ISSN 1392–6195 (print)
ISSN 2029–2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2012, 19(2), p. 697–713.

WORKPLACE PRIVACY: DIFFERENT VIEWS AND ARISING ISSUES

Tomas Bagdanskis, Paulius Sartatavičius

Mykolas Romeris University, Faculty of Law,
Department of Labour Law and Social Security
Ateities 20, LT-08303 Vilnius, Lithuania
Telephone (+370 5) 2714 633
E-mail: tomas@bagdanskis.lt

Received on 1 June, 2012; accepted on 26 June, 2012

Abstract. *This article discusses the problematic aspects relating to the employee privacy in his workplace and its limits reacting to employer's interests. It contains analysis of National, European and transatlantic legislation of privacy in the workplace and concentrates on the electronic privacy (e-mails, communications, etc.). The article is based on legal acts and judgements of the Supreme court of Lithuania, European Court of Human Rights and other countries courts judgements in order to provide the legislative execution practice as well as reveal the problems in this field of labour law.*

Keywords: *workplace privacy, employee, employer, privacy security, fundamental rights, privacy legislation.*

Introduction

Although the law and international practice dictates that individual's privacy should be protected, in some countries, including Lithuania, employees are still afraid to claim their right to privacy in workplace or even are not aware of the legal base and their rights.

The purpose of this article is to analyze the workplace privacy implementation and legal issues related to it as well as the current situation in practice and in theory focusing on Europe, USA and Lithuanian legal base and its fulfillment.

To achieve this objective, the legal regulation will be analyzed in terms of privacy protection. Judicial practice shall be analyzed in order to reveal the problematic aspects of current situation. This article discloses and summarizes the problems arising in the field of theory and practice.

This topic is relevant in today‘s society because privacy is highly valued nowadays and some employers fail to understand and properly apply the privacy laws and other privacy requirements and often abuse the employers possition thus violating the privacy of employees.

1. Right to Privacy and Privacy Definition in Labour Law

Right to privacy is one of the few basic rights that at the same time can and cannot be described in few words. Right to privacy is the individuals right to have a private and domestic life that no one could track or get involved in without the consent of the individual.

As a matter of fact it is hard to tell if unified definition of privacy and right to privacy can be determined. Although there are some long lasting definitions.

Alan Westin describes privacy as the ability to determine for ourselves when, how, and to what extent information about us is communicated to others[1].

Other fundamental view is provided by Ruth Gavison, who claims that interests in privacy are related to concerns over accessibility to others, that is, what others know about us, the extent to which they have physical access to us, and the extent to which we are the subject of the attention of others. “Thus the concept of privacy is best understood as a concern for limited accessibility and one has perfect privacy when one is completely inaccessible to others.”[2] Privacy can be gained in three independent but interrelated ways:

1) through secrecy, when no one has information about one;
2) through anonymity, when no one pays attention to one;
3) and through solitude, when no one has physical access to one.[3]

Talking about privacy, there are 4 main privacy “types”, elements:

1) Informational privacy (the right to control the information associated with you) In labour law it can be described as knowing where the information gathered about you by the employer is being used;
2) Physical privacy (bodily integrity – no one can perform medical or scientific experiments without the consent of the subject);

1 Westin, A. *Privacy and Freedom.* New York: Atheneum, 1967.

2 Gavison, R. Privacy and the Limits of Law. *Yale Law Journal.* 1980, 89: 421−71.

3 *Ibid.*

3) Communicational privacy (conversation over telephone, e-mail and other communications). In labour law perspective it means that right to communicate with others not associated with business relations must be respected;
4) Territorial privacy (personal integrity of the housing and private territory).

In modern times right to privacy evolved, especially regarding the all new environment in cyberspace and its development nowadays. Right to privacy is now protected by national laws and international doctrines and is even ensured by the Charter of Fundamental Rights of European Union[4] and should mean that individual's privacy is guaranteed in workplace as well as anywhere else. Lithuanian Supreme Court provided such a conclusion:

Private life - is a human right to live as he wants, to establish and maintain relationships with others, to be protected against arbitrary interference with his private life, thus making parts of this life public. Freedom of a private life is a win-win recognition of the existence of a space that belongs to the same person and that others may not enter into. According to professor V. Mikelėnas, „... what to consider a private life is often a question of the fact, because this definition is an evaluative criteria based on phenomenon: the qualification of privacy and publicity depends on many factors."[5]

But the question rises, what is the current situation. Before moving onto the privacy in the workplace, employer often uses the Internet to gather information about job applicant.

Jackson Lewis LLP recently conducted a survey of employers in the New York metropolitan areas to determine how online social networking sites have affected the employer-employee relationship. It revealed that some employers use these sites as an informative recruiting and screening tool. Even after a job offer is made, online social networking may impact employment. The thing is that no federal laws (talking about United States) expressly prohibit this kind of information gathering and only few states argue about it[6].

Employee, as a person has the right to private life and expects that this right of his will not be violated even in his workplace. However there is a number of reasons and conditions forcing employers to undertake monitoring and control of the employee in his workplace with the help of electronic devices. Authors distinguish these main reasons:

1) Ensuring employee's working order and discipline;
2) Improving employee productivity and efficiency;
3) Saving employers financial resources;
4) Preservation of employers good reputation;
5) Meeting the computer system security and performance needs.

---

4 European convention on human rights [interactive]. [accessed on 12-04-2012]. <http://eur-lex.europa.eu/lt/treaties/dat/32007X1214/htm/C2007303LT.01000101.htm>.

5 Mikelėnas, V. The right to privacy. In: Petrauskienė (ed.). *Moral rights and their protection.* Vilnius: Justitia, 2001, p. 84.

6 Siegel, P. J.; Shields, A. C.; Lewis, J. Should Employers "Google" Applicants? February 2009 [interactive]. [accessed on 15-04-2012]. <http://www.irmi.com/expert/articles/2009/siegel02-employment-practices-liability.aspx>.

In different law traditions employer and employee relations controlling employee's electronic workplace is legislated differently.

2. European Approach to Workplace Privacy and Arising Issues

In Europe a lot of attention is being paid to workplace privacy and its legislation compared to United States example.

European Convention on Human Rights Article 8 guarantees every person the right to private and family life, home and correspondence[7]. These are the fundamental rights given to everyone and it affects the privacy in all areas of life.

One of the main acts that established a whole bunch of principles for employee e-mail monitoring is the European Parliament and Council Directive on the person protection of personal data and on the free movement of such data[8].

European Court of Human Rights (ECHR), whose decisions are binding to all member states (including Lithuania), in the *Niemietz v. Germany* case, stated that protection of private life includes workplace[9]. In this case a lawyer complained that a search of his offices was an interference with his private life. The court held: In construing the term 'private life', 'it would be too restrictive to limit the notion of an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.' Article 8 should not be construed as necessarily excluding business activities.

In respect to few precedential decisions made by European Court of Human Rights, the basic principles regarding the protection of electronic workplace can be summarized. A workgroup (formed according to EU General Data Protection Directive 95/46/EC, Article 29[10] consisting of various national data protection authorities (data Protection Working Party)) mentions *Halford v. United Kingdom* and other ECHR case-files and sets out three principles to be applied to electronic workplace:

1) Employees have a legitimate expectation of privacy at the workplace, which is not overridden by the fact workers use communication devices or any other business facilities of the employer.
   However the provision of proper information by the employer to the employee may reduce the employee's legitimate expectation of privacy.

---

7 European convention on human rights, *supra* note 4.

8 European Parliament Directive of 24 10 1995 for the protection of personal data and on the free movement of such data 95/46/EC, Official Journal L, Nr. 281 1995-31.

9 Case: *Niemietz v. Germany*, No. 13710/88, ECHR, Judgment of 16 December 1992, A251-B.

10 European Parliament and Council directive of General Data Protection 1995-10-24, 95/46/EC [interactive]. [accessed on 16-04-2012]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF>.

2) The general principle of secrecy of correspondence covers communications at the workplace. This is likely to include electronic e-mail and related files attached thereto.
3) Respect for private life also includes to a certain degree the right to establish and develop relationships with other human beings. The fact that such relationships, to a great extent, take place at the workplace puts limits to employer's legitimate need for surveillance measures.[11]

Right to privacy must be balanced with other rights and legitimate interests, particularly with the employer's right to operate efficiently, to a certain degree, and, among other things, to protect themselves from liability or damage which may result in the worker's actions. These rights and interests is a legitimate reason that can justify certain measures to limit the employee's right to privacy.

In practice, often thought that if the employer warns the employee in advance of the procedures limiting his right to privacy, for example, the possibility to take over his e-mails, the employee cannot expect privacy. Although early warning is an important element in limiting the electronic workplace privacy, but it is not sufficient. Employers must not only clearly define conditions for the control of electronic information in the workplace, but also follow the fundamental principles of privacy limitation, that means there must be a legal basis and such a restriction must pursue a legitimate aim and be proportionate to those objectives.

Talking about the legal basis, at the moment the main European Union document partly regulating the relationship between the employer and the employee in the matter of controlling electronic workplace is the European Parliament and Council Directive on the protection of personal data and on the free movement of such data (95/46/EC). This Directive lays down the general principles under which data controllers must process personal data (including employers handling employees personal data), but is not intended to specifically regulate electronic workplace monitoring. In 2002, the EU has raised an initiative to regulate the electronic privacy of employees in the workplace at the European Union level[12]. Initiatives have included the following:

1) Employee's consent to processing of personal data carried out by the employer;
2) Access to sensitive data and processing of such data;
3) Drug Abuse Control;
4) Employee communications monitoring and control.

However, the above-mentioned motion (initiative) after a series of hearings was not adopted. In considering this initiative, it was argued that the employee's personal data is to be kept by the employer in accordance with the requirements of Directive 95/46/EC. It was also assumed that the electronic workplace security need not be regulated

11 „Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace", 29-05-2002 [interactive]. [accessed on 16-04-2012]. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf>.

12 Initiative on Privacy Standardization in Europe, IPSE Report Final, 13-02-2002 [interactive]. [accessed on 16-04-2012]. <http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/ipsefinalreportwebversion.pdf>.

at EU level - each state can do this at the national level. In accordance to that, some member states already adopted legislation governing electronic workplace monitoring. At the national level, the first legislation regulating privacy in the workplace was in 2001 Finland's protection of privacy in the work activities act[13].

The 6th section of the law governs the interception of employer-owned e-mail messages. The principal rule - in some cases, the employer may control (monitor) e-mails belonging to him, if the fulfilment of certain conditions exists (i.e., e-mail message must be related to labour relations, e-mail messages can be opened only in the presence server administrator and others). Section 6 of the act in detail describes *The employer's obligations regarding necessary arrangements:* The employer has the right to retrieve and open electronic mail messages sent to an electronic mail address allocated by him for the use of the employee or electronic mail messages sent by the employee from such an address only if the employer has planned and arranged for the employee the necessary measures to protect electronic mail messages sent in the employee's name or by the employee and, to this end, has specifically ensured that:

1) The employee can, with the aid of the electronic mail system's automatic reply function, send notification to a message sender about his/her absence and the length of absence, and information about the person who is to take care of the tasks of the absent employee; or
2) The employee can direct messages to another person approved by the employer for this task or to another employer-approved address of the employee; or
3) The employee can give his/her consent to an arrangement whereby in his/her absence another person of his/her choosing and approved by the employer for the task can receive messages sent to the employee, with the aim of establishing whether the employee has been sent a message that is clearly intended for the employer for the purpose of managing the work and on which it is essential for the employer to have information on account of his operations or the appropriate organization of the work.

Section 20 (*Opening of electronic messages belonging to the employer*) of the mentioned act provides:

(1) If, on the basis of the information on the sender or recipient of an electronic message or the message title, it is apparent that a message sent to the employee or by the employee is clearly one that belongs to the employer and about whose content it is essential that the employer obtains information in order to complete negotiations concerning his operations or to serve customers or safeguard his operations, and the message sender and recipient cannot be contacted for the purpose of establishing the content of the message or for the purpose of sending it to an address indicated by the employer, the employer may, in cases referred to in section 19, open the message with the assistance of the person vested with the authority of information system administrator and in the presence of another person.

---

13 Act on the Protection of Privacy in Working Life, 01-10-2004, (759/2004), Finland [interactive]. [accessed on 16-04-2012]. <http://ec.europa.eu/justice/policies/privacy/docs/implementation/finland_759_04_en.pdf>.

(2) A report about the opening shall be drawn up, signed by the persons involved, stating which message was opened, why it was opened, the time of opening[14]... and so on.

In fact, Finland has the most detailed legislation of the privacy issues in the workplace, so it‘s approach could be stated as an example to other member states. One other interesting aspect of Finland‘s legislation of workplace privacy is that even the physical workstation must be build in the manner that no one from the entrance to the workplace or from any other place of the room except from the employee position could see the employee computer monitor.

Workplace monitoring also includes the visual (Camera) surveillance. Finland‘s privacy control act states that the employer may operate a system of continuous surveillance within his premises based on the use of technical equipment which transmits or records images (camera surveillance) for the purpose of ensuring the personal security of employees and other persons on the premises, protecting property or supervising the proper operation of production processes, and for preventing or investigating situations that endanger safety, property or the production process. Camera surveillance may not, however, be used for the surveillance of a particular employee or particular employees in the workplace. Neither may camera surveillance be used in lavatories, changing rooms or other similar places, in other staff facilities or in work rooms designated for the personal use of employees.

So it is seen that visual monitoring is allowed only for the safety of employee and the assets. That does not mean that camera can be directed at the computer monitor in that matter violating other sections of the law.

One of the cases that has caused the biggest repercussions in society - telecommunication services company Sonera Safety Division employee privacy infringement case. The five defendants - former Sonera security department employees, has been convicted for having secretly and illegally monitored phone conversations of other Sonera employees.[15] This case is an example for other employers that secret and unlawful interception of telephone conversations of employees (control) are punishable as criminal offenses.

Similar initiatives as in Finland can be found in other EU countries as well. Special electronic workplace privacy legislation acts are in force in Portugal, Austria, France and Italy.

3. Lithuanian Issues Regarding Workplace Privacy

In May 8, 2000 ruling of the Constitutional Court stated that the legal concept of privacy is related to personal status when a person can expect privacy, with the

14 Act on the Protection of Privacy in Working Life, 01-10-2004, (759/2004), Finland, *supra* note 13.

15 “Five get suspended sentences in Sonera telephone record case Appeals expected“ article of “Helsinki Sanomat” [interactive]. [accessed on 16-04-2012]. <http://www.hs.fi/english/article/1101979719153>.

legitimate expectations of private life[16]. If a person performs acts of a public nature, and understands that or can and should understand, even though in his house or other private premises, this kind of public activities will not be the subject of protection under Article 22 of the Constitution of Lithuanian Republic and Article 8 of the Convention, and the person cannot expect privacy.

Overall the main law regulating employer-employee relationship in Lithuania is the Labour Code of Republic of Lithuania[17]. Unfortunately, this law does not regulate the electronic workplace security. Law on Legal Protection of Personal Data of Lithuanian Republic[18] lays down the conditions and principles regarding the legitimacy of collection of personal data. Based on these principles, an employer may collect the employee's personal data, but this collection of personal data is related to informational privacy and does not include employee's communicational privacy.

In fact Lithuania is missing at least the minimum legal regulation of relations between employer and employee within the meaning of privacy. That kind of regulation should help to avoid ambiguities.

The Constitutional Court of Lithuanian Republic said that under the Constitution to limit the constitutional rights and freedoms may be allowed if the following conditions exist:

1) It is done by the law;
2) Restrictions are necessary in a democratic society for the protection of the rights and freedoms and values enshrined in the Constitution;
3) In the matter of constitutionally important objectives;
4) The restrictions do not deny the nature and essence of the rights and freedoms;
5) The Constitutional principle of proportionality is not violated.[19]

European Convention of Human Rights Article 8 also provides: "State authorities have no right to limit the exercise of these rights, except for cases prescribed by law and when it is necessary in a democratic society for national security, public safety or the economic well-being, for the prevention of disorder or crime, for the protection of health or morals, or the rights and freedoms"[20]. Thus, the employer unlawfully limiting the worker's right to privacy, for example. Illegally controlling employee's e-mail messages or phone calls, can even be held **criminally** liable (as mentioned above). It is therefore very important that in this area there would be more clarity, especially for electronic communications related to the communication privacy, control.

16 Ruling of the Constitutional Court of the Republic of Lithuania, issued on 8 May 2000 [interactive]. [accessed on 16-04-2012]. <http://www.lrkt.lt/dokumentai/2000/r000508.htm>.

17 Labour Code of the Republic of Lithuania. *Official Gazette.* 2002, No. 64-2569.

18 Law on Legal Protection of Personal Data of the Republic of Lithuania. *Official Gazette.* 1996, No. 63-1479.

19 Ruling of Constitutional Court of the Republic of Lithuania, issued on 23 October 2002 [interactive]. [accessed on 16-04-2012]. <http://www.lrkt.lt/dokumentai/2002/n021023.htm>.

20 European convention on human rights, *supra* note 4.

3.1. General Principles for the Employee E-Mail and Internet Browsing Supervision (Monitoring)

The main principle that should be followed by employers is the proportionality principle - electronic workplace monitoring must be conducted only when it is absolutely essential. Personal data including the one collected during monitoring must be adequate and proportionate to the objectives of such data. This principle prevents formal employees online activity monitoring (monitoring in the name of monitoring) by limiting it to only those cases where it is absolutely necessary to achieve specific business goals (eg to protect corporate reputation, and so on.).

The other principle that should be followed is the principle of necessity. The 1995 EU Data Protection Directive requires that any employee tracking form, and measures must be absolutely necessary for a particular, pre-set goal. This implies that the employer, before taking any electronic workplace control measures need to assess whether this measure is necessary for a particular purpose. Employee e-mail and web browsing tracking should be regarded as exceptional measures (*ultima ratio*). For example: The employee's e-mail surveillance may become necessary in order to obtain proof that an employee performs a number of unauthorized, unwanted actions at his working time. Tracking can also be justified to protect the employer's informational system (i.e., from the outside hacking, viruses, etc.).

The expediency principle means that the data collected about an employee may only be used for a particular, pre-determined purpose. For example, if the employer informs the employee that collected data can be processed in order to protect the employer's information system, that data later cannot be used for the employee's conduct or performance evaluation.

Principle of transparency states that the employer has to give employee clear and transparent information on its activities related to the control of the electronic workplace and data. Any employee secret e-mail tracking is prohibited (except in relation to public order, public security, etc.). The clearest expression of this principle - the employer must provide employees easily accessible, clear and precise document that would establish basic principles used by an employer of staff overseeing the online activities. It is advisable for the employer to promptly inform the employee of the perceived misuse of e-mail and / or web use case.

Legitimacy principle - Any data processing operation can be carried out only if it is performed a legitimate objective (Article 7 of directive). An example of a legitimate objective - the need to protect the interests of employers against the risks associated with the forwarding of confidential information to a competitor.

Accuracy and storage time principle. This principle requires that any legally collected employee data, including the employee's online activity data must be accurate and kept for no longer than is unavoidably necessary for data processing purposes. The employer should clearly indicate the e-mail messages storage time on a central enterprise server. Generally reasonable storage period should not exceed 3 months.[21]

---

21 Civilka, M. Dar kartą apie darbuotojų privatumą, 2002 [Once again on employee privacy]. [interactive]. [accessed on 16-04-2012]. <http://www.ic.lt/e-teise/Default.asp?DL=L&TopicID=11>.

In conclusion, the principle of consent, although it is not absolute, is actually necessary. The thing is that in order to monitor employee's electronic communications employer has to agree with before mentioned principles and get the employee's consent, that way any surveillance initiated in violation of these basic principles leads to a situation when this way collected evidence would not be assessed in court. If the employer is actually thinking about employee monitoring, the main advise regarding online monitoring, is not to monitor employee's actions online but to block certain websites (i.e. new sites, social media, etc.) and specify that e-mail can be used only for direct work purposes. That way no questions related to privacy violation should arise.

In the Lithuanian Supreme Court practice in the case *J.B v. Viešoji įstaiga „Humana people to people Baltic"* the court stated that: "<...> under the Article 2.23 of the Civil Code of Lithuanian Republic, according to established legal concept of privacy private is a person's life, which is not in public <...> public workplace is not a private personal sphere. The seller cannot demand that his right to privacy would be ensured in his workplace that is the sales room (hall), so the monitoring of the sales room, together with the employee work is not a secret surveillance of person's private life".[22]

That means that in a workplace that is not publicly available, the employee may have a right to privacy and this right must be respected. However the question remains in which case employee can expect privacy in the workplace and in which not.

Another case that has relevance is the Supreme administrative court of Lithuania case Nr. A[662]-3548/2011, the court stated that employee can object to the processing of his personal data, in this case – image.[23]

The National Labour Inspection also noted that if the employer fails to comply with the requirements set by law or the employee proves that his interests are more important for trade protection, which can be done by any other means, he may object to the processing of personal data.[24]

3.2. Voice Recording

One more aspect regarding infringements of privacy is voice recording. For example, if a person willingly records his own conversation with another person without consent of that other person, not only he violates privacy of that other person but also could inflict a criminal violation. If the mentioned conversation is made by special electronic communications then this kind of recording falls under the section 166 of the Criminal Code of the Republic of Lithuania[25].

On the other hand if a conversation is made not by special electronic communications, but directly (face to face), and the recording is made by a recorder or other device that can record sound, this raises a few questions. Firstly, if that kind of recording is made by an undercover officer and is sanctioned by the court or other institution with the authority

22 Supreme Court of Republic of Lithuania ruling in the civil case No. 3K-3-565/2003, 5 May, 2003.

23 Supreme Administrative Court of Republic of Lithuania, case No. A[662]-3548/2011.

24 National Labour Inspection opinion [interactive]. [accessed on 16-04-2012]. <http://www.vdi.lt/index.php?-1950470149>.

25 Criminal Code of the Republic of Lithuania, sec 166. *Official Gazette.* 2000, No. 89-2741.

to sanction surveillance it falls under the Law on Operational Activities of Republic of Lithuania[26]. But the question is, what if a regular person records a conversation? Seems that section 166 of Criminal Code cannot be incriminated because there is no electronic communications. The Law on Operational Activities also cannot be implied because the subject is not an officer. Another important question is if this kind of proof can be used in Court.

In the civil case No. 2A-2706-656/2011 of Vilnius District Court, the Court stated that actually this kind of recording falls under the Law of Operational Activities of Republic of Lithuania. The Court's opinion was that the recording of the conversation, made by employee secretly and without the consent of the other person (employer) cannot be assessed as evidence because it is made in violation of the Law on Operational Activities of Republic of Lithuania.[27]

In conclusion, it should be noted that:

1) It should be assessed if employee's right to privacy limitations is proportional to the protection of employer's interests;
2) It should be assessed if provocation for the recording exists or not;
3) In case special technical measures were used to secretly collect evidence (record), according to case practice, court would not assess this kind of evidence.

3.3. Video Surveillance of the Workplace

Section 2.22 part 1 of Lithuanian Civil Code indicates that:

Photo of a person (or part of it), portrait or other image may be reproduced, sold, displayed, printed, and the person may be photographed only with his consent.[28]

The thing is that Civil Code does not specify in what form this consent must be obtained and that leaves a lot of room for interpretations.

The term "image" includes not only personal photos, portraits or other images that the person depicted, but also parts of the body, from which a person can be identified.

Law on Legal Protection of Personal Data of Republic of Lithuania indicates that video surveillance can be carried out to ensure public safety, public order, protect the life, health, property and other rights and freedoms, but only in cases where other methods or means are insufficient and (or) not suitable for the following purposes and if the data entity's interests are not important.[29]

Video surveillance in the workplace can be initiated when the work specifics requires it to ensure the safety of the persons, property or public and in other cases where other methods or means are insufficient and (or) not suitable for the following purposes[30].

---

26 Law on Operational Activities of Republic of Lithuania. *Official Gazette.* 2002, No. 65-2633.

27 Vilnius District Court, civil case No. 2A-2706-656/2011.

28 Civil Code of Republic of Lithuania, sec. 2.22 part 1. *Official Gazette.* 2000, No. 74-2262.

29 Law on Legal Protection of Personal Data of Republic of Lithuania, sec 3, Video surveillance. *Official Gazette.* 1996, No. 63-1479.

30 *Ibid*.

Law on Legal Protection of Personal Data of Republic of Lithuania also specifies the requirements that need to be met for initiating video surveillance of the workplace. Video data must be approved by the controller in a written document which sets out the purpose of video surveillance and extent of the image data retention period, access to the processed image data by these conditions and data destruction procedures, and the other requirements for lawful processing of image data. The controller ensures that the video data is handled only by persons authorized by the controller who must be aware of the legislation of the legal protection of personal data and must give a signature commitment to comply with this legislation[31].

4. USA View to Workplace Privacy

In order to understand employee's position in the USA the first thing you need to know is that USA and Europe has two radically different approaches to privacy and it's protection, especially when talking about workplace.

The Constitution of USA historically protects employee's electronic workplace very poorly. In US federal and state laws also very little attention is paid in regard to employee's privacy protection. One of the main acts related to protection of employee's privacy in workplace is the Electronic communications privacy act.

The whole legal base and practice show that in US there is an employee-not friendly environment when it comes to privacy protection.

USA electronic communications privacy act[32], though has a purpose to protect privacy during the electronic communications, indicates, that there are three exceptions when an employer is given the right to monitor employees workplace, or in that case electronic workplace:

1) **Providers exception** (when employer provides the equipment – computer, mobile phone, etc.);
2) **Ordinary course of business exception** (empowers the employer to monitor his employees if it is needed to protect corporate interest or assets);
3) **Consent exception** (if consent is given that means right to privacy is void. The main issue is that the consent in US can be foreseeable and does not require active actions to be made).

But these exceptions go beyond mere website blocking or statistical overview of all employees without excluding any individual. Provider exception means that employer is allowed to control the information sent and received by his equipment. That means he can monitor employee's e-mails, skype conversations, facebook profile (if it is not blocked) and so on. This also indicates that sms messages and phone calls are no longer private, because this exception grants the ability to monitor these at well. And of course company's transport is being monitored by GPS.

---

31 Law on Legal Protection of Personal Data of Republic of Lithuania, sec 3, Video surveillance. *Official Gazette.* 1996, No. 63-1479.

32 Electronic Communications Privacy Act, 18 U.S.C. § 2510-20; 2701-2711 (1986).

The second exception grants the ability to monitor employees if there is a slightest suspicion that employee's communications could infringe company's rights and interests. And for that there does not have to be any real evidence.

Third, the consent exception is the most empowering, because if the consent is given then any type of surveillance is possible and no opposition is valid. Employee's consent implies his own right to privacy restriction and means employer's unconditional right to monitor e-workplace. The consent doesn't have to be active. If employee knowing that the possibility to monitor his e-mails exists, still uses the e-mail system it is presumed that he gave his consent.

The fact that employer's workplace monitoring and control interests outweigh employee's right to privacy is shown by few cases examined in California courts.

For example the case *Bourke v. Nissan Corp.*[33] In this case plaintiffs Bonita Bourke and Rhonda Hall appeal the entry of summary judgment in their suit against Nissan Motor Corporation in U.S.A. ("Nissan") alleging wrongful termination, invasion of privacy and violation of their constitutional right to privacy in connection with Nissan's retrieval, printing and reading of E-mail messages authored by plaintiffs. In the original case the court stated that employer had the full right to inspect employee's e-mail because the employee was informed about such possibility. The fact that employee had a password had no effect, since the employee's expectation of privacy was not objectively reasonable.

For a long period of time, employers in the USA had absolutely no boundaries in monitoring and controlling the content of employee's communications. While controlling these communications, employer learns the content of phone calls, e-mails and so on. In the long run USA courts divided the communications to personal and business related. Employers now are concerned about this kind of practice, because it is very difficult to tell if the phone call is private. For example in the case *Watkins v. L.M. Berry&Co* court stated that a personal phone call cannot be intercepted during the normal business practices <…> except when employer needs to protect himself against unauthorized use of telephone or to determine whether the phone call is personal or not.[34] In later case, interception must be immediately terminated as soon as it appears that the call is personal. This is a real problem for employers, because there is no technical possibility to separate private call from business related communication.

In some states, legislation limits the employer's right to monitor employee e-mail without the consent of the employee. For example, in Connecticut there is a state law that prohibits an employer to monitor employee e-mail, without the consent of the employee, subject to certain exceptions. The one exception is that the e-mail surveillance may be conducted without notice, if the employer has reasonable grounds to believe that the employee violated the law or the employee's conduct poses a threat to job security.[35] In

33 USA case: *Bourke v. Nissan Motor Corp*., No. B068705 (Cal. Ct. App. 26 July, 1993).

34 Civil case *Watkins v. L.M. Berry & Co,* No. 82-7007 [interactive]. [accessed on 16-04-2012]. <http://scholar.google.ca/scholar_case?case=11212446034094840663&hl=en&as_sdt=2&as_vis=1&oi=scholarr>.

35 Conn. Gen. Stat. § 31-48d (2008), Id. at § 31-48d(b)(2).

California similar legislation was enacted in 2001. However, these regulatory examples are more the exception than the rule.

At the federal level initiatives in the U.S. Congress were to pass laws that prohibit an employer to monitor employee e-mail. However, none of these laws were adopted.

Both U.S. federal and state laws and court precedents largely favours the interests of employer to monitor employee electronic workplace before the interests of the employee. Judicial interpretation is largely based on the fact that the electronic workplace belongs to employer so he reasonably expects that the workplace is properly used. For this reason, the employer in the United States has broad rights to monitor employee electronic workplace.

Conclusion

The analysis of workplace privacy legislation and its practical application lead to the following conclusions:

1. Privacy in the workplace limits should end there, where a crime or an offense is committed, or law or agreements are violated. Employee privacy cannot be guaranteed in the event of breach or attempted breach of the employer's legitimate business interest.
2. Control of the electronic workplace should be subject to the general data protection principles. It should be noted that complete ignorance of the employer's interests cannot exist, there must be a balance. Practice must not only be governed by the principle of consent.
3. The main issue in Lithuania is that employees should be more active in defending their rights to private life, demanding explanations from employers on electronic workplace control measures.
4. E-workplace monitoring should be carried out only for a specific purpose, the information collected must be adequate and only needed for the legitimate purposes. The data collected should be prohibited to manage for other purposes than those for which they were collected.
5. The employer, in order to monitor employee e-mail should state the following key elements:
    1) Whether the employee is allowed to use provided electronic mail for personal purposes;
    2) When and in what circumstances an employee is authorized to use personal e-mail account;
    3) In what cases e-mail backups are made;
    4) Information on when email messages are being deleted from the server.
6. In the case of internet access tracking, employer should apply technical access control measures, like blocking unwanted websites, as much as possible instead of monitoring the content of employees browsing, e-mails and data.
7. Video and audio surveillance can be initiated only if it is necessary, and if all other measures aren't enough. It should be assessed if employee's right to privacy

limitations is proportional to the protection of employer's interests; it should be assessed if provocation for the recording exists or not; In case special technical measures were used to secretly collect evidence (record), according to case practice, court would not assess this kind of evidence.

8. United States example indicates three absolute and broadly interpreted exceptions when employee privacy can be violated. In European view only "the ordinary course of business exception" can be implied and only when there is a reasonable ground to believe that employee is performing unlawful act that can cause damage to the company.

References

Act on the Protection of Privacy in Working Life, 01-10-2004, (759/2004), Finland [interactive]. [accessed on 16-04-2012]. <http://ec.europa.eu/justice/policies/privacy/docs/implementation/finland_759_04_en.pdf>.

Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace, 29-05-2002 [interactive]. [accessed on 16-04-2012]. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf>.

Case of Supreme Court of Lithuania No. 3K-3-461.

Civil case Watkins v. L.M. Berry & Co, No. 82-7007 [interactive]. [accessed on 16-04-2012]. <http://scholar.google.ca/scholar_case?case=11212446034094840663&hl=en&as_sdt=2&as_vis=1&oi=scholarr>.

Civil Code of the Republic of Lithuania. *Official Gazette.* 2000, No. 74-2262.

Civilka, M. Dar kartą apie darbuotojų privatumą, 2002 [Once again on employee privacy] [interactive]. [accessed on 16-04-2012]. <http://www.ic.lt/e-teise/Default.asp?DL=L&TopicID=11>.

Criminal Code of the Republic of Lithuania. *Official Gazette.* 2000, No. 89-2741.

Electronic Communications Privacy Act, 18 U.S.C. § 2510-20; 2701-2711 (1986).

European Parliament and Council directive of General Data Protection, 1995-10-24, 95/46/EC [interactive]. [accessed on 16-04-2012]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF>.

European Parliament Directive of 24 10 1995 for the protection of personal data and on the free movement of such data, 95/46/EC, Official Journal L 'Nr. 281 1995-31.

Five get suspended sentences in Sonera telephone record case Appeals expected. *Helsinki Sanomat* [interactive]. [accessed on 16-04-2012]. <http://www.hs.fi/english/article/1101979719153>.

Gavison, R. Privacy and the Limits of Law. *Yale Law Journal.* 1980, 89: 421−71.

Initiative on Privacy Standardization in Europe, IPSE Report Final, 13-02-2002 [interactive]. [accessed on 16-04-2012]. <http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/ipsefinalreportwebversion.pdf>.

Labour Code of the Republic of Lithuania. *Official Gazette.* 2002, No. 64-2569.

Law on Legal Protection of Personal Data of the Republic of Lithuania. *Official Gazette.* 1996, No. 63-1479.

Law on Operational Activities of the Republic of Lithuania. *Official Gazette.* 2002, No. 65-2633.

Mikelėnas, V. The right to privacy. In: Petrauskienė, D. (ed.). *Moral rights and their protection.* Vilnius: Justitia, 2001.

National Labour Inspection opinion [interactive]. [accessed on 16-04-2012]. <http://www.vdi.lt/index.php?-1950470149>.

Niemietz v. Germany, No. 13710/88, ECHR, Judgment of 16 December 1992, A251-B.

Ruling of the Constitutional Court of the Republic of Lithuania, issued on 8 May 2000 [interactive]. [accessed on 16-04-2012]. <http://www.lrkt.lt/dokumentai/2000/r000508.htm>.

Ruling of the Constitutional Court of the Republic of Lithuania, issued on 23 October 2002 [interactive]. [accessed on 16-04-2012]. <http://www.lrkt.lt/dokumentai/2002/n021023.htm>.

Siegel, P. J.; Shields, A. C.; Lewis, J. Should Employers "Google" Applicants? February 2009 [interactive]. [accessed on 15-04-2012]. <http://www.irmi.com/expert/articles/2009/siegel02-employment-practices- liability.aspx>.

Supreme Administrative Court of Republic of Lithuania, case No. A[662]-3548/2011.

Supreme Court of Republic of Lithuania ruling in the civil case No. 3K-3-565/2003, May 5, 2003.

The Connecticut law (Conn. Gen. Stat. § 31-48d (2008), Id. at § 31-48d(b)(2)).

The European convention on human rights [interactive]. [accessed on 12-04-2012]. <http://eur-lex.europa.eu/lt/treaties/dat/32007X1214/htm/C2007303LT.01000101.htm>.

USA case: *Bourke v. Nissan Motor Corp*. No. B068705 (Cal. Ct. App. 26 July, 1993).

Vilnius District Court, civil case No. 2A-2706-656/2011.

Westin, A. *Privacy and Freedom*. New York: Atheneum, 1967.

PRIVATUMAS DARBE: SKIRTINGI POŽIŪRIAI IR PROBLEMOS

Tomas Bagdanskis, Paulius Sartatavičius

Mykolo Romerio universitetas, Lietuva

Santrauka. *Šiame straipsnyje yra aptariami pagrindiniai probleminiai aspektai, susiję su darbuotojų privatumu darbo vietoje bei jo ribų nustatymu, atsižvelgiant į darbdavio interesus. Straipsnyje analizuojami užsienio ir Lietuvos teisės aktai, skirti reglamentuoti privatumą darbovietėje, ypač atkreipiant dėmesį į elektroninę darbo vietą ir jos stebėjimą (el. paštas, ryšių priemonės). Straipsnyje remiamasi teisės aktais ir Lietuvos Aukščiausiojo Teismo, Europos Žmogaus Teisių Teismo ir kitų teisminių institucijų sprendimais, siekiant pateikti reguliavimo įstatymu taikymo praktiką bei kartu atskleisti problemas, kylančias šioje darbo teisės srityje. Atskleidžiami skirtingi požiūriai, susiklostę šioje darbo teisės sferoje. Darbe išryškinama privatumo darbo vietoje reglamentavimo problema bei siūloma labiau orientuotis tiek į nacionalinius, tiek ir į tarptautinius teisės aktus, reguliuojančius asmens duomenų apsaugą, ir tokiu atveju daugiau dėmesio įstatymuose skirti darbuotojų privatumo darbo vietoje aspektui. Elektroninės darbo vietos kontrolė turėtų remtis pagrindiniais asmens duomenų apsaugos principais. Pabrėžtina, jog yra būtina išlaikyti pusiausvyrą tarp darbuotojo teisės į privatumą bei darbdavio interesų. Privatumo darbo vietoje ribos turėtų baigtis ten, kur padaromas nusikaltimas, nusižengimas ar yra pažeidžiamos sutarties ar įstatymo normos. Jeigu darbdavio teisėti verslo interesai yra pažeidžiami ar yra pagrindo manyti, kad*

jie gali būti pažeisti, darbuotojo teisė į privatumą gali būti suvaržoma. Straipsnyje minima, jog pagrindinė problema Lietuvoje yra ta, kad darbuotojai iš esmės turėtų būti aktyvesni savo teisių apsaugos atžvilgiu. Jie turėtų reikalauti darbdavio, kad šis nurodytų, kokios (*jei iš viso naudojamos*) *kontrolės priemonės ir kokiu tikslu gali būti naudojamos darbo vietos stebėjimui. Pabrėžtina, jog darbo vietos kontrolė turi atitikti straipsnyje aptariamus principus ir ypač proporcingumo principą. Darbe išryškinama galimybė darbdaviui kontroliuoti elektroninio darbo vietą blokuojant tam tikrus pasirinktus internetinius tinklalapius, tokius kaip: naujienų portalai, socialiniai tinklai ir t. t. Tokios kontrolės atveju nekyla grėsmė darbuotojo teisės į privatumą pažeidimui. Straipsnyje taip pat išskiriami pagrindiniai akcentai, kuriuos darbdavys turėtų darbuotojui nurodyti iš anksto, norėdamas vykdyti elektroninio pašto kontrolę: darbdavys aiškiai turi nurodyti, ar darbuotojui yra leidžiama naudoti darbinį elektroninį paštą asmeniniais tikslais; kada ir kokiomis sąlygomis darbuotojas gali naudoti asmeninį elektroninį paštą darbo metu; kokiais atvejais yra daromos elektroninių laiškų atsarginės kopijos bei turėtų suteikti informaciją, kai iš serverio yra ištrinami elektroniniai laiškai. Darbe taip pat aptartas ir garso bei vaizdo įrašų darymas bei kada tai yra leistina ir tokių įrašų įrodomoji vertė teisme. Kaip atsvara europinei sistemai ir siekiamam rezultatui straipsnyje analizuotas taip pat ir JAV privatumo darbo vietoje teisinis reglamentavimas bei atkreiptas dėmesys į pagrindinius šių sistemų skirtumus.*

Reikšminiai žodžiai: *darbuotojas, darbdavys, privatumas darbo vietoje, komunikacijos privatumas, privatumo apsauga, pagrindinės teisės ir laisvės.*

Tomas Bagdanskis, Mykolo Romerio universiteto Teisės fakulteto Darbo teisės ir socialinės saugos katedros docentas. Mokslinių tyrimų kryptys: darbo teisė, Europos Sąjungos darbo teisė.

Tomas Bagdanskis, Mykolas Romeris University, Faculty of Law, Department of Labour Law and Social Security, Associate Professor. Reasearch interests: labour law, EU labour law.

Paulius Sartatavičius, advokatų profesinės bendrijos „Bagdanskis iLAW“ teisininkas, lektorius. Mokslinių tyrimų kryptys: informacinių technologijų teisė, intelektinės nuosavybės teisė.

Paulius Sartatavičius, Professional law partnership “Bagdanskis iLAW”, Lawyer, Lecturer. Research interests: IT law, intellectual property law.