, personal data

INTRODUCTION

Nowadays, it is hard to imagine a life without advanced telecommunications' systems, information technologies, computers and cyberspace, which are used in a variety of areas, for example, schools, universities, public service, etc. Telephones, computers and internet help us to get and to share information, communicate with people who live far away from us. There are many social networks, programs that help us in our daily life. Therefore, it is obvious that part of individual's life moved to the virtual space. No matter whether individuals spend their time in cyberspace, or in "old fashioned reality", they have a right to privacy. The problem is especially relevant today as more and more of our privacy is stripped away. Despite that fact, individuals cherish their privacy, which covers many things and is, according U.S. Supreme

Court Justice L. Brandeis, "the most comprehensive of rights and the right most valued by civilized men"[1]. Privacy means many things in different contexts, but at the same time "nobody can articulate what it means"[2]. Usually privacy is defined as the fundamental right of individual, essential for freedom, democracy, psychological well-being, individuality, creativity, safety, etc.

It is worth noticing that over the past several decades' right to privacy has been embedded into the main laws of many states – constitutions, international agreements, etc. Thus privacy certainly became paramount and constitutional value protected by national laws and international agreements.

However, the development of new technologies simultaneously raised concern about privacy. Achievements of scientists and engineers create huge possibilities for people, but at the same time the development of the computer made privacy erupt into a frontline issue around the world. Since 1970s there is increasing attention of scholars to the issue of privacy observed: for example Arthur R. Miller, one of the Americans' most distinguished legal scholars in the area of privacy, wrote the first book warning of the threat to privacy posed by modern information technology in 1971[3]. Professor at Temple University John C. Raines wrote a book "Attack on Privacy"[4] in 1974. An American Attorney, scholar and journalist Robert E. Smith, whose focus is mainly privacy rights, in 1979, published a book "Privacy: How to Protect What's Left of It"[5]. This book gives some advices about protecting of privacy against information collection by business and government, and against electronic surveillance. A number of books in Britain and Germany in the 1970s likewise examined the issue. Today, the concern remains largely the same, especially keeping in mind enlarging influence of the cyber technologies on the human life.

The aim of the article is to disclose whether there are legal guarantees ensuring the right to privacy in using information technologies.

In order to achieve the determined aim the following *tasks* will be settled:

- To discuss the peculiarity of the right to privacy and emerging threats to privacy, which arise by using information technologies;

[1] Olmstead v. United States, 277 U.S. 277 U.S. 438, 478 (1928) [2011-09-20] <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=277&invol=438>
[2] Solove, D.J. *Understanding Privacy*. Harvard University Press., 2009, p.1
[3] Miller, A.R.*The Assault on Privacy: Computers, Data Banks, and Dossiers*. University of Michigan Press, 1971.
[4] Raines, J.C. *Attack on Privacy*. Judson Press, 1974.
[5] Smith, R.E. *Privacy: How to Protect What's Left of It*. Anchor Press, 1979.

- To present the need of legal protection of privacy in cyberspace and to analyze international documents ensuring right to privacy;

Methodology of the Research. In the course of reaching the objective of the research were used the methods of systemic, analytical-critical, and analysis of legal acts.

1. THE PECULIARITY OF THE RIGHT TO PRIVACY, THREATS TO PRIVACY AND THE NEED OF ITS LEGAL PROTECTION IN CYBERSPACE

Privacy is a sweeping concept, embracing a lot of values, such as protection from searches and interrogations, freedom from surveillance, control over one's body and over personal information, solitude in one's home, protection of one's reputation, freedom of thought, right to make decisions involving family life, etc. The term "privacy" originates from Latin word "*privatus*", which means personal, belonging to someone personally, separated from the rest, deprived of something[6]. When something is private to a person, it usually means there is something what he/she values and it is considered inherently special or personally sensitive. Privacy by definition is a personal right.

It is interesting to note that this Latin term naturalized in many countries and in different languages there are no specific words to translate "*privatus*" (for ex. English – "*privacy*", German – "*privat*", French – "*prives*", Polish – *prywatny*, Lithuanian – "*privatus*"). Despite the fact, that the same term ("privacy") is used in different countries, this term means many things in different contexts. Different legal systems, culture and people have a variety of expectations about how much privacy a person is entitled to. For example, in some legal systems a woman's right to terminate a pregnancy or refuse medical treatment is justified because of her right to privacy, while in other legal systems such rights are not an issue of privacy, because of a state's interest in protecting life or potential life. The compromises between privacy and competing social values or legal rights are different in each area.

There are a few slightly different conceptions of privacy, emphasizing different aspects of the right to privacy. For example, conception which is called "*the right to be let alone*"[7] states that the underlying principle of privacy is that of inviolate personality. Warren and Brandeis asserted that the "common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to

[6] Vaitkevičiūtė, V. *Tarptautinių žodžių žodynas* [*Dictionary of International Words*].Vilnius: Žodynas, 2001, p.793

[7] In 1890, Samuel Warren and Louis Brandeis wrote the article „The Right to Privacy", 4 Harvard Law Review 193, 1890

others."[8] Thus, "the right to be let alone" means a "general right to the immunity of the person, the right to one's personality".[9] As Abe Fortas, the judge of the Supreme Court of the United States, noticed, privacy is related with the right "to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law".[10] This conception of privacy is criticized because "the conception of privacy as the right to be let alone, however, fails to provide much guidance about what privacy entails. Understanding privacy as being let alone does not inform us about the matters in which we should be let alone."[11] This conception of privacy is usually considered as a broad and vague conception of privacy.

Another conception of privacy is known as a conception of "*limited access to the self*" – it means the ability to cover oneself from unwanted access by others. The presumption is made that the individuals desire to take a cover and to be apart from others. According Sissela Bok, privacy is "the condition of being protected from unwanted access by others – either physical access, personal information, or attention".[12] The right to privacy is the right to exclude others from watching, utilizing, intruding upon, or in other ways affecting his private sphere. Like "the right to be let alone" conception, "the limited access" conception leaves us without a notion of what matters are private.

"Secrecy" is the concept of privacy, which means the concealment of certain matters from others. Under this view, privacy is violated by the public disclosure of previously concealed information. "The word "privacy" seems to embrace at least two distinct interests. One is the interest in being left alone – the interest that is invaded by the unwanted telephone solicitation, the noisy sound truck, the music in elevators, being jostled in the street, or even an obscene theater billboard or shouted obscenity […] The other privacy interest, concealment of information, is invaded whenever private information is obtained against the wishes of the person to whom the information pertains"[13]. R. A. Posner treats privacy as a form of self-interested economic behavior, concealing true but deleterious facts about oneself for one's own benefit. People "want to manipulate the world around them by selective disclosure of facts about themselves".[14]

[8] Warren, S., Brandeis, L. „*The Right to Privacy*", 4 Harvard Law Review 193, 1890, p. 198
[9] Warren, S., Brandeis, L. „*The Right to Privacy*", 4 Harvard Law Review 193, 1890, p. 207
[10] Time, Inc. v. Hill, 385 U. S., 374 (1967) [2011-09-24] < http://supreme.justia.com/us/385/374>
[11] Solove, D., p. 17
[12] Bok, S. *Secrets:on the Ethics of Concealment and Revelation*. Oxford University Press, 1984, p. 10-11.
[13] Posner, R.A. *The Economics of Justice*. Harvard University Press., 1981, p. 272-273.
[14] Posner, R.A. *The Economics of Justice*. Harvard University Press., 1981, p. 234.

The privacy as a secrecy conception can be understood as a subset of limited access to the self, because secrecy of personal information is a way to limit access to the self. But this conception is narrower than limited access conceptions, because secrecy involves only one dimension of access to the self – the concealment of personal facts. There are very important decisions of the Supreme Court of the United States related with this concept: in a number of cases the Supreme Court has held that there can be no "reasonable expectation of privacy" in things exposed to the public, even if it is highly unlikely that anybody will see or discover them.[15]

"Control over personal information" is the concept of privacy, which essence is related with the ability to exercise control over information about oneself. Alan Westin stated: "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]. The similar theory presented Charles Fried: "Privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves."[17] This theory focuses on information and thus it could be valued as too narrow, because it excludes those aspects of privacy that are not informational, such as the right to make certain decisions about one's body. Also, this theory fails to define the types of information over which individuals should have control, therefore it could be evaluated as too vague. In addition to failing to exactly define the scope of information, *control over information* conception fails to define what is meant by "control". Ordinarily, control is understood as a form of ownership of information. According to John Locke, "Every man has a property in his own person: this no body has any right to but himself"[18]. Conceptualizing of personal information as a property is upholding by viewing it as an extension of personality. As the authors of our own lives, we create information as we develop our personalities. Such extension of property's concepts to personal information meets difficulties. Information can be easily transferred and, once known by others, cannot be eliminated from their minds.

One more conception of privacy is known as "*personhood*" – the protection of one's personality, individuality and dignity. According Daniel Solove, "The theory of privacy as personhood differs from the theories discussed earlier because it is constructed around a

[15] California v. Greenwood, 486 U.S. 35 (1988) [2011-09-24] < http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&vol=486&invol=35>
[16] Westin, A. *Privacy and Freedom*. New York: Atheneum, 1967, p. 7.
[17] Fried, Ch., *Privacy: A Moral Analysis*,Yale Law Journal 77(1), 1968, p. 482.
[18] Locke, J., Second Treatise of Government,1690, Chapter 5 „Of property" [2011-09-25] < http://www.constitution.org/jl/2ndtr05.txt>

normative end of privacy, namely, the protection of the integrity of personality"[19]. This theory is related with the other theories, and it often is used in connection with them explaining why privacy is important, what aspects of the self should be limited, or what information we should have control over. There are certain types of decisions of an individual, which are very important and essential defining personhood: they are decisions related to marriage, procreation, contraception, family relationships, etc. Theory of privacy as personhood, however, fails to explain what privacy is, because it does not provide an adequate definition of personhood.

"Intimacy" is another theory about privacy, which include control over or limited access to, one's intimate relationships or aspects of life. Julie Innes proposed an intimacy conception of privacy: "The content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three area […] I suggest that these apparently disparate areas are linked by the common denominator of intimacy – privacy's content covers intimate information, access, and decisions."[20] J. Innes distinguished several important aspects in the privacy, including intimacy, secrecy, autonomy, liberty, isolation, care, love, and respect for persons. According "*Intimacy*" theory, privacy protects intimate access to ourselves, intimate information about ourselves, and intimate decisions that we make. It is worth to mention, that the nature of intimacy could be different in different cultures (for example, kissing is often an intimate act, but it could be interpreted otherwise, because in certain cultures it might be equal to a non intimate gesture like handshake). Hence, privacy, understandable as "intimacy", claims to preserve autonomy with respect to our expression of love, care or liking. Privacy as "intimacy" theory is too narrow, because it involves just interpersonal relationships and the particular feelings engendered by them. Even information about our finances is not intimate, it is still private.

Some of the above mentioned conceptions concentrate on the ends or goals of privacy, while others focus on the means to achieve privacy. There is an overlap among those conceptions and all of them could be evaluated as complementary.

[19] Solove, D. p. 30.
[20] Ines, J. *Privacy, Intimacy, and Isolation*. New York and Oxford: Oxford University Press, 1992, P.56.

Various types of privacy behaviors are used in order to explain a desired level of access by others to one's self. Dahrl Pedersen introduced six types of privacy—solitude, isolation, anonymity, reserve, intimacy with friends, and intimacy with family[21].

Another way to explain what privacy means is to divide it into different types of privacy: (a) physical; (b) informational; (c) organizational; (d) spiritual and intellectual.

To summarize, privacy can be explained as a concept, concentrating on control over information about oneself, as well as broader phenomenon required for human dignity or crucial for intimacy. Also privacy is necessary for the development of various and significant interpersonal relationships, or as the value that gives us the ability to control the access that other have to us, or as a set of norms necessary not only to control access, but also to raise personal expression and choice, or some combinations of these.

During last decades, privacy has been one of the most problematical social issues related with digital electronic information technologies. As Helen Nissenbaum wrote, "since 1960s, when the dominant concern was massive databases of government and other large institutions housed in large stand-alone computers, concerns have multiplied in type and extent as radical transformations of the technology have yielded the remarkable range of present-day systems, including distributed networking, the World Wide Web, mobile devices, video, audio, and biometric surveillance, global positioning, ubiquitous computing, social networks, sensor networks, databases of compiled information, data mining and more"[22]. Thus part of human lives has moved to cyberspace: in many areas of life of individuals began to use digital technologies, especially for communication and commerce. This situation has created new threats to human privacy, therefore privacy issue has been given much attention by the international community.

2. RIGHT TO PRIVACY AND EVOLUTION OF DATA PROTECTION: INTERNATIONAL LEVEL

Despite the fact, that there is no precise and universal definition of privacy, single concept of privacy, almost all countries have laws which ensure the right to privacy. Moreover, there are a lot of international agreements, which oblige countries to keep the same high standard of ensuring individual's right to privacy.

[21] Pedersen, D. M**.** Model for Types of Privacy by Privacy Functions. *Journal of Environmental Psychology*, Volume 19, Issue 4, 1999 December, Pages 397- 405.
[22] Nissenbaum, H. Privacy in Context California, Stanford: Stanford University Press, 2010, p. 1

The most important and historically significant international documents embedded the right to privacy. The Universal Declaration of Human Rights, adopted by the United Nations in 1948, states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[23] European Convention for the Protection of Human Rights and Fundamental Freedoms, adopted by the Council of Europe in 1953, enshrines right to respect for private and family life:" Everyone has the right to respect for his private and family life, his home and his correspondence." [24] This right involves not just preventing intimate acts or one's body from being seen by others, preventing unwelcome searching of one's personal possessions, preventing unauthorized access to one's home, but also it involves protection from all possible invasions to our privacy. Prof. Jeffrey Rosen noticed, that the internet has raised new concerns about privacy in an age where computers can permanently store records of everything, "where every online photo, status update, Twitter post and blog entry by and about us can be stored forever"[25]

In 1980, the Organization for Economic Cooperation and development (OECD) issued its Privacy Guidelines[26], which were determined by changed situation in societies. As the 1970s may be described as a period of intensified legislative activities concerning the protection of privacy with respect to the collection and use of personal data, the OECD decided to deal with the problems of diverging national legislation. Thus, in 1978 OECD formed a group of experts to create Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to assist the harmonization of national legislation. The group of experts noticed that public interest focused on the risks and implications related with the computerized processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries chose a more general approach to privacy protection issues no matter of the particular data processing technology involved.

OECD experts noticed the legal problems of automatic data processing (ADP), which cause difficulties with the protection of privacy and individual. The ubiquitous use of

[23] The Universal Declaration of Human Rights, Article 12 [2011-09-20] <http://www.un.org/en/documents/udhr>
[24] Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 [2011-09-20] <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf>
[25] Jeffrey, R. *The Web Means the End of Forgetting*. New Yotk Times, July 19, 2010.
[26] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [2011-09-20] <http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html>

computers for the processing of personal data, significantly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically spread locations and lets the pooling of data and the creation of complex national and international data networks, caused widely debated concern about ADP. Experts concluded that certain problems required „particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.“[27]

There are similar approaches to protection of privacy and individual liberties adopted by the various countries, therefore it is possible to identify certain main interests which are considered to be basic components of the area of protection. Some recognized principles of this type are: (1) setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; (2) restricting the usage of data to conform with openly specified purposes; (3) creating facilities for individuals to learn of the existence and contents of data and have data corrected; (4) the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions.

Those countries, which enacted laws intending to ensure the right to privacy and to protect individuals against abuse of data relating to them, and to give them the right of access to data, attempted to cover the successive stages of the cycle beginning with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

Despite that fact, that countries made efforts to regulate protection of personal data enacting particular laws, we have to admit that the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The enormous increase in data flows across national borders and the creation of international data banks showed the need for coordinated national action and at the same time motivate arguments in favour of free flows of information which must often be balanced

[27] Explanatory memorandum of OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [2011-09-20] <http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html#introduction>

against requirements for data protection and for restrictions on their collection, processing and dissemination.

In order to protect person's right to private life, with regard to the automatic processing of the personal data, in 1981 the Council of Europe drafted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[28]. The aim of the Convention is „to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")"[29]. Convention proposed definitions of "personal data" (which means any information relating to an identified or identifiable individual); of "automated data file" (which means any set of data undergoing automatic processing); of "automatic processing" (which includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination) and of "controller of the file" (which means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.). The Convention was the first legally binding international treaty in the data protection field. Under this Convention, the parties must take the necessary steps in their domestic legislation order to ensure the rights of all individuals with regard to processing of personal data.

In 1995, the European Union's Directive on Data Protection was issued, specifying fundamental principles for privacy protection in Europe[30]. The economic and social integration related to operating of the internal European market caused a substantial increase in cross-border flows of personal data. Therefore Directive was issued in order to create the standards and principles of the protection of personal data. Directive is like a regulatory framework which aims to find a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. The Directive

[28] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [2011-08-20] <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

[29] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Article 1 [2011-08-20] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.*

[30] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [2011-09-20] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

sets strict limits on the collection and use of personal data and requires that each Member State set up an independent national body responsible for the protection of these data. The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by creating guidelines determining when this processing is lawful.

This Directive established basic principles: (1) the right to know where the data originated; (2) the right to have inaccurate data rectified, (3) a right of recourse in the event of unlawful processing and (4) the right to withhold permission to use data in some circumstances.

In 1997, The European Union supplemented the 1995 Directive by introducing the Telecommunications privacy directive[31]. The object of this Directive is to provide for "the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community."[32] The directive set forth specific protections encompassing telephone, digital television, mobile networks and other telecommunications systems. It obliged carriers and service providers to ensure the privacy of user's communications, including Internet-related activities. "The provider of a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security."[33] Directive obliges Member States to ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. Member states shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users. There are exceptions of the right to privacy, and confidentiality of communication is not ensured when there is a necessary measure to safeguard national security, defence, public security, the prevention, investigation,

[31] Directive 97/66/EC of the European Parliament and of the Council of 15 Decenber 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. [2011-09-22] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:024:0001:0001:EN:PDF>.

[32] Directive 97/66/EC of the European Parliament and of the Council of 15 Decenber 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. Article 1 [2011-09-22] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:024:0001:0001:EN:PDF>

[33] Directive 97/66/EC of the European Parliament and of the Council of 15 Decenber 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. Article 4 [2011-09-22] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:024:0001:0001:EN:PDF>

detection and prosecution of criminal offences or of unauthorised use of the telecommunications system.

Events on September 11, 2001 in the United States of America changed world significantly. The political climate changed and almost all countries raised a question about national security. This issue was one of the reasons to start discussions about data retention and to look for the right balance between privacy and the needs of the law enforcement agencies in the light of the fighting against terrorism. Thus, in 2002, The European Union Council adopted the Privacy and Electronic Communications Directive[34]. This Directive seeks to respect the fundamental rights and concerns the processing of personal data relating to the delivery of communications services. It deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies. The Directive also regulates data retention issue and, according the Directive, Member States may withdraw the protection of data only to allow criminal investigations or to safeguard national security, defence and public security. Such action may be taken only where it constitutes a "necessary, appropriate and proportionate measure within a democratic society". In order to ensure the availability of communication data for the purpose of investigation, detection and prosecution of criminal offences, the Directive lays down provisions for the retention of data: .

It was noticed, that the Internet changed traditional market structures by providing a global infrastructure for the delivery of a wide range of electronic communications services. Advanced electronic communications services over the Internet created new possibilities for users but also new risks for their personal data and privacy. Therefore, according this Directive, “Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should

[34] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2011-09-28] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF

inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service".

On 2006 the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 was issued by European Parliament and Council. This document requires that at member state level each EU country should have national law on data retention. The data retention regulations should impact public communication providers (fixed, mobile telecoms) that have communications data generated or processed on their networks or from using the services they provide. The regulations require traffic, location and subscriber data to be retained for a minimum of 6 months up to 4 years – so called storage of call detail records (CDRs) and transaction data (IPDRs).

The regulations also outline four data security principles that should apply to retained data:

- data must have the same security levels when retained and must remain the same quality;
- technical and organisational measures should be adequate in order to protect against accidental or unlawful disclosure, access, alteration and loss;
- retained data must be able to be accessed only by authorised persons;
- all data retained must be destroyed at the end of the retention period.

When data is requested by law enforcement the data must be transmitted "without undue delay". But the request for the information will be possible only with a court order. Summarizing, this Directive determines a process for recording details of who communicated with whom by various electronic communications systems. Even physical location of a person, who used mobile phone, is also recorded.

Directive states: "Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period,

subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure."[35] Nevertheless, there are a lot of doubts about compliance of the Directive with ECHR. As Peter Hustinx, European Data Protection supervisor stated, "The Directive is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects."[36] Thus, even if there are specific needs in societies of withdrawing the protection of data (in order to make criminal investigations or to safeguard national security, defence and public security), it appears to be worldwide consensus about the importance of privacy and the need for its protection. Privacy is recognized as a fundamental human right. „Privacy is an issue of profound importance around the world. In nearly every nation, numerous statutes, constitutional rights, and judicial decisions seek to protect privacy".[37]

CONCLUSIONS

Privacy by definition is a personal right. Despite the fact, that the same term ("privacy") is used in different countries, this term means many things in different context. Different legal systems, culture and people have a variety of expectations about how much privacy a person is entitled to.

There are a few slightly different conceptions of privacy, emphasizing different aspects of the right to privacy: "*the right to be let alone, "limited access to the self*", "*secrecy*", *"control over personal information",* "*personhood*", *"intimacy"*. Some of privacy conceptions concentrate on the ends or goals of privacy, while others focus on means to achieve privacy. There is an overlap among those conceptions and all of them could be evaluated as complementary. Privacy can be explained as a theory concentrating on control over information about oneself, as well as a broader concept required for human dignity or crucial for intimacy. Also privacy is necessary for the development of various and significant interpersonal relationships, or as the value that gives us the ability to control the access other

[35] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly acailable electronic communications services or of public communications networks and amending Directive 2002/58/EC [2011-10-01] < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT>

[36] Hustinx, P. *"The moment of truth for the Data Retention Directive",* Conference "Taking on the Data Retention Directive", [2011-09-28] <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf>

[37] Solove, D.J. *Understanding Privacy*. Harvard University Press, 2009, p.2.

have to us, or as a set of norms necessary not only to control access but also to raise personal expression and choice, or some combinations of these.

During last decades, privacy has been one of the most problematical social issues related with development of digital electronic information technologies. A specific part of human lives has moved to cyberspace, individuals began to use digital technologies in many areas of life , especially in communication and commerce. This situation has created new threats to human privacy.

Privacy became legally protected value. The right to privacy has been embedded into the main laws of many states – constitutions, international agreements, etc. International agreements oblige countries to keep the same high standard of ensuring individual's right to privacy. However, development of new technologies simultaneously raised not only new threats for privacy, but also formulated a need for such legal regulation, which limits right to privacy.

There are a few EU Directives issued in order to create the standards and principles of the protection of personal data and safe use of informational technologies. After several terrorist acts, European legislation tried to balance values of the right to privacy and national security. The issue of national security was one of the reasons to legitimize data retention in the field of Electronic Communications.

REFERENCES

1. Bok, S., Secrets:on the Ethics of Concealment and Revelation, Oxford University Press, 1984, p. 10-11
2. California v. Greenwood, 486 U.S. 35 (1988) < http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&vol=486&invol=35>
3. Convention for the Protection of Human Rights and Fundamental Freedoms, http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf
4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
5. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF
6. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT>

7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
8. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:024:0001:0001:EN:PDF>
9. Explanatory memorandum of OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html#introduction>
10. Fried, Ch., *Privacy: A Moral Analysis*“, Yale Law Journal 77(1), 1968
11. Hustinx, P. *"The moment of truth for the Data Retention Directive",* Conference "Taking on the Data Retention Directive", <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf>
12. Ines, J. Privacy, Intimacy, and Isolation, New York and Oxford: Oxford University Press, 1992
13. Jeffrey, R., The Web Means the End of Forgetting“, New York Times, July 19, 2010
14. Locke, J., Second Treatise of Government,1690, Chapter 5 „Of property“ < http://www.constitution.org/jl/2ndtr05.txt>
15. Miller, A.R.,The Assault on Privacy: Computers, Data Banks, and Dossiers, University of Michigan Press, 1971
16. Nissenbaum, H. Privacy in Context California, Stanford: Stanford University Press, 2010
17. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html>
18. Olmstead v. United States, 277 U.S. 277 U.S. 438, 478 (1928) <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=277&invol=438>
19. Pedersen, D. M. , Model for Types of Privacy by Privacy Functions, Journal of Environmental Psychology, Volume 19, Issue 4, 1999 December
20. Posner, R.A. The Economics of Justice, Harvard University Press., 1981
21. Raines, J.C., Attack on Privacy, Judson Press, 1974
22. Smith, R.E., Privacy: How to Protect What’s Left of It, Anchor Press, 1979
23. Solove, D.J. *Understanding Privacy*. Harvard University Press., 2009
24. The Universal Declaration of Human Rights, <http://www.un.org/en/documents/udhr>
25. Time, Inc. v. Hill, 385 U. S., 374 (1967) < http://supreme.justia.com/us/385/374>
26. Vaitkevičiūtė, V. Tarptautinių žodžių žodynas [Dictionary of International Words].Vilnius: Žodynas, 2001
27. Warren, S., Brandeis, L. „*The Right to Privacy*“, 4 Harvard Law Review 193, 1890
28. Westin, A. Privacy and Freedom, New York: Atheneum, 1967

ISSN 2029-1701

Mokslinių straipsnių rinkinys
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2011 (6) Scientific articles

TEISĖ Į PRIVATUMĄ INFORMACINIŲ TECHNOLOGIJŲ VYSTYMOSI KONTEKSTE

Birutė Pranevičienė*
Mykolo Romerio universitetas

S a n t r a u k a

Teisė į privatumą yra laikoma viena iš pagrindinių ir neatimamų žmogaus teisių, kuri civilizuotoje visuomenėje turėtų būti apsaugota. Tačiau vykstantys pokyčiai visuomenėse, besivystančios ir vis plačiau naudojamos kompiuterinės technologijos iškėlė naujus iššūkius teisės į privatumą užtikrinimo sistemoje.

Straipsnyje analizuojama teisės į privatumą ir teisėtų lūkesčių dėl privatumo apsaugos problema. Straipsnį sudaro dvi dalys. Pirmoje dalyje pristatomos teisės į privatumą ypatybės, atskleidžiamos grėsmės privatumui ir teisinės privatumo apsaugos poreikis. Aptariamos skirtingos privatumą aiškinančios koncepcijos ir dėl informacinių technologijų naudojimo atsirandančios grėsmės asmens privatumui. Antrojoje straipsnio dalyje tiriama privatumo teisinė apsauga informacinių technologijų naudojimo srityje, analizuojami tarptautiniai dokumentai, užtikrinantys teisę į privatumą. Straipsnyje prieinama išvados, kad per pastaruosius dešimtmečius privatumas buvo ir yra vienas iš labiausiai probleminių klausimų, susijusių su skaitmeninių elektroninių informacinių technologijų plėtra. Dalis žmonių gyvenimo persikėlė į elektroninę erdvę, daugelyje žmonių gyvenimo sričių buvo pradėtos naudoti skaitmeninės technologijos. Ši situacija sukėlė naujas grėsmes žmonių privatumui. Todėl asmens privatumas tapo teisės saugoma vertybė. Teisė į privatumą buvo įtvirtinta daugelio valstybių teisėje – konstitucijose, tarptautinėse sutartyse ir kt. Tarptautinės sutartys įpareigoja valstybes išlaikyti tuos pačius aukštus standartus, užtikrinant asmens teisę į privatumą. Tačiau tuo pačiu metu naujų technologijų išsivystymas kelia ne tik naujas grėsmes privatumui, bet ir nulemia teisinį reguliavimą, kuris apriboja teisę į privatumą. Todėl ES direktyvos nustatė ne tik asmens duomenų apsaugos standartus ir informacinių technologijų saugaus naudojimo principus, bet taip pat įteisino duomenų rinkimą bei saugojimą elektroninių ryšių srityje.

Reikšminiai žodžiai: teisė į privatumą, žmogaus teisės, elektroninė erdvė, informacinės technologijos, asmens duomenys.

Birutė Pranevičienė*, Mykolo Romerio universiteto Viešojo saugumo fakulteto Teisės katedros profesorė. Mokslinių tyrimų kryptys: administracinė teisė, konstitucinė teisė.
Birutė Pranevičienė*, Mykolas Romeris University, Faculty of Public security, Department of Law, professor. Research interests: administrative law, constitutional law.