Privacy at Workplace: Monitoring of Electronic Communications

by Anastasiia Nekrasova

LL.M. Long Thesis

Supervisor: Petra Bard, S.J.D.

Central European University

1051 Budapest, Nador utca 9

Hungary

Abstract

The thesis analyzes under which conditions an employer could lawfully monitor employee's electronic communications. The analysis is based on comparison of three jurisdictions: the Council of Europe, Canada and USA. It covers legal preconditions for protection of employee's digital privacy, peculiarities of judicial application of reasonable expectation of privacy test in each jurisdiction and tries to deliver employer's standpoint toward workplace electronic surveillance. The thesis shows that the existing balance between employees' and employer's interests is far to be fair. While employees in USA are almost deprived of privacy rights at workplace, in certain cases of Canadian jurisdiction employers' interests are completely neglected in favour of an employee's privacy.

Table of contents

Introduction

Our world becomes more and more digitalized each and every day: bank cards instead of cash, e-mails and messengers instead of calls, online shopping, smartphones, geolocation, activity trackers and much more to come. On the one hand, all these modern devices make our lives easier, on the other – every movement is recorded, we put our privacy in a more vulnerable position. Beyond any doubt, it is better to think about privacy before we find ourselves in a reality, which is close to dystopia that is described in the "Black Mirror" fiction, where electronic gadgets could record all your movements, thoughts and memories.

Even though today working conditions are sometimes described as contemporary slavery, we still do have rights at work. The right to privacy, as well. Will it be fine if an employer requires everyday written report about your sexual life? Probably not, it will break your right to privacy. Nowadays, private e-mails, Facebook messages and history of Internet surfing could be not less intimate. Monitoring of the latter by an employer in most cases would amount to intrusion to the right to privacy of employee. But would it be a violation of the right? Right to privacy is not absolute. It is neither absolute at workplace. This thesis seeks to find the balance between an employer's and an employee's interests and to answer the question of how to find this balance with regard to the monitoring of electronic communications by an employer.

The research and the issue itself is important not only for employees who suffer from intrusion to their privacy, but also has broader societal impact, as far as "protecting privacy in employment is, therefore, not only about safeguarding individual interests in preserving a modicum of solitude and anonymity but, most of all, it is about safeguarding our 'common'

interest in maintain a democratic, pluralistic society and the meaningful dignity planted in its midts".[1]

The object of the research is limited to Internet or Intranet usage, e-mail and other messaging applications. The research does not cover cases of dismissal which were resulted from public social media posts of employees.

The analysis of the issue is based on comparison of three jurisdictions: the Council of Europe, Canada and the United States of America. The choice of these jurisdictions was caused by clear gradation of the level of employees' right to privacy protection from the U.S. jurisdiction, which grants the poorest level of privacy to its employees, to the Council of Europe that embodies high standard of protecting workplace digital privacy. The case of Canada lies somewhere in between these two jurisdictions, as having similar legal inputs as USA does, Canada managed to reach European-like outcomes.

The **first chapter** provides analysis of legal frameworks of three jurisdictions that are applicable to the issue of workplace monitoring (including EU legal framework, however without description of relevant regulations of Member Staes). Employee's digital privacy is regarded from human rights and personal data protection perspectives. The **second chapter** focuses on differences and similarities of the reasonable expectation of privacy test application in different jurisdictions, as well as provide some critical assessment of the test methodology. In order to put case law of international institution in a more or less comparable situation with case law of particular states, this chapter also examines the exercise of the margin of appreciation by Member States of the Council of Europe. The **third chapter** reveals employers' arguments for workplace monitoring with the aim to avoid one-sided approach to the issue, as to certain extent employer is even forced to exercise workplace

[1] Otto M. The Right to Privacy in Employment: A Comparative Analysis. Oxford: Hart Publishing, 2016, p. 242.

monitoring of electronic communications. On the basis of the own subjective perception the author also presents some recommendations for employers on how to optimally balance interests of an employer and employees.

Chapter 1 Legal framework

This chapter makes an overview of the Council of Europe treaties and recommendations, EU, Canada and U.S. legislation that regulates employee monitoring at workplace in a particular jurisdiction. It should be noted that the legal framework to address employee's privacy at workplace is more complex than the one that regulates one's privacy in relations with governmental services, for instance. In particular, what makes it complicated is that the conditions of employee's monitoring is additionally regulated by labor law, different working and/or collective agreements and therefore the conflicts that arise between an employer and employees could also be brought before labour tribunals.

1.1. Council of Europe

The Council of Europe regulates employee's digital privacy from two angles: a human rights perspective and a perspective of processing of personal data. Even though protection of personal data is regarded as a part of the right to privacy, particularly an informational aspect of privacy, these two approaches could not be considered as overlapping, but rather as supplementing each other.

The following paragraph makes an overview not only of the relevant legislative acts of the Council of Europe, but also covers EU legal framework, which is also important to consider in order to have full picture of employee's digital privacy in Europe. The comprehensive understanding of privacy rights in Europe is possibly only within the framework of its horizontal multilayer structure, which consists of three levels: international (the Council of Europe jurisdiction), supranational (the EU jurisdiction) and national jurisdictions of the Member States.[2]

Human rights perspective

On the European terrain the right to privacy was first vested in the Convention for the Protection of Human Rights and Fundamental Freedoms in 1950. Namely, Article 8 of the Convention guarantees to every person the right to private and family life, home and correspondence[3]. Application of this

[2] Otto M. The right to privacy in the employment in search of the European model of protection, *European Labour Law Journal*, vol.6 №4 (2015), - p. 348.
[3] Convention for the Protection of Human Rights and Fundamental Freedoms (1950), Art. 8.

Article to the relations between employer and employees appears through the case law of the European Court of Human Rights.

The notion of private life is quite vague and has no legal exhaustive definition. The European Court of Human Rights even does not make an attempt to provide a definition for 'private life', however in Pretty v. United Kingdom the Court makes an overview of the spheres that are encompassed by the concept of private life, which among others include right to establish and develop relationships with other human beings and the outside world.[4]

It should be noted that partly the Court justifies the usage of such a broad concept for privacy[5] by reference to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which defines personal data as "any information relating to an identified or identifiable individual"[6]. However, it should be clear that despite of several references to personal data protection, Article 8 of the Convention does not absorb completely the concept of personal data protection and certain distinctions could be derived. For example, in Gaskin v. United Kingdom it was stated by the Court that even if refusal to access to Mr. Gaskin personal data falls within the ambit of Article 8 of the Convention, it does not mean that general rights of access to personal data may be derived from the Article 8[7]. By contrast, data protection law recognize right to access to his/her personal data as basic right of personal data subject[8].

Going back to the scope of private life under the Article 8 of the European Convention, it was in the case of Niemietz v. Germany, where the Court has extended it to the professional

[4] Pretty v. United Kingdom *(*Application no. 2346/02), judgment of 29 July 2002, § 61.
[5] See for example Rotaru v. Romania (Application no. 28341/95), judgment of 4 May 2000, § 43
[6] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Jan. 28, 1981), Art.2.
[7] Gaskin v. United Kingdom (Application no. 10454/83), judgment of 7 July 1989, § 37.
[8] See for example Article 8 of the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Article 12 of the 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

(business) sphere by stating that "it would be too restrictive to limit the notion [of private life] to an "inner circle" in which the individual may live his own personal life as he chooses[9]" and there is no reason "to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that […] it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not.[10]"

Apart from establishing the extension of private life to the professional sphere with respect to search in office (as it was in Niemietz case), it was affirmed by the Court that tapping of employees' telephone conversations by state actors also fall within the Article 8 of the European Convention[11].

Nevertheless, the application of the Article 8 of the Convention to the professional sphere of life was considered by the Court mostly with respect to state actions, the Article 8 enshrines both negative and positive obligations of the State. This was explicitly confirmed by Marckx v. Belgium decision: "the object of the Article [8] is "essentially" that of protecting the individual against arbitrary interference by the public authorities […] nevertheless it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective "respect" for family life"[12]. Positive obligation under the Article 8 equally to all spheres of private life that were mentioned in the case of Pretty v. United Kingdom (§ 61) and therefore has horizontal effect on private relations between employer and employee. However, it should be noted that

[9] Niemietz v. Germany (Application no. 13710/88), judgment of 16 December 1992, § 29.
[10] Niemietz v. Germany (Application no. 13710/88), judgment of 16 December 1992, § 29.
[11] Kopp v. Switzerland (13/1997/797/1000), judgment of 25 March 1998, § 50.
[12] Marckx v. Belgium (Application no. 6833/74), judgment of 13 June 1979, § 31.

the choice of means to secure compliance with the Article 8 of the Convention by private individuals lies within the State's margin of appreciation[13].

Personal Data Protection perspective

In contrast to human rights approach, data protection framework specifies concrete rules of processing personal data that are directly applicable to relations between employer and employee. In 1981 the member states of the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[14], which was ratified by 46 out of 47 member states except Turkey[15]. For the purpose of the Convention №108 employee and employer will be regarded as an individual and a controller of the file respectively. Making no specific provisions on employment relationship, the Convention establishes a set of basic principles for data protection, which would be applicable in case of workplace monitoring as well. According to the Article 5 of the Convention № 108 employees' personal data shall be "a) obtained and processed fairly and lawfully; b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are stored; d) accurate and, where necessary, kept up to date; e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."[16] Moreover, the Convention № 108 distinguishes special categories of personal data (so called "sensitive" personal data) that may not be processed automatically unless domestic law provides appropriate safeguards.[17] This category includes "personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life … and data relating to criminal convictions."[18]

[13] M.C. v. Bulgaria (Application no. 39272/98), judgment of 4 December 2003, §150.
[14] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Jan. 28, 1981).
[15] Data as of the 1st January 2016.
[16] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Jan. 28, 1981), Art. 5.
[17] Ibid, Art. 6.
[18] Ibid.

Even though the existence of the 'sensitive' personal data concept in the European legal framework is usually perceived as an advantage of the system in comparison to the U.S. and Canadian legal frameworks. However, it would be fair to note that the definition abovementioned category of personal data is not so unambiguous. At least, the degree of sensitivity of data could depend on different characteristics: not only on the type of data, but also on the content of data, the person of controller of personal data and the context of processing.[19]

However, special attention is paid by the Committee of Ministers of the Council of Europe to the issue of personal data protection at the workplace. Recently the Recommendation on the protection of personal data used for employment purposes (1989)[20] was replaced by more progressive Recommendation on the processing of personal data in the context of employment (2015).[21] As refers to the use of Internet and electronic communications the Recommendation specifies that employees "should be properly and periodically informed in application of a clear privacy policy […]; access by employers to the professional electronic communications of their employees who have been informed in advance of the existence of that possibility can only occur, where necessary, for security or other legitimate reasons. […] in the event of processing of personal data relating to Internet or Intranet pages accessed by the employee, preference should be given to the adoption of preventive measures, such as the use of filters[…]The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances."[22]

[19] Otto M. The Right to Privacy in Employment: A Comparative Analysis. Oxford: Hart Publishing, 2016, p. 130.
[20] Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (Adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies).
[21] Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies)
[22] Ibid, Article 14.

1.1.1. European Union

Even though the Charter of Fundamental Rights of the European Union guarantees right of everyone to the protection of personal data concerning him or her[23] as one of the fundamental rights, there is no need to distinguish data protection approach and fundamental rights approach within EU jurisdiction, as provisions of the Charter are addressed to EU bodies and institutions with due regard for the principle of subsidiarity and to the EU Member States only when they are implementing EU law[24].

The distinction of right to the protection of personal data from right to respect for private and family life, home and correspondence (Article 7 of the Charter) could be explained by specified system of checks and balances, envisaged in the right to data protection, which is not typical for the right to respect for private and family life. [25] Besides, the inclusion of separate right to data protection underlines its importance in modern world.

From 1995 till nowadays the sphere of personal data protection in EU Member States is regulated by the Directive 95/46/EC[26], which is generally applicable to all relationships related to the processing of personal data. Specific regulations apply to the processing of personal data in the electronic communications sector; by the institutions and bodies of the European Union; in the framework of police and judicial cooperation in criminal matters.[27]

[23] EU (2012), Charter of Fundamental Rights of the European Union, OJ 2012 C 326, Article 8.
[24] Ibid, Article 51.
[25] Peers, Steve. n.d. The EU Charter of Fundamental Rights: a commentary. n.p.: Oxford : Hart Publishing, 2014. – p.229.
[26] 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
[27] 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; Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data; Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

While the Council of Europe Convention № 108 determines main principles and guidelines for processing personal data, the Directive 95/46/EC fills these principles with relatively concrete substance. Thus, the EU Directive among other provisions introduces exhaustive list of grounds for lawful processing of personal data[28], provides establishment of independent supervisory authority and safeguards data subject's right to access to his/her personal data and to receive information related to the processing of his/her personal data[29]. It should be noted, as well, that even though the Directive 95/46/EC is binding only for 28 Member States, a number of states has successfully implemented provisions of the Directive to their national legislation including Iceland, Liechtenstein, Norway, Macedonia, Albania, Moldova, Georgia, Ukraine and others.

As for the implementation of EU Personal Data Protection Directive by EU Member States, specifics of EU functioning requires Member States not only to ensure minimal standards of personal data protection provided by the Directive 95/46/EC, but actually precludes Member States from establishing higher level of personal data protection than the Directive 95/46/EC does. In particular, the European Court of Justice has ruled in the joined case of ASNEF and FECEMD v. Administración del Estado that establishing additional requirements to the lawfulness of the processing of personal data under the Article 7 of the Directive 95/46/EC is forbidden, as it would amount to the amendment of the scope of abovementioned article and would make more complicated a free flow of personal data from one Member State to another.[30]

This example illustrates why is it important to consider EU legal framework within the legal framework of protecting personal data in the Council of Europe. While the Council of Europe

[28] Directive 95/46/EC, Articles 7, 8.
[29] Ibid, Articles 10-12, 28.
[30] Joined Cases C-468/10 and C-469/10: Judgment of the Court (Third Chamber) of 24 November 2011, § 27-39.

Convention No. 108 does not preclude member States of the Council of Europe to establish higher (stricter) standards of processing personal data, more than a half of these Member States are restricted to do so by the relevant EU regulation.

In terms of the Directive 95/46/EC employee acts as a personal data subject, while employer is a controller of personal data. Article 6 of the Directive requires from employer to process personal data of employees fairly and lawfully, for specified, explicit and legitimate purposes; the scope of collected data shall be accurate and not excessive in relation to the purpose; personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they were collected. Carrying out the obligations and specific rights of the controller in the field of employment law insofar as it is authorized by national law providing for adequate safeguards is considered as a legitimate ground for employer to process special categories[31] of employees' data[32].

Therefore, EU law does not regulate processing of personal data in terms of employee-employer relationships. Some EU member states have introduced specific legislative provisions that regulate employee's privacy. In particular, such regulations exist in France, Portugal, Austria, Finland and Italy.[33] For example, the Finland's Act on the Protection of Privacy in Working Life contains a list of conditions that an employer needs to meet in order to lawfully intercept employee's electronic messages. In case if other conditions are fulfilled, employer may open the concrete message in the presence of two persons (including

[31] To special categories refer personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
[32] Directive 95/46/EC, Articles 8.
[33] Bagdanskis, T., Sartatavicius, P. Workplace privacy: different views and arising issues. Jurisprudence, № 19(2), 2012 – p. 703.

information system administrator) and the act of opening shall be fixed in the respective report.[34]

Certain guidelines could be found in the Opinion of the Article 29 Working Party on the processing of personal data in the employment context .[35] With regard to monitoring of email use and internet access by employer mentioned Opinion does not provide deep analysis, but states three main points: 1) any monitoring must be a proportionate response to the risks that employer faces; 2) monitoring must be carried out in the least intrusive way possible; 3) employees must be informed of the existence of the monitoring; existence of video surveillance does not reduce data protection requirements applicable to monitoring of Internet and email usage[36].

Next year after Opinion on the processing of personal data in the employment context has been adopted Article 29 Data Protection Working Party adopted the Working document on surveillance and monitoring of electronic communications in the workplace[37] that provides extensive analysis of the issue. In particular, with regard to Internet monitoring three main principles were highlighted: 1) employers should rather use prevention than detection of Internet misuse, when applicable; 2) employers should carefully balance the need to analyze the content and the risk, which employer could potentially face; 3) Internet misuse by employees should be well-grounded.[38]

[34] Act on the Protection of Privacy in Working Life, 759/2004, section 20. (Unofficial translation of the Ministry of Labour, Finland)
[35] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final/WP 48 (September 13, 2001).
[36] Ibid, p. 25.
[37] Article 29 Data Protection Working Party, Working document on surveillance and monitoring of electronic communications in the workplace, 5401/01/EN/ Final/WP55 (29.05.2002)
[38] Ibid, p. 24.

Despite the fact that Member States are not obliged to comply with recommendations produced by Article 29 Working Party, they treat it as a respective source of information and try to follow the Working Party guidelines as much possible.

Prospects of regulation

At the moment EU data protection legislation is in the process of its reformation[39], which is mainly provoked by challenges that right to privacy faces in the era of technological growth. New legislation on personal data is supposed to be effective in 2018.[40] Proposal of the European Commission contains many progressive provisions, including extraterritorial effect of the General Data Protection Regulation (GDPR), processing of personal data of a child, designation of data protection officer, right to data portability and many others, analysis of which could amount to autonomous scientific paper.

As refers to the processing of personal data in the employment context, GDPR recommends (but not obliges) Member States to adopt by law specific rules regulating the processing of employees' personal data in the employment context.[41] It introduces provision called for securing of employees' privacy rights at the local level - designation of data protection officer, who supposed to act independently and directly report to the management of the controller.[42] And what is the most relevant for the research issue of the instant thesis, it amends existing conditions for data subject's consent. According to the Article 7 of GDPR "Consent shall not provide a legal basis for the processing, where there is a significant

[39] In January 2012 the European Commission introduced Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.
[40] Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), 442/16/EN, WP 236, 2 February 2016.
[41] Ibid, Article 82.
[42] Ibid, Section 4.

imbalance between the position of the data subject and the controller."[43] Adoption of the latter provision would prospectively reduce cases of workplace monitoring, as most of employees give their consent to be monitored exactly because of subordinate position.

1.2. Canada

Canadian example is particularly interesting, because it could be considered as a buffer between European and U.S. models of protecting employees' privacy at workplace. Similarly to U.S. jurisdiction, employees' privacy in Canada is not protected at constitutional level, as section 8 of the Canadian Charter of Rights and Freedoms protects privacy only in the context of unreasonable search and seizure.[44] The Supreme Court of Canada applied provisions 7 and 8 of the Canadian Charter to the employment context only in three cases, therefore no specifics trends could be derived. [45] In general, Canadian legal framework could be characterized as a diverse one. As of January 2015 there are 28 federal, provincial and territorial privacy statutes in Canada[46]. The heterogeneity of Canadian legal system is fraught with different inconsistencies, however as refers to employees' digital privacy Canadian case law develops without crucial deviations.

While European legislation examined in the previous chapter make no distinction in regulation depending on private or public form of the controller of personal data, in Canada the level of employee's privacy would depend on the location of the employer (provincial jurisdiction), the nature of organization he/she works for (federal institution, provincial institution or private organization) and in case of private organization - its involvement in

[43] Ibid, Article 7.
[44] Canadian Charter of Rights and Freedoms, s 8, Part I of the Constitution Act, *1982*, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.
[45] Otto M. The Right to Privacy in Employment: A Comparative Analysis. Oxford: Hart Publishing, 2016, p. 172.
[46] DLA Piper's Data Protection Laws of the World Handbook, accessed 01 February 2016, http://www.dlapiperdataprotection.com/#handbook/law-section/c1_CA

commercial activities. Federal privacy legislation of Canada consists of two laws, the Privacy Act[47] and the Personal Information Protection and Electronic Documents Act (PIPEDA)[48], which would be examined in turn.

The Privacy Act is designed to protect privacy rights of individuals (including employees) with respect to personal information, which is held by government institutions and ensure right of individuals to access to such information about them.[49] The act applies only to those institutions, which are listed in the annex to act. According to provisions of the Privacy Act personal information shall be collected only if it relates directly to an operating program or activity of the government institution; individual shall be informed of the purpose for which his/her personal information is being collected; collected personal information shall be accurate and retained for a defined period of time[50]. In fact, all five principles of data quality ensured by the Council of Europe Convention № 108 and the Directive 95/46/EC are reflected in Privacy Act, but in other wording. However, as one the main purposes of the Privacy Act is to ensure access of individual to his/her personal information, information should be retained for a certain period prescribed by regulation "in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information."[51]

In the context of employment, PIPEDA applies to private organizations that process personal information of employees engaged in federal work, undertaking or business (e.g. banks, telecommunications, transportation, nuclear energy etc.).[52] Privacy rights of those who work neither for federal institutions, nor engaged in federal work, undertaking or business, are often protected by provincial privacy laws, but not every such law extends its application to employees.

[47] Privacy Act (R.S.C., 1985, c. P-21)
[48] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)
[49] Privacy Act, Article 2.
[50] Ibid, Articles 5, 6.
[51] Ibid, Article 6.
[52] PIPEDA, Article 4.

Similarly to the U.S. practice, private sector in Canada can be proud of the broad freedom of self-regulation. To a great extant codes of practice that determine the scope of privacy for private employees in Canada were influenced by OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereinafter OECD Guidelines).[53] The OECD Guidelines highlighted six main principles with regard to processing of personal data, which are: 1) collection limitation principle; 2) data quality principle; 3) purpose specification principle; 3) use limitation principle; 4) security safeguards principle; openness principle; 5) individual participation principle; 6) accountability principle[54]. Without going deeper into the meaning of each and every principle, it could be fairly deduced that the above principles of OECD Guidelines clearly reflect principles of processing personal data within the European legal framework. What is more, the Article 29 Data Protection Working Party in his Opinion[55] has confirmed that PIPEDA grants adequate level of personal data protection.

PIPEDA aims not only to protect privacy rights of individuals, but to balance individual rights and organization interests, namely "to establish … rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[56]

In Schedule 1 PIPEDA provides the following principles of the protection of personal information that need to be observed by organizations:

[53] Otto M. The Right to Privacy in Employment: A Comparative Analysis. Oxford: Hart Publishing, 2016, p. 122.
[54] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79
[55] Article 29 Working Party, Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act, 5109/00/EN WP 39.
[56] PIPEDA, Article 3.

- accountability of organization for the compliance with principles;
- identification of purposes at or before the time personal information is collected;
- knowledge and consent of individual are required, except where inappropriate;
- information shall be collected by fair, lawful means and shall be limited to that which is necessary for the identified purposes identified by the organization;
- information shall be retained only as long as necessary for the fulfilment of the purposes;
- accuracy of information; protection by security safeguards appropriate to the sensitivity of the information;
- openness of policies and practices relating to the management of personal information; individual access to personal information;
- ability of an individual to address a challenge concerning compliance of organisation with the above principles.

As refers to the identification of purposes, personal information is not required to be processed with legitimate aim, but for the purposes that "a reasonable person would consider are appropriate in the circumstances"[57], that is quite vague criteria. Despite of security safeguards that shall be in accordance with sensitivity of personal information, neither Privacy Act, nor PIPEDA distinguishes a category of personal information, which is called 'sensitive data' in the European framework.

1.3. United States

[57] Ibid, Article 5.

The level of protection of privacy-rights in the United States is traditionally defined as poor or not adequate.[58] To certain extant this difference in protection of privacy could be explained by otherness of conceptual background. While in European countries the right to privacy is based on the concept of human dignity, in the USA the right to privacy was initially deprived from property rights (home search and seizure) and then extended to the concept of liberty. Obviously human dignity symbolizes something essential and absolutely valuable, whereas according to the famous saying one's liberty ends just where the liberty of other man begins. What is more, some scholars argue that modern concept of privacy circled back to property rights: "the *sui generis* instrumentalization of privacy which is valued only as subservient to personal freedom or liberty, and the resultant omnipresent reliance upon individual will / consent paradoxically pushes it towards property rights".[59]

As for the data protection legal framework, in contrast to European approach there is no comprehensive federal law regulating the use of personal information, but the U.S. use sectoral approach that is based on palette of federal and state laws and regulations. M. Otto explains the absence of comprehensive regulation that would protect employees' privacy by "general absenteeism of American federal law in the area of employment relationships, these being perceived as of a private nature, as well as the specific American prioritization of self-regulation over legislation".[60]

First of all, it should be noted the Constitution of the United States does not contain express right to privacy, but only some aspects of it (privacy of home, possession, beliefs). The absence of the specific provision in the U.S. Constitution for sure has its negative impact on the final outcome of courts' rulings. Employees' claims for privacy could be based on four

[58] Maximillian Schrems v. Data Protection Commissioner, European Court of Justice, Case C-362/13, 6 October 2015
[59] Otto M. The Right to Privacy in Employment: A Comparative Analysis. Oxford : Hart Publishing, 2016, p. 62.
[60] Ibid, p. 26.

different sources: the Fourth Amendment of the U.S. Constitution, the Electronic Communications Privacy Act[61], state law and the privacy tort of "intrusion into seclusion".[62] With regard to Fourth Amendment, it should be noted that it refers only to search and seizure[63] and it does not have horizontal effect, therefore, applies only to individuals employed in public sector.[64]

Examination of the Electronic Communications Privacy Act (ECPA) tends to be the most relevant for the purpose of this thesis. It should be noted that the structure of ECPA is absolutely different from European data protection statutes. Neither principles of data quality, nor grounds for interception are explicitly listed. Going back to data quality principles enshrined in the EU Directive 95/46/EC, at least two of them could be found in ECPA between lines: lawfulness and proportionality.[65] The lawfulness principle could be derived from requirement of authorized access, while proportionality principle is reflected in findings of U.S. Appeal Court that established that under the ECPA, a personal call might be intercepted in the ordinary course of business only to the extent necessary to guard against unauthorized telephone use or to determine whether a call is personal.[66]

Even though ECPA prohibits unauthorized interception of electronic communications[67] and establishes both criminal and civil liabilities for violation of this prohibition[68], employees of private sector find their privacy rights in a vulnerable position. The reason for that are three exceptions to electronic communications interception: prior consent of employee, business use of equipment or facilities, and system provider exception. According to paragraph §

[61] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.
[62] Cuijpers C., ICT and Employer-Employee Power Dynamics: A Comparative Perspective of United States' and Netherlands' Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning of Employees, 25 J. Marshall J. Computer & Info. L. 37 (2007), p. 40-41.
[63] U.S. Constitution, Amendment IV.
[64] Suda Y., Monitoring E-mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States, 4 Wash. U. Global Stud. L. Rev. 209 (2005).- p. 231.
[65] Ibid, p. 235.
[66] Watkins v. L. M. Berry & Co., 704 F.2d 577, 582–83 (11th Cir. 1983).
[67] 18 U.S.C. § 2511 (2000)
[68] 18 U.S.C. 2511(1)(e), (4)(a), 2520.

2511(2)(d) of ECPA it shall not be unlawful for a person not acting under color of law to intercept communications where one of the parties to the communication has given prior consent to such interception.[69] The main difference between employee's consent according to ECPA and according to the EU Directive 95/46/EC, is that consent of U.S. employee gives to employer unconditional right to monitor employee's electronic communications, while the European Personal Data Protection framework requires such monitoring to be lawful, to have legitimate aim, to be not excessive etc. Besides, within the European Data Protection framework a concept could be potentially withdrawn. As considers the second exception, equipment and facilities furnished to employee in the ordinary course of business are simply exempted from the scope of ECPA, as they do not refer to "electronic, mechanical, or other device" in the meaning of ECPA.[70] And finally, as a matter of fact, employers often act as private network providers (owners of company's e-mail system, for example)[71], that allows to monitor employees' electronic communications freely.[72]

It should be noted that in USA there were several attempts to adopt federal law that would somehow protect employees' right to privacy. Protection of workplace privacy according to both Privacy for Consumers and Workers Act[73] (1993) and Notice of Electronic Monitoring Act (2000)[74] had the right to know basis and required employer to provide notification about monitoring, but were never passed. It should be noted that mentioned acts did not limit abilities of employers to monitor electronic communications, but simply require to notify employees about the fact and means of monitoring. So the bills were still far from the level of privacy protection, which is granted in the Council of Europe Member States or Canada

[69] 18 U.S.C. § 2511(2)(d) (2000).
[70] 18 U.S.C. § 2510(5)(a) (2000).
[71] Suda Y., p. 239.
[72] 18 U.S.C. § 2511(2)(a)(i).
[73] The Privacy for Consumers and Workers Act, H.R. 1900, S. 984, 103rd Congress (1993).
[74] The Notice of Electronic Monitoring Act, H.R. 4908, 106th Congress (2000).

1.4. Concluding notes

Among three jurisdictions, the highest level of protection of employee's right to privacy against digital workplace monitoring is guaranteed in European states. In both the Council of Europe and EU legal frameworks, employees' digital privacy could be protected from two angles: human (fundamental) rights perspective and data protection perspective. While protection in terms of right to respect for private and family life could be sometimes vague and subjective, personal data protection framework establishes the system of checks and balances, which is based on five main data quality principles and exhaustive list of grounds for processing of personal data. Exactly this system of checks and balances led to inclusion of right to data protection as a separate fundamental right in the EU Charter of Fundamental Rights.

Employees subjected to monitoring in U.S. and Canada could not claim that their fundamental rights were violated as both states consider fundamental right to privacy only with regard to unlawful search and seizure. Therefore, U.S. and Canada protect employees' right within the data protection frameworks. While using different vocabulary Canadian data protection framework in general goes in conformity with European one, as all five principles of data quality ensured by the Council of Europe Convention № 108 and the Directive 95/46/EC are reflected in the Canadian law. However, it should be pointed out that Canadian regulations differs depending on private or public form of the employer and it does not establish higher level of protection for the processing of 'sensitive' personal data (nor USA does).

USA provides the poorest level of protection to its employees. While there is no comprehensive data protection law and U.S. uses sectoral approach to data protection, monitoring of employees' e-mails and Internet usage fall under regulation of the Electronic Communications Privacy Act (ECPA). However, application of this law in the employment

context is almost useless due to three exceptions that allows interception of employees' electronic communications if 1) employee gave his prior consent for such interception; 2) employer provides equipment or facilities for electronic communications; 3) employer acts as a private network provider. It should be stressed that scholars express their concerns with regard to consent of employee as a legal ground for monitoring even within the European context, where such monitoring needs to fulfill other requirements of data protection legislation. What can be said about employee consent for monitoring in the U.S., which makes employee almost deprived of his/her privacy rights?!

Chapter 2 Reasonable expectation of privacy test

The reasonable expectation of privacy test, as well as the concept of privacy itself, emerged in the United States. For the very first time reasonable expectation of privacy test was used in Katz v. United States decision in 1967.[75] The appearance of this concept was due to the issue of whether there could be a private conversation in public phone booth. Justice Stewart delivered the opinion of the Court by stating:

"No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." [76]

And as it was summarized by Justice Harlan: "an enclosed telephone booth is an area where, like a home and unlike a field, a person has a constitutionally protected reasonable expectation of privacy".[77]

The reasonable expectation of privacy test was applied by the Supreme Court of Canada in 1984[78] and by the European Court of Human Rights in 1992.[79] The peculiarities of applying the reasonable expectation of privacy test in each three jurisdictions, as well as in some Member States of the Council of Europe, will be discussed in the following chapter.

2.1. European Court of Human Rights

[75] Katz v. United States, 389 U.S. 347 (1967)
[76] Ibid
[77] Ibid
[78] Hunter v Southam Inc [1984] 2 S.C.R. 145
[79] Lüdi v. Switzerland (application no. 12433/86), judgment of 15 June 1992.

In the ECtHR jurisprudence the concept of reasonable expectation of privacy was first used in Lüdi v. Switzerland, where the Court stated that being engaged in a criminal act, Mr. Lüdi must therefore have been aware of the risk of encountering an undercover police officer whose task would in fact be to expose him[80]. The test consists of two elements: 1) the person must act as though he/she expect privacy; 2) society recognizes this expectation as reasonable.[81]

In Copland v. United Kingdom[82] the Court considered employees' privacy as a negative obligation of the state. Based on findings of Halford v. the United Kingdom, where the Court established that telephone calls made from business premises may fall under the notions of "private life" and "correspondence" within the meaning of the Article 8 of the Convention[83], in Copland the Court similarly applied it to e-mail and Internet usage at the workplace.[84]

The applicant received no warning about the monitoring and the College had no policy regarding monitoring of telephone, e-mail or Internet usage by employees. The United Kingdom failed to comply with three-part already at the first stage, as at that time there were no domestic law regulating such monitoring. The Court rejected Government's argument that "the College was authorised under its statutory powers to do "anything necessary or expedient" for the purposes of providing higher and further education"[85], as it does not fulfil the requirement of foreseeability. It was irrelevant for the case that the data were not disclosed to anybody or used against the employee in disciplinary proceedings[86].

[80] Ibid, § 40.
[81] Rikke Frank Jørgensen. Human Rights in the Global Information Society. MIT Press, 2006. – p. 142.
[82] Copland v. the United Kingdom (application no. 62617/00), judgment of 3 April 2007.
[83] Halford v. the United Kingdom (application no. 20605/92), judgment of 25 June 1997, § 44.
[84] Copland, § 41.
[85] Copland, § 47.
[86] Aidan O'Neill. EU Law for UK Lawyers. Oxford: Hart Publishing, 2011. – p. 448.

In deciding whether there was any interference with the rights guaranteed under the Article 8 of the European Convention the Court took into account the fact that these data may have been legitimately obtained in the form of telephone bills and assess whether the applicant had a reasonable expectation as to the privacy of calls made from her work telephone, e-mail and Internet usage.[87]

It could be derived that in a case of prior notification of an employee or in other situation, where the employee could not have a reasonable expectation of privacy, interception of communications does not constitute a violation of the right to respect for private life and correspondence. However, it was clarified by the Court that a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive factor.[88] For example, in a decision as to the admissibility of application by Mr. Kopke, where an employer ordered the covert video surveillance of the applicant's place of work without her knowledge and consent, the Court ruled that interference with right to respect for private life was in compliance with Article 8 of the Convention (even though the applicant could have a reasonable expectation of privacy)[89]. The Court accepted the position of the German domestic court, which stressed: "employer was only authorised to set up the video surveillance of an employee at his or her workplace if there was a prior substantiated suspicion that the employee had committed an offence and if such surveillance was altogether proportionate to the aim of investigating the offence at issue."[90]

In the most recent case of Barbulescu v. Romania [91] the Court examined employee's monitoring from the standpoint of State's positive obligation under the Article 8 of the Convention. The applicant was employed by private company and the latter asked Barbulescu

[87] Ibid Copland § 42, 43
[88] P.G. and J.H. v. the United Kingdom (application no. 44787/98), judgment of 25 September 2001, § 57.
[89] Kopke v. Germany (application no. 420/07), decision as to the admissibility of 5 October 2010.
[90] Ibid Kopke
[91] Barbulescu v. Romania (application no. 61496/08), judgment of 12 January 2016.

to create an account in Yahoo Messenger for professional purposes and then monitored it without specific warning. The Court noted that despite broad notion of private life, Article 8 does not protect every activity a person might seek to engage in with other human beings. In particular, «it will not, for example, protect interpersonal relations of such broad and indeterminate scope that there can be no conceivable direct link between the action or inaction of a State and a person's private life»[92].

The Court concluded that there was no violation of the Article 8 in the case of Barbulescu v. Romania as the employer had accessed the applicant's messenger with good faith in the belief that it was used only for professional messages. The Court finds that it is reasonably justified for employer «that the employees are completing their professional tasks during working hours.»[93] What is more, employer's monitoring was limited in scope (only Yahoo Messenger) and proportional.[94]

Findings of the Court in Barbulescu v. Romania are quite disputable. Even though the Labour Code of Romania provided that the employer had the right to monitor the manner in which the employees completed their professional tasks[95], the foreseeability of monitoring is not guaranteed. Employer's requirement to create Yahoo Messenger account for professional use does not mean that account will be monitored and there is no space for private communications.

In support of this thesis it could be mentioned that Judge Pinto de Albuquerque in his partly dissenting opinion to Barbulescu v. Romania argues that Internet communications are not less protected on the sole ground that they occur in the context of employment relationship:

[92] Barbulescu, § 35.
[93] Barbulescu, § 59.
[94] Barbulescu, § 60.
[95] Barbulescu, § 15.

"The pursuit of maximum profitability and productivity from the workforce is not *per se* an interest covered by the Article 8, but the purpose of ensuring the fair fulfilment of contractual obligations may justify certain restrictions."[96]

Judge Pinto de Albuquerque emphasized the existence of an Internet usage policy in the workplace by saying that "All employees should be notified personally of the said policy and consent to it explicitly".[97] The Irish Data Protection Commissioner develops this argument in a way that "In the absence of a clear policy, employees may be assumed to have a reasonable expectation of privacy in the workplace."[98]

Good faith of the employer is under question as well. According to facts of the case Yahoo Messenger communications had been monitored from 5 to 13 July 2007.[99] It is quite disturbing that even though very sensitive issues (like health and sexual life) were discussed in messenger, the employer did not inform the applicant about the monitoring as soon as first private messages occurred, but on the contrary disclosed the content of communications to colleagues of Mr. Barbulescu.[100]

Considering the precondition of prior knowledge and/or consent of an employee to a certain form of monitoring by employer or video surveillance at his/her workplace, the nature of employment relations should be taken into account. With respect to the subordinate position of an employee, his/her ability to give free consent remains questionable. Even if an employer would not be able to dismiss an employee because of non-signed consent for monitoring of electronic communications, an average employee usually does not want to be in a conflict with his/her employer, as it could distant him from promotion, rise in wages or other benefits.

[96] Barbulescu, § 5 of the Partly Dissenting Opinion of Judge Pinto de Albuquerque.
[97] Barbulescu, § 12 of the Partly Dissenting Opinion of Judge Pinto de Albuquerque.
[98] Guidance Notes on Monitoring of Staff, accessed at https://www.dataprotection.ie/docs/Guidance-Notes-Monitoring-of-Staff/m/208.htm
[99] Barbulescu, § 7
[100] Barbulescu, § 7, 30.

Without going deeper into the privacy of third parties, it would be good to mention that the case of Barbulescu raised another complicated issue, which was not considered by the Court. According to the facts of the case, the applicant was communicating with his brother and fiancée. For reasonable grounds the transcript of the conversations between them is not available, but it could be rationally assumed that the employer has also intruded into privacy of the mentioned persons, with whom he had no labor relations.

2.1.1. Exercising states' margin of appreciation.

The doctrine of margin of appreciation is applicable for employees' privacy cases, as this type of cases often include interest-balancing component. As it was explained by the Court "by reason of their direct and continuous contact with the vital forces of their countries, State authorities are in principle in a better position than the international judge to give an opinion on the exact content of these requirements [legality and finality], as well as on the "necessity" of a "restriction" or "penalty" intended to meet them [pressing social need].[101] The way of how States exercise their discretion in balancing employee and employer interests and assess employee's expectation of privacy will be examined in the following subparagraph. However, it should be mentioned that the specifics of this category does not encourage the existence of massive case law base. National courts often do not explicitly address the issue of lawfulness of Internet and e-mail monitoring, but rather the issues of dismissal and disciplinary actions applied as a result of such monitoring.

France, being among the first states that enacted data protection laws[102], serves as an examples of state that guarantee high level of protection for employees. Due to general

[101] Handyside v. the United Kingdom *(*application no. 5493/72*)*, judgement of 7 December 1976, § 48.
[102] Gutwirth S, Leenes R, de Hert P. Reforming European Data Protection Law [e-book]. Dordrecht : Springer Netherlands : Imprint: Springer, 2015. – p. 313.

principle of confidentiality of correspondence in France[103], employees have rather strong and justified expectation of privacy at workplace.

Referring to comments to Barbulescu v. Romania in the previous chapter, in particular that employer's requirement to use electronic communications for professional purposes only does not automatically mean that this account will be subjected to monitoring (see p. 20), it should be noted that French courts agree with this thesis. In the case Nikon France v. Onof the Court established that the employer can not violate the right to privacy of the employee by reading his/her personal messages received through workplace devices, even if the employer has prohibited the personal use of these devices.[104]

Despite the high level of protection, employee's privacy rights in France are not absolute. Employer's supervisory authority, while is required to comply with legitimate aim and proportionality principle, is limited to the monitoring of recipients or senders of emails; access to personal information contained on employee's computer (including content of e-mails) is legitimate after obtaining a judicial order upon request.[105] Content of employee's emails sent through his/her company email could be monitored in case if the employer complies with transparency principle and have introduced relevant policy prior to the monitoring itself.[106]

Obviously, not all Member States share position expressed by French court in Nikon France v. Onof. For example, The Spanish Constitutional Court found no violation of right to privacy in the case, when the employer read employees' conversation in the messaging program

[103] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.
[104] Décision de Cour de Cassation, Chambre sociale, du 2 octobre 2001, 99-42.942.
[105] Kambellari, E. Employee email monitoring and workplace privacy in the European perspective. - Iustinianus Primus Law Review № 08 - volume 5:1 (2014). – pp. 11-12.
[106] Ibid, p.11.

installed by them.[107] The Court stated that employees had no reasonable expectation of privacy due to the facts that 1) the computer was for common use without password; 2) installation of software without authorization, as well as their use for non-professional purposes were explicitly forbidden. [108]

Not employee-friendly approach in assessing employees' reasonable expectation of privacy could be found in Italian jurisprudence. The Italian Court of Cassation in one of its decisions[109] ruled that the monitoring of employee's email was lawful, as internal policy of the company prescribes for employees to disclose computer and email passwords to employer.[110] The mere fact of existence of such policy again raises the issue of unequal positions of employee and employer. Moreover, the Turin District Court[111] ruled that in cases when the company has introduced relevant internal policy, emails sent through work email should be considered as email sent by the company. [112] Thus, the Turin District Court provided an employer with blanket right to monitor employees' emails.

Similar approach is used in the EU law. For example, in Tzoanos v. Commission[113] the European Court of First Instance ruled that the European Commission could monitor the computer used by the applicant, as the computer is in the ownership of the Commission and shall be used to serve the interests of the European Commission.[114]

Therefore, it could be concluded that within the jurisdiction of the Council of Europe employer's ability to monitor employee's digital communications depends on three main factors 1) existence of internal Internet (e-mail) usage policy; 2) notification of employee

[107] The Spanish Constitutional Court, judgement 241/2012 of 17 December 2012.

[108] Blanpain, R.'Protection of employees' personal information and privacy'. Bulletin for Comparative Labour relations № 88, 2014. – p. 179.
[109] Decision of the Italian Court of Cassation no. 47096, dated 11. 12. 2007
[110] Kambellari, p. 14.
[111] Decision of the District Court of Turin, no. 143, dated, 20.08.2006.
[112] Kambellari, p. 14.
[113] Case T-74/96, Tzoanos v. Commission, 44 E.C.R. IA-00129, II-00343 (1998).
[114] Ibid, § 321.

about such policy or consent to be monitored; 3) permission to use email or other electronic communications provided by employer for private purposes. As for the one of them, if employer's regulations forbid to use electronic communications for private purposes – it is itself an issue how reasonable and proportional it is. According Article 29 Working Party "a blanket ban on personal use of the Internet by employees does not appear to be reasonable and fails to reflect the degree to which the Internet can assist employees in their daily lives."[115]

Even though Israel jurisdiction does not fall within the scope of this research, it will be beneficial to mention that the Israeli National Labor Court [116] distinguishes privacy expectation with reference to four types of email accounts: 1) used strictly for business purposes; 2) merely personal accounts; 3) "mixed" accounts; 4) personal accounts provided by employer.[117]

As for the "mixed" email accounts, simple and wise solution was introduced by the Community Gateway Association (UK), the email use policy of which prescribes to mark all personal e-mail as "personal" or "private" in the subject line.[118] Therefore, basing on the facts that 1) an employee did not mark his private e-mail as "private"; 2) the employee was aware of this rule as he was the author of the email use policy; in Atkinson v Community Gateway Association the Employment Appeal Tribunal concluded there could be no expectation of privacy in this case.[119]

[115] Article 29 Data Protection Working Party, Working document on surveillance and monitoring of electronic communications in the workplace, 5401/01/EN/ Final/WP55 (29.05.2002), p.4.
[116] Labor Appeal no. 90/08 Tali Isakov Inbar v. Commissioner for Women Labor, dated *08.02.2011*.
[117] Mirchin, D. (2012). Monitoring Employee Online Activity: Landmark Case Establishes Guidelines. Information Today, 29(2). – p.32.
[118] Appeal No. UKEAT/0457/12/BA Atkinson v Community Gateway Association, judgment of the Employment Appeal Tribunal, dated 21.08.2014, § 58.
[119] Ibid, § 61.

However, even if e-mail or files were marked as "private/personal", there is no guarantee of unambiguous interpretation. Currently, the case of Libert v. France[120] is pending before European Court of Human Rights. The applicant stored pornographic content in a file called "laugh" which was put on a hard disk called "D:/personal data", whereas the employer pointed out that the entire hard disk on professional computer cannot be used for private purposes only; besides the disk "D" is called "D:/data" by default.[121] The way Mr. Libert name the file at stake ("laugh") was also not enough eloquent to express it's private nature. Consequently, when internal policy requires employee to mark private e-mail and files as "personal", it should be done as clear as possible.

2.2. Canada

Even though in Hunter v Southam Inc[122] the Canadian Supreme Court explicitly referred to U.S. jurisprudence[123]with regard to the reasonable expectation of privacy notion, it developed the reasonable expectation of privacy test in its own manner. According to the Canadian Supreme Court, assessment of "reasonable expectation of privacy" depends on "the totality of the circumstances" of a particular case.[124]

In terms of the "totality of the circumstances", the Court examines the following issues:

"a. What was the subject matter of the alleged search (seizure)?

b. Did the claimant had a direct interest in the subject matter?

c. Did the claimant have a *subjective* expectation of privacy in the subject matter?

d. If so, was that subjective expectation *objectively* reasonable? In this respect, regard must be to:

- the place where the alleged "search" ("seizure") occurred;

[120] Libert v. France (application № 588/13) (pending), communicated on 30 March 2015.
[121] Ibid.
[122] Hunter v Southam Inc [1984] 2 S.C.R. 145
[123] Katz v. United States, 389 U.S. 347 (1967)
[124] R. v. Edwards, [1996] 1 S.C.R. 128, R. v. Debot, [1989] 2 S.C.R. 1140. R. v. Plant, [1993] 3 S.C.R. 281

- whether the subject matter was in public view;
- whether the subject matter had been abandoned;
- whether the information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?
- whether the police technique was intrusive in relation to the privacy interest;
- whether the use of technology was itself objectively unreasonable;
- whether the use of technology exposed any intimate details of the respondent's lifestyle, or information of a biographical nature."[125]

If the defendant had a reasonable expectation of privacy, the court than examines whether it was violated by conduct of public authorities (warrantless searches are presumptively unreasonable). The holistic approach of "totality of circumstances" allows to minimize subjectivity of judges and to consider each case individually avoiding strong dependency on previous case law.

In 2012 the Supreme Court of Canada issued a landmark decision[126] in the sphere of workplace privacy. While performing maintenance activities, a technician found nude photographs of an underage female student on the laptop of the high-school teacher. The latter was charged with possession of child pornography and unauthorized use of a computer. The Court found a violation of the right to be secure against unreasonable search or seizure protected by the Article 8 of the Canadian Charter of Rights and Freedoms. The "totality of the circumstances" test was based on four abovementioned lines of the inquiry.[127] As for objective reasonabless of his subjective expectation of privacy, the complexity of the situation is that school written policy permitted Mr. Cole to use his work-issued laptop for personal purposes, but deprived him of exclusive control over it.[128] The Court actually balanced these two arguments and ruled that ownership of property and workplace policies are relevant considerations, but are not determinative. They may diminish an individual's expectation of privacy in a work computer, they do not remove it completely. A reasonable though

[125] R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67, § 32.
[126] R. v. Cole, 2012 SCC 53, [2012] 3 S.C.R. 34
[127] Ibid, § 40.
[128] Ibid, § 54.

diminished expectation of privacy is nonetheless a reasonable expectation of privacy, protected by Article 8 of the Canadian Charter.[129]

Even though Canadian Charter does not apply to relationships between private parties directly, the common law must nonetheless be developed in accordance with the Charter values.[130] Thus, the standard of the reasonable expectation of privacy would apply as well. In Re Doman Forest Ltd labor arbitrator related standard of reasonableness to the realm of a private dispute between an employer and an employee whose relationship is governed by the terms of a collective agreement.[131] The issue at stake was whether the evidence obtained by surveillance of private investigator could be admissible in case when there is a concern about sickleave abuse. The arbitrator balanced employee's right to privacy against the employer's right to investigate what it might consider to be an abuse of sick leave by answering three questions:

"(1) Was it reasonable, in all of the circumstances, to request a surveillance?

(2) Was the surveillance conducted in a reasonable manner?

(3) Were other alternatives open to the company to obtain the evidence it sought?"[132]

In such cases the focus shifts from reasonableness of employee's expectations to reasonableness to employer's actions. Nonetheless, the latter is considered "in all of the circumstances" of the case, that to certain extant reflects the totality of circumstances test.

Paradoxically so it may sound, while solving disputes between private parties labor arbitrators could treat employee's privacy interest even more favorably than public courts, who apply Canadian Charter directly. Thus in SGEU v Unifor it was established that an employee could have reasonable expectation of privacy even when it was clearly stated in the workplace policy that *"*employees should not expect that their communications or use of the SGEU office network system is either confidential or private".[133]

[129] Ibid, § 51 - 57.
[130] Hill v. Church of Scientology of Toronto, [1995] 2 S.C.R. 1130, § 206.
[131] Re Doman Forest Ltd., [1990] 3 L.A.C. (B.C.) (4th) 275 at 280, § 19, 20.
[132] Ibid, § 32.
[133] *S*GEU v Unifor, Local 481 (2015), 255 LAC (4th) 353 (Ponak)

SGEU had to establish employee's affiliation with motorcycle gang, as the latter contradicts to SGEU's Code of conduct. With this purpose employee's emails on the SGEU server were investigated.

Arbitrator Ponak ruled that even IT policy reduces privacy expectation of employees to the minimum level, reasonable expectation of privacy can not be completely eliminated because of the ubiquitousness of email and close interconnection between work time and non-work time.

"Personal emails and calls will invariably come to business email addresses and business phones. Even if senders are aware of the personal email address, some email programs automatically route a personal email to the business email address unless the sender carefully checks the address."[134]

In my view, such a broad interpretation completely neglect employer's privacy policy and fails to strike a fair balance between employer's and employee's interests. Following such argumentation would always end up by establishing the existence of employee's reasonable expectation of privacy.

It should be remembered, that establishment of the fact that an employee had a reasonable expectation of privacy does not automatically indicate a violation of his employee's right to privacy. According to the Doman test the search must be reasonable in the circumstances, carried out in a reasonable manner and there should be no alternatives to access the evidence. Even though SGEU had legitimate justification for the search, there were less intrusive alternatives to receive information about employee's affiliation with motorcycle gang.[135]

2.3. United States

[134] Ibid
[135] Ibid

As it was already mentioned the reasonable expectation of privacy test was introduced Katz v. United States. Justice Harlan identified a twofold requirement of the reasonable expectation of privacy test: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[136]

Apart from reasonable expectation of privacy, in the case of Katz v. United States the court introduced simple, but peremptory doctrine called "the third party doctrine", according to which after personal information was once disclosed to any third party, it is no longer protected by the Fourth Amendment.[137] The Court formulated it as "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection".[138]

As one of the approaches to assess whether one's expectation of privacy is indeed reasonable courts use risk analysis. The Western District Court of Virginia defines objective reasonableness prong of the privacy test as a determination of how much privacy we should have as a society.

"To have any interest in privacy, there must be some exclusion of others. To have a reasonable expectation of privacy under the Supreme Court's risk-analysis approach to the Fourth Amendment, two conditions must be met: (1) the data must not be knowingly exposed to others, and (2) the Internet service provider's ability to access the data must not constitute a disclosure.»[139]

[136] Katz v. United States, 389 U.S. 347 (1967)
[137] Stanley J. (May 2010) The crisis in Fourth Amendment Jurisprudence. *American Constitution Society for Law and Policy,1-20, p.2.*
[138] Katz v. United States, 389 U.S. 347 (1967)
[139] United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999).

In Hambrick case Internet service provider in response to subpoena of police officer released personal information of IP address subscriber (name, address, credit card number). On the basis of risk assessment the court declared that Mr Hamrick knowlingly revealed his personal information to Internet service provider. Employees of the latter had ready access to these records in the normal course of the business. As there was no agreement between the defendant and Internet service provider that would prohibit to reveal the defendant's personal information, there can be no reasonable expectation of privacy in that information.[140] Following the same logic, one could not reasonably expect privacy in conversation as there is a risk that interlocutor is equipped with electronic eavesdropping devices.[141] As well as the use of beeper surveillance without warrant does not violate one's right to privacy, as a person traveling in an automobile on public thoroughfares is always under risk to be followed and could not expect privacy in his/her movements. [142]

From the perspective of protection of right to privacy, this approach does not stand any critics. I would say after exposing some personal information to a bank or Internet provider one could not only expect, but demand privacy. Freedom of speech, which is so highly appreciated in the United States would suffer greatly if a person is afraid to speak because of the permanent risk of being recorded.

However, U.S. justice has already made some steps towards reconsidering the third party doctrine. In particular, Justice Sotomayor in his concurring opinion to the decision in United States v. Jones stated that "this approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. … I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth

[140] Ibid at 508, 509.
[141] United States v White, 401 U.S. 745 (1971)
[142] United States v. Knotts, 460 U.S. 276 (1983)

Amendment protection."[143] Nonetheless, the concrete way of how the doctrine should be modified was not introduced as this issue falls outside the scope of the case.

In contrast to the European and Canadian approaches, warrantless searches in the United States that were conducted in circumstances where a person could reasonably expect privacy, does not necessary signify a violation of the 4th Amendment as it was in Katz case. In O'Connor v. Ortega[144] administration of state hospital conducted a search in the office of one of its employees in terms of investigation of alleged misconduct while the employee was on administrative leave. It was ruled by the U.S. Supreme Court that "The employee's expectation of privacy must be assessed in the context of the employment relation. An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees"[145] As Dr. Ortega did not share his desk or file cabinets with any other employees, at least he could reasonably expect privacy in his desk and file cabinets.[146] After it was established that the employee could have reasonably expect privacy, the Court applied the standard of reasonableness to warrantless search by the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.[147] Court's justification for reasonableness of warrantless search was quite trivial: warrant procedures would seriously disrupt the routine conduct of business in the hospital. In short, the Court declared it reasonable to conduct warrantless search in order to investigate work-related misconduct by government employee.

In City of Ontario v. Quon[148] the Court applied O'Connors approach of accepting the search used for non-investigatory work-related purpose to monitoring of electronic communications,

[143] United States v. Jones, 132 S. Ct. 945 (2012)
[144] O'Connor v. Ortega, 480 U.S. 709 (1987)
[145] Ibid
[146] Ibid
[147] Ibid
[148] Ontario v. Quon, 560 U.S. 746 (2010)

in particular pager text messages. The "Computer Usage, Internet and E-Mail Policy" of the City made it quite clear that the City has right to monitor all network activities including e-mail and Internet use. Text messages were not explicitly mentioned in a policy, but employees were told that pager text messages (pagers were provided by employer) are also subjected to this policy. Interestingly that the fact of ubiquitousness of emails and text messages in City of Ontario v. Quon was used in completely different manner than in Canadian case of *S*GEU v Unifor. The U.S. Supreme Court ruled that "ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own."[149]

As it was already mentioned, the 4th Amendment of the U.S. Constitution does not apply to relations between private parties and three ECPA exceptions to electronic communications interception make private-sector employees almost deprived of privacy rights. But even when confidentiality of e-mails is assured by employer, the court could find no reasonable expectation of privacy. For example, in Smyth v. Pillsbury Company the court found no reasonable expectation of privacy in e-mail communications notwithstanding any assurances that such communications would not be intercepted by stating:

"Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."[150]

Besides, in addition to employee's reasonable expectation of privacy common law tort of intrusion requires the intrusion to be highly offensive. Offensive nature of the invasion

[149] Ibid

[150] Michael A. Smyth v. The Pillsbury Company, 914 F. Supp. 97 (E.D. Pa. 1996)

requires intrusion to be unreasonable, unjustified, or unwarranted.[151] In Smyth case the court concluded:

"even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. … Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[152]

2.4. Critical assessment

A number of scholars subjected the concept of reasonable expectation of privacy to critics. Within the European context the main critics is that it might "eventually lead to lesser privacy protection, since some forms of privacy intrusions might fall outside of the protective reach of Article 8 , paragraph 3 ECHR."[153] Thus, it may be treated in a way that prescription by law and legitimate aim is no longer required if a person does not have a reasonable expectation of privacy.

Gomez-Arostegui and H. Tomas raised two reasonable issues with regard to pitfalls of the reasonable expectation of privacy test. The first one concerns Court's silence as to the subjective or objective character of one's expectation of privacy. The second one regards the applicability of the test only to private life or to home, correspondence and family life as well[154]. Using of such wordings as "reasonable expectation of privacy for calls" in Halford

[151] Bill McLaren, Jr. v. Microsoft Corp. Case No. 05-97-00824, 1999 (Tex. App.), § 3
[152] Michael A. Smyth v. The Pillsbury Company at 101.
[153] Sjaak Nouwt, Berend R. de Vries, Corien Prins. Reasonable Expectations of Privacy?: Eleven Country Reports on Camera Surveillance and Workplace Privacy. The Hague: T.M.C. Asser Press. – p. 334
[154] Gomez-Arostegui, H. Tomas. Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations. - California Western International Law Journal, Vol. 35, Issue 2 (Spring 2005), p. 167.

case[155] is more likely to be interpreted in the way that reasonable expectation test equally applies to the correspondence component of the Article 8. However, correlation between the test and both home and family life still remains unclear.

As for the U.S. context, it is not merely the application of the reasonable expectation of privacy test, but the American concept itself is highly criticized. Famous American sociologist Amitai Etzioni criticizes the reasonable expectation of privacy test for being tautological. He argues that expectation of privacy exists only when individual's idea of what reasonable expectation is, corresponds to the view of judge.[156] Professor advocates for his own conception of balancing individual privacy rights and common goods to be used by U.S. legal system that would replace the reasonable expectation of privacy test.[157] For this purpose he suggests to use an analysis, based on the four following questions. The first is "Is there a compelling need for corrective action? Or are we about to recalibrate privacy unnecessary?" [158] As soon as we discover that either privacy or common good is in underprivileged position it should be decided "Can privacy be enhanced without recalibrating the common good?"[159] The third question asks whether intrusive interventions are minimally needed.[160] Lastly it needs to be defined "whether the suggested changes in law and public policy should include treatments from undesirable side effects of the needed interventions"[161]

The described analysis represents one of the modifications of the proportionality test, which is widely used to determine whether limitation of a certain right was justified. A traditional proportionality test consists of three main elements:

[155] Halford v. United Kingdom, § 45.
[156] Etzioni A., Rice C.J. Privacy in a Cyber Age: Policy and Practice. Palgrave Macmillan, 2015. – p. 23.
[157] Etzioni A. The Limits of Privacy, Basic Books, 1999. – p. 183-184.
[158] Ibid, p. 184.
[159] Ibid, p. 185
[160] Ibid, p. 185
[161] Ibid, p. 186.

"i) suitability: the means adopted to advance a particular aim must be appropriate (reasonably and demonstrably designed) for achieving that goal; ii) necessity: the means must be those that infringe least at the right of individual; and iii) proportionality *strictu sensu:* the loss resulting from the infringement on the right must be proportional to the gain in terms of furthering the particular goal."[162]

If we apply the Etzioni's test, for example, to the case of the City of Ontario v. Quon, the result would be completely different. As it was already mentioned in the previous paragraph, the employer intercepted the content of pager text messages for non-investigatory work-related purpose. The ground for interception is that "Quon exceeded his monthly text message character allotment."[163] It should be noted that excessive communications of Mr. Quon did not cause any additional costs for the City of Ontario as he reimbursed the overage fee.[164] I would suggest that under the Etzioni's test the City of Ontario would fail already on the first step of it, as in these circumstances there was no compelling need for intrusion into the employee's privacy.

As the analysis shows, the application of the reasonable expectation of privacy test in USA imply distorted understanding of what is reasonable and fails to find a fair balance between employer's and employee's interests. As a way to protect employees of the United States from arbitrary monitoring and surveillance at the workplace some scholars propose to perceive the issue from the standpoint of human dignity. L.E. Rothstein asserts that "The worker's dignity is denied when she is treated as a mechanism transparent to the view of others at a distance and therefore manipulable or disposable without the ability to confront the

[162] Otto M. The Right to Privacy in Employment: A Comparative Analysis. Oxford: Hart Publishing, 2016, p. 234.
[163] Ontario v. Quon, 560 U.S. 746 (2010)
[164] Ibid.

observer."[165] He argues that human dignity argument would lead to more positive results for those who advocate for privacy rights of employees.

The raised arguments pretend to be quite fair and weighty. Summing up, reasonable expectation of privacy test contain a lot of errors and is far to be just in balancing an employer's and employees' interests. I would suggest that proportionality test will be more successful in protecting employee's privacy.

2.5. Concluding notes

Even though the reasonable expectation of privacy test emerged in the United States, from the human rights standpoint it applies more progressively in Canada and European countries. It consists of two basic elements, which are common for all three jurisdictions: subjective expectation of privacy and recognition of that expectation by society as reasonable. The main purpose of the test is to define whether alleged infringement falls within the scope of right to privacy. It is common for all three jurisdictions that existence of reasonable expectation of privacy does not automatically mean that the right of the person was violated.

In the majority of U.S. cases application of the test is predestined by the ECPA which does not prohibit interception of electronic communications by employer in cases of prior consent of employee, business use of equipment or facilities and when employer acts as private network provider. In cases where the answer for reasonable expectation of privacy test is not obviously negative, courts define reasonableness of privacy expectation with the help of risk analysis. Namely the court defines whether a person, for example could predict the risk of the information disclosure or the risk of being followed by someone. As reasonable risks the court could consider even the most hypothetical and ridiculous assumptions.

[165] Rothstein L.E. (2000) Privacy or Dignity?: Electronic Monitoring in the Workplace, New York Law Journal of International and Comparative Law, 19, 379-412, p. 384.

Canadian courts assess the reasonableness of privacy expectation in the totality of circumstances of particular case. That encompass detailed examination of all the relevant circumstances: place of the search, subject matter, whether intimate details were exposed etc. Such holistic approach allows to avoid subjectivity of judges and pretends to be the most justified. In contrast to the U.S. justice that obviously acts as employers' advocate, Canadian courts to certain extant are excessively favorable to employees (e.g. SGEU v Unifor, Local). ECtHR in its turn have not developed any specific method of assessing reasonableness of privacy expectation and tries to adhere to the golden mean.

Chapter 3 Employer's standpoint

The issue of electronic surveillance at workplace is usually considered through the prism of employees' rights and little attention is paid to causes and purposes of such monitoring. It is more than reasonable that employer can establish internal rules and control performance of duties by employees, otherwise he could suffer serious economic losses. Taking into account widespread digitalization of working process the issue of monitoring will not disappear and is need to be addressed in a balanced proportional way. Neither USA, nor Canada and ECHR guarantee an absolute right to privacy. Individual privacy interests are always balanced against community interests or rights of others. Nobody can claim that employee's monitoring is per se illegal. Taking into account that main data quality principles are based around the purpose of the processing personal data (data shall not be excessive in relation to the purpose; and stored no longer than it is required by the purpose), the definition of the purpose for processing personal is of crucial importance. So, let us consider what are the main business interests in employee's electronic surveillance and which of them could pretend to be legitimate interests.

First of all, one shall distinguish systematic and occasional employee monitoring that have different purposes behind them. While systematic monitoring is always an intended one, occasional employee monitoring could either be intended (e.g. in case of disciplinary investigation) or happen by chance.

Professor Michael Geist points out six main purposes of computer surveillance that illustrate systematic monitoring of employees: 1) preservation of employee productivity; 2) preservation of the computer network efficiency; 3) prevention of computer misuse and

potential liability for it; 4) ensuring corporate confidentiality; 5) uncovering computer crimes; 6) legal obligation of protecting information.[166]

Preservation of employee's productivity is not about employer's meanness and inclination for slave-owing, but about economic well-being of the company. As reported by L. Court "a company with 500 Internet users could lose almost a million dollars in productivity annually from just a half hour of daily Internet surfing by employees".[167] It's a quite fair interest of employer, but not weighty enough to intrude in employees' private lives, as far as this goal could be achieved by less intrusive means. For example, an employer could install software that would block access to social media and other websites that are not related to the exercise of work responsibilities. As far as all blocked websites could be easily accessed from personal smartphones, probably the better way is to use time tracking tools (e.g. daily reports on what you have done and how many time did you spend on each activity). Such tools would increase self-discipline of employees and therefore will have a positive effect on employees' productivity. What is more, monitoring of electronic communications as a method of raising employees' productivity could lead to completely different results, in particular "increased levels of stress, decreased job satisfaction and quality of work life, decreased levels of customer service and poor quality."[168]

Preservation of computer network efficiency means to protect it from downloading films and music and playing games that decelerate operation of the whole computer network and other employees cannot use it effectively. This reason is closely connected with the next one – prevention of computer misuse and potential liability for it. For example, in case of

[166] Geist, M.(2003) Computer and E-Mail Workplace Surveillance in Canada: The Shift From Reasonable Expectation of Privacy to Reasonable Surveillance, 82 Canadian Bar Review 151-189, p. 156-165.
[167] Court, L., & Warmington, C. (2004). The workplace privacy myth: why electronic monitoring is here to stay. *Employment and Labor Law*, *1*(1), 1-20. p. 18
[168] Watson, N. (2001). The private workplace and the proposed "notice of electronic monitoring act": is "notice" enough? *Federal Communications Law Journal*, 54(1), 79-104. p. 82.

downloading piracy content an employer could be liable for violation of copyright laws as Internet Service Provider. Traditionally the doctrine of respondeat superior makes the employer liable only for those acts of employee that fall within the scope of employment or correspond to employer's interests. However, courts could consider the scope employment in a broad sense. In Doe v. XYC Corporation[169]the employer was liable for actions of employee who published nude pictures of his stepdaughter using employer's computer. The Superior Court of New Jersey held that

"employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties. No privacy interest of the employee stands in the way of this duty on the part of the employer." [170]

Surprisingly though it may sound, employees could also benefit from workplace surveillance. For example, by increasing organization's efficiency, workplace monitoring raises employee's ability to advance. It can also assist in reducing or eliminating sexual, racial and other forms of harassment.[171] According to C. Muhl's "e-mail evidence itself is not enough to result in employer liability for sexual or racial harassment, especially when an employer has a mechanism for employees to report such complaints and takes remedial action after learning of the complaint".[172] At the same time he argues it could entail liability in case if e-mail evidence supplements other employer's pitfalls in this respect. Employer could be liable for harassment not only in case of civil claim, but even in criminal proceedings. According to the French Criminal Code employer could be criminally liable for rape and sexual aggression

[169] Doe v. XYC Corporation, 382 N.J. Super. 122 (App. Div. 2005)
[170] Ibid
[171] Weckert J. Electronic Monitoring in the Workplace: Controversies and Solutions. Hershey, PA: Idea Group Publishing, 2005- p. 6-7.
[172] Muhl C.H. Workplace e-mail and Internet use: employees and employers beware. Monthly Labor Review, v126 n2 p36-45 Feb 2003. – p.42

"committed on their account by their organs or representatives».[173] It could be concluded that under certain circumstances employer is even obliged to monitor employees' communications. However, it should be noted that prevention of harassment at workplace does not necessary requires motoring of the content of employees' e-mail. Special software exists for this purpose; it could identify specific harassment words and photos of certain body parts. For example, a program called Assentor uses linguistic analysis to detect abusing indicators; after that it rates the email on a scale of offensiveness and notifies a respective person about e-mail that breach the minimum level of offensiveness.[174] Thus, the intrusion into one's privacy would not be arbitrary, but based on a reasonable suspicion.

In the Information age, information serves as a main resource. Disclosure of company's confidential information could be resulted in its bankruptcy. According to "2009 Electronic Business Communication Policies and Procedures Survey" 14% of employees admitted to emailing confidential company information to third parties; 6% sent customers' credit-card data and Social Security numbers; and another 6% transmitted patients' electronic protected health information.[175] Confidentiality agreements could not always be considered as a sufficient measure to protect business secrets. One of the possible preventive measures to ensure corporate confidentiality is to introduce high financial sanctions in terms of confidentiality agreements.

Protection of confidential information is closely connected to legal obligation of protecting information – secret of adoption, medical, lawyer, bank secrecy etc. Thus, an obligation of a

[173] Penal Code of the French Republic [C. PEN.] art.121-2, 222-22, 222-31.
[174] Sundstrom S.A. (1998) You've got mail (and the government knows it): Aplying the Forth Amendment to workplace e-mail monitoring. New York University Law Review, 73, 2064-2102. p. 2065.
[175] Should Companies Monitor Their Employees' Social Media?,*Wall Street Journal*, October 23, 2014, sec. Special, http://www.wsj.com/articles/should-companies-monitor-their-employees-social-media-1399648685.

company to protect personal data of their clients leads to lesser level of personal data protection for employees, who have access to this information.

It would be fair to notice that monitoring of certain category of employees could be conducted for the interests of national security. For example, when an employee has access to state secrets, the employer has a legitimate interest in monitoring electronic communication of the employee in order to be sure in his/her reliability.

With regard to public employees another important concern is the correlation public employees' right to privacy and transparency of the government, which is a required attribute of a democratic society. Taxpayers are primarily interested in expenditure of budget money that would usually mean the disclosure of information about employees' salaries, pensions and other benefits which are financed from the budget. However, the context of public employees' electronic communications could also turn out to be an object of public scrutiny, as it occurred to be in City of San Jose vs. the Superior Court (Smith).[176] The main issue to be decided by the court is was whether electronic messages on business matters sent by public employees with the help of private devices (accounts) should be considered as "public records" according to the law and therefore disclosed to the public. The California Supreme Court ruled in favor of transparency. It has stated that files that comply with the definition of "public records" "do not lose this status because they are located in an employee's personal account".177 Thus it could be concluded that in case if public officials use private electronic communications to discuss business matters, the content of the messages could be legitimately disclosed not only to employers, but also to the general public with the purpose of transparency of governmental activities.

[176] City of San Jose v. Superior Court of Santa Clara County (Mar. 2, 2017, S218066).

[177] Ibid, p. 13.

Finally, employee monitoring could serve as a tool for fighting cyber crimes. The latter include unauthorized access, data modificatins and thefts, cyber frauds, cyber gambling etc. According to the findings of Ponemon Institute based on surveys of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil it was established the most serious consequances of cyber attacks for business are business disruption, loss of sensitive information and diminishment of reputation.[178] The cost to investigate, recover brand and reputation and invest in technologies ranges from an average high of $298,359 (U.S. $ dollars) for German organizations to an average low of $106,904 (U.S. $ dollars) for Brazilian organizations.[179]

An employer could use employee monitoring in order to prevent both internal and external cyber crimes. In addition to M. Geist classification, it should be noted that workplace monitoring could serve as a preventive measure not only for cyber-crimes, but for crimes and offenses in general, as it was for example, in Kopke v. Germany (see p. 19). When a certain crime is already committed, information received with the help of the monitoring of employee's electronic communications could be used as evidence.

Recommendations to employers

Even though employers registered in the United States are subjected to much stricter requirements than U.S. and European employers are in terms of protecting employees' digital privacy at workplace, I am strongly convinced that employers would only benefit from positive work environment and reputation of the company that respects employees right to privacy. Besides, perspectives of amending U.S. case law towards granting higher level of protection to employee's right to privacy at workplace are no so illusory at it may seem at the

[178] The Impact of Cybercrime on Business Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil, Independently conducted study by Ponemon Institute, May 2012, p. 16. Could be accessed at https://www.ponemon.org/local/upload/file/Impact_of_Cybercrime_on_Business_FINAL.pdf
[179] Ibid, p. 2.

first sight. First of all, the judges themselves already realize the need of reconsidering privacy concept in conformity with nowadays digital reality (see case United States v. Jones, § 2.3). Then, the aim could be achieved by the efforts of advocates who push an approach of considering employee monitoring through the prism of human dignity.

Transparency. As for now, I believe that transparency is the best way to balance interests of an employer and employees. Clear workplace privacy policy and notification of employees about means, objects and limits of monitoring digital communications could serve as the most obvious personalization of transparency principle. To a great extent an employee's expectation of privacy depends (or ideally should depend) on the clarity of the workplace privacy policy.

Personal use. One of the important issues that should be reflected in the internal policy is whether the use of communications for private purposes is actually allowed. Taking into account the important role, which electronic communications play in our everyday life and the urgent need to be connected with your family and relatives, a blanket ban on the use of electronic communication for private purposes looks at least disproportionate. Of course, this conclusion does not apply to professions where such ban is conditioned by safety reasons (e.g. aircrew) of simply impossible for technical reasons. It would be better to use different accounts for private and business purposes, however mark of personal e-mails also could serve as a worthy strategy.

Consent. With regard to a consent of employee to be subjected to monitoring, which is usually considered along with privacy policy, I would opt out to consider employee's consent as a legal ground to monitor electronic communications of employees. I am pretty sure that in case if same employees who gave their consent for electronic surveillance were asked to do it anonymously, the results would be quite opposite. Due to the dependent nature of employment relations the consent of employee does not usually represent the true will of an

employee and thus the notion of consent almost loses its initial meaning in the employment context.

Data protection principles. In any case even the most clear and detailed policy shall not lead to absolute monitoring of an employee's activity at workplace. There is no need to reinvent the wheel, in my view, requirements to the processing of personal data, introduced by the Council of Europe Convention No. 108, would perfectly safeguard the balance between employers' and employees' interests. The central issue here is the legitimate purpose of processing personal data (monitoring electronic communications of employees). The legitimate purpose criteria is quite flexible to adjust specific requirements posed to employers by the national legislation. So, obviously in the United States this spectrum will be broader than in European countries, but at least it will filter out the most ridiculous and foolish purposes of monitoring behind which employers could hide.

Supervision. I am deeply convinced that the way how employer draft the internal privacy policy for employees and the way he complies with the abovementioned policy should be subjected to external supervision. In the United States of America such control is possible only after concrete case is brought to the court and only within the limits of the plaintiff's claim. Besides the findings of the court apply only to relations between an employer and concrete employee, but does not create any implications for other less active employees who do not want to bother themselves by litigation procedures. And obviously if no one report about violation of privacy rights at the workplace – the court will never start the proceeding. Within the European legal framework the issue was solved by introduction of special data privacy authority that could consider employees' appeals in administrative procedure. Usually data protection commissioners are entitled to conduct investigations and issue binding prescriptions for an employer that violates data protection law.

Conclusion

Digitalization of our everyday life leads to the enlargement of the scope of right to privacy. Since the use of electronic communications became essential component of average working day the issue arise whether monitoring of the latter constitutes just another working condition established by an employer or embodies a new threat for employee's privacy? Well, actually both. Workplace monitoring interferes with right to privacy, but to certain extant, it is a compulsory measure that an employer needs to take in order to comply with legal obligation to protect confidential or secret information, to avoid potential liability for misuse of company's equipment by employees or to ensure democratic principle of transparency in case of public employees. With this regard, the task of the state is to provide more or less fair balance between employees' and employer's interests.

The comparative analysis shows that in U.S. employees' digital privacy is almost unprotected. It is not only employees who have poor level of protection of their privacy in the United States; it is a systemic issue condition by the peculiarities of the privacy concept in the United States. The main problem is that U.S. legislation lacks comprehensive data protection law that would enshrine the main principle of personal data processing that are represented in both the Council of Europe and Canada relevant legislation. The Electronic Communications Privacy Act allows U.S. employers to intercept employee's electronic communications unconditionally if 1) an employee gave his prior consent for such interception; 2) an employer provides equipment or facilities for electronic communications; 3) an employer acts as a private network provider. It is a rare case, but even if an employer does not provide equipment or does not act as network provider, he can always demand employee's formal consent for such interception. Taking into account unequal positions of an employee and an employer, employee's consent to be monitored is not likely to be indeed voluntary. In the absence of legal framework that provides clear system of checks and balances with regard to

processing of personal data (including legitimate purpose, not excessive amount of data, limited period of storage etc), employee's position could be potentially improved by court's human rights-oriented interpretation. But, as the analysis shows, American courts on the contrary tend to favor employers interests. In order to define whether employee's expectation of privacy was indeed reasonable courts use risk analysis test in terms of which they consider even the most hypothetical assumptions.

The application of the reasonable expectation of privacy test in the United States goes hand by hand with the third party doctrine, according to which once the information was voluntary disclosed to the third party. Even though courts started to make some attempts towards reconsidering the third party doctrine, in particular, to adjust it nowadays digital world reality, but for the moment it is still one of the judicial obstacles that does not allow to grant protection for employees' (and not only employees') right to privacy.

Even though Canadian jurisdiction had preconditions similar to the United States (absence of constitutional protection to right to privacy, strong distinction in regulating activity of public and private employers, developed federal structure, belonging to a common law system), Canada managed provide nearly similar level of protection for employees' digital privacy, as in Europe. The approach is based on exhaustive list of grounds for processing of personal data and five main data quality principles: 1) data shall be obtained fairly and lawfully; 2) data shall be processed in accordance with specified legitimate purpose; 3) data shall not be excessive in relation to the purpose; 4) data shall be accurate; 5) data shall be stored no longer than it is required by the purpose. The only substantial difference between the Council of Europe and Canadian jurisdictions is that Canadian legal framework does not provide higher level of protection for the processing of 'sensitive' personal data, disclosure of which would be especially harmful for individual, as far as personal data concerning health, sexual life, political opinions or religious beliefs are of exceptionally intimate nature. In contrast to U.S.

jurisdiction, Canadian courts assess reasonable expectation of privacy depending on «the totality of the circumstances» of a particular case (place, subject matter, prior display etc.) Such approach seems to be prudent and sound, as it considerably reduces judge's subjectivity. The European Court of Human Rights probably does not have sufficient practice yet to develop its own approach of applying a reasonable expectation of privacy test. However, the concept of the European Convention as a 'living instrument' is quite promising with regard to ensuring high level of right to privacy protection at the workplace.

On the basis of analyzed cases it could be concluded that the reasonable expectation of privacy test is quite subjective and in a broader sense it could actually lead to a lesser privacy protection as far as in a modern world one's expectation of privacy diminishes every day and the test does not pay proper attention to the fact whether the intrusion into privacy was indeed legitimate (even though it was expected). With this regard, application of the proportionality test seems to be far more fair and comprehensive.

I believe that the best way to balance employer's and employees' interests with regard to workplace monitoring is to develop clear and detailed privacy policy that would correspond to the main principles of personal data processing: data shall be obtained and processed fairly and lawfully for specified and legitimate purposes in an adequate not excessive manner in relation to the purpose. Private and business accounts of an employee should be clearly distinguished. As an option, to follow Israeli example and to distinguish four types of e-mail accounts: 1) used strictly for business purposes; 2) merely personal accounts; 3) "mixed" accounts; 4) personal accounts provided by employer. Definitely higher standards of protection should be applied to the monitoring of the content of electronic communications.

Ideally, statements of such policies should be so clear to exclude court's potential neglect. Remarkably though, in the USA the court found no reasonable expectation of privacy in case

where confidentiality of e-mails was assured by employer (Smyth v. Pillsbury Company). While in Canada it was established that employees could have reasonable expectation of privacy even when it is clearly stated in workplace policy that employees should not expect their communications to be confidential (SGEU v. Unifor).

Bibliography

Legal documents

International acts

Convention for the Protection of Human Rights and Fundamental Freedoms (1950)

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Jan. 28, 1981)

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

Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (Adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies).

Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies)

EU (2012), Charter of Fundamental Rights of the European Union, OJ 2012 C 326

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

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data;

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Article 29 Working Party, Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act, 5109/00/EN WP 39.

Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final/WP 48 (September 13, 2001).

Article 29 Data Protection Working Party, Working document on surveillance and monitoring of electronic communications in the workplace, 5401/01/EN/ Final/WP55 (29.05.2002).

Canada

Canadian Charter of Rights and Freedoms, s 8, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

Privacy Act (R.S.C., 1985, c. P-21)

Finland

Act on the Protection of Privacy in Working Life, 759/2004 (unofficial translation of the Ministry of Labour, Finland), available at
http://ec.europa.eu/justice/policies/privacy/docs/implementation/finland_759_04_en.pdf

France

Law of French Republic No. 91-646 of 10 July 1991 on the secrecy of correspondence issued by means of electronic communications. (Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques)

Penal Code of the French Republic, available at
https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations

USA

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C

U.S. Constitution

Cases

ECHR

Barbulescu v. Romania (application no. 61496/08), judgment of 12 January 2016.

Copland v. the United Kingdom (application no. 62617/00), judgment of 3 April 2007.

Gaskin v. United Kingdom (Application no. 10454/83), judgment of 7 July 1989

Halford v. the United Kingdom (application no. 20605/92), judgment of 25 June 1997

Handyside v. the United Kingdom *(*application no. 5493/72*)*, judgement of 7 December 1976

Kopke v. Germany (Application no. 420/07), decision as to the admissibility of 5 October 2010.

Kopp v. Switzerland (13/1997/797/1000), judgment of 25 March 1998
Lüdi v. Switzerland (application no. 12433/86), judgment of 15 June 1992.

Marckx v. Belgium (Application no. 6833/74), judgment of 13 June 1979

M.C. v. Bulgaria (Application no. 39272/98), judgment of 4 December 2003

Niemietz v. Germany (Application no. 13710/88), judgment of 16 December 1992

P.G. and J.H. v. the United Kingdom (application no. 44787/98), judgment of 25 September 2001.

Pretty v. United Kingdom *(*Application no. 2346/02), judgment of 29 July 2002

Rotaru v. Romania (Application no. 28341/95), judgment of 4 May 2000

Libert v. France (application № 588/13) (pending), communicated on 30 March 2015.

ECJ

ASNEF and FECEMD v. Administración del Estado, joined cases C-468/10 and C-469/10: Judgment of the Court (Third Chamber) of 24 November 2011.

Maximillian Schrems v. Data Protection Commissioner, European Court of Justice, Case C-362/13, 6 October 2015

Tzoanos v. Commission, Case T-74/96, 44 E.C.R. IA-00129, II-00343 (1998)

Canada

Hill v. Church of Scientology of Toronto, [1995] 2 S.C.R. 1130

Hunter v Southam Inc [1984] 2 S.C.R. 145

R. v. Cole, [2012] SCC 53, [2012] 3 S.C.R. 34
R. v. Debot, [1989] 2 S.C.R. 1140

R. v. Edwards, [1996] 1 S.C.R. 128

R. v. Plant, [1993] 3 S.C.R. 281

R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67

Re Doman Forest Ltd., [1990] 3 L.A.C. (B.C.) (4th) 275 at 280

S*GEU v* Unifor, Local 481 (2015), 255 LAC (4th) 353 (Ponak)

France

Décision de Cour de Cassation, Chambre sociale, du 2 octobre 2001, 99-42.942.

Israel

Labor Appeal no. 90/08 Tali Isakov Inbar v. Commissioner for Women Labor, dated, 08.02.2011.

Italy

Decision of the District Court of Turin, no. 143, dated, 20.08.2006.

Decision of the Italian Court of Cassation no. 47096, dated 11. 12. 2007

Spain

The Spanish Constitutional Court, judgement 241/2012 of 17 December 2012.

United Kingdom

Appeal No. UKEAT/0457/12/BA Atkinson v Community Gateway Association, judgment of the Employment Appeal Tribunal, dated 21.08.2014.

USA

Bill McLaren, Jr. v. Microsoft Corp. Case No. 05-97-00824, 1999 (Tex. App.)

City of San Jose v. Superior Court of Santa Clara County (Mar. 2, 2017, S218066)

Doe v. XYC Corporation, 382 N.J. Super. 122 (App. Div. 2005)

Katz v. United States, 389 U.S. 347 (1967)

Michael A. Smyth v. The Pillsbury Company, 914 F. Supp. 97 (E.D. Pa. 1996)

O'Connor v. Ortega, 480 U.S. 709 (1987)

Ontario v. Quon, 560 U.S. 746 (2010)

Watkins v. L. M. Berry & Co., 704 F.2d 577, 582–83 (11th Cir. 1983)

United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999)

United States v. Jones, 132 S. Ct. 945 (2012)

United States v. Knotts, 460 U.S. 276 (1983)

United States v White, 401 U.S. 745 (1971)

Books

Aidan O'Neill. EU Law for UK Lawyers. Oxford: Hart Publishing, 2011

Amitai Etzioni, Christopher J Rice. Privacy in a Cyber Age: Policy and Practice. Palgrave Macmillan, 2015.

Amitai Etzioni, The Limits of Privacy. Basic Books, 1999.

Gutwirth S, Leenes R, de Hert P. Reforming European Data Protection Law [e-book]. Dordrecht : Springer Netherlands : Imprint: Springer, 2015

Otto M. The Right to Privacy in Employment: A Comparative Analysis. Oxford: Hart Publishing, 2016.

Peers, Steve. n.d. The EU Charter of Fundamental Rights: a commentary. n.p.: Oxford : Hart Publishing, 2014.

Rikke Frank Jørgensen. Human Rights in the Global Information Society. MIT Press, 2006.

Sjaak Nouwt, Berend R. de Vries, Corien Prins. Reasonable Expectations of Privacy?: Eleven Country Reports on Camera Surveillance and Workplace Privacy. The Hague: T.M.C. Asser Press, 2005.

Weckert J. Electronic Monitoring in the Workplace: Controversies and Solutions. Hershey, PA: Idea Group Publishing, 2005.

Articles

Bagdanskis, T., Sartatavicius, P. Workplace privacy: different views and arising issues. Jurisprudence, № 19(2) (2012).

Blanpain, R.'Protection of employees' personal information and privacy'. Bulletin for Comparative Labour relations № 88 (2014)

Colette Cuijpers, ICT and Employer-Employee Power Dynamics: A Comparative Perspective of United States' and Netherlands' Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning of Employees, 25 J. Marshall J. Computer & Info. L. 37 (2007).

Court, L., & Warmington, C. The workplace privacy myth: why electronic monitoring is here to stay. Employment and Labor Law, *1*(1), 1-20. (2004).

Geist, M.Computer and E-Mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance, 82 Canadian Bar Review 151-189 (2003).

Gomez-Arostegui, H. Tomas. Defining Private Life under the European Convention on Human Rights by Referring to Reasonable Expectations. - California Western International Law Journal, Vol. 35, Issue 2 (Spring 2005)

Kambellari, E. Employee email monitoring and workplace privacy in the European perspective. - Iustinianus Primus Law Review № 08 - volume 5:1 (2014)

Muhl C.H. Workplace e-mail and Internet use: employees and employers beware. Monthly Labor Review, Vol.126 №2, 36-45 (Feb 2003)

Otto M. The right to privacy in the employment: in search of the European model of protection, European Labour Law Journal, vol.6 №4 (2015).

Rothstein L.E. Privacy or Dignity?: Electronic Monitoring in the Workplace, New York Law Journal of International and Comparative Law, 19, 379-412 (2000).

Stanley J. The crisis in Fourth Amendment Jurisprudence. *American Constitution Society for Law and Policy,1-20* (May 2010)

Sundstrom S.A. You've got mail (and the government knows it): Aplying the Forth Amendment to workplace e-mail monitoring. New York University Law Review, 73, 2064-2102 (1998)

Watson, N. The private workplace and the proposed "notice of electronic monitoring act": is "notice" enough? *Federal Communications Law Journal*, 54(1), 79-104 (2001).

Yohei Suda, Monitoring E-mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States, 4 Wash. U. Global Stud. L. Rev. 209 (2005)

Publications

Mirchin, D. (2012). Monitoring Employee Online Activity: Landmark Case Establishes Guidelines. Information Today, 29 (2).

Should Companies Monitor Their Employees' Social Media? Wall Street Journal, October 23, 2014, sec. Special, http://www.wsj.com/articles/should-companies-monitor-their-employees-social-media-1399648685.

Other sources

DLA Piper's Data Protection Laws of the World Handbook, accessed 01 February 2016, http://www.dlapiperdataprotection.com/#handbook/law-section/c1_CA

Guidance Notes on Monitoring of Staff by Data Protection Commissioner of Ireland, accessed at https://www.dataprotection.ie/docs/Guidance-Notes-Monitoring-of-Staff/m/208.htm.

Official web-site of the Council of Europe www.coe.int

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.
Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), 442/16/EN, WP 236, 2 February 2016.

The Impact of Cybercrime on Business Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil, Independently conducted study by Ponemon Institute, May 2012

The Notice of Electronic Monitoring Act, H.R. 4908, 106th Congress (2000).

The Privacy for Consumers and Workers Act, H.R. 1900, S. 984, 103rd Congress (1993).