DOI: 10.5817/MUJLT2017-2-1

# TO POST, OR NOT TO POST – THAT IS THE QUESTION: EMPLOYEE MONITORING AND EMPLOYEES' RIGHT TO DATA PROTECTION

*by*

ADRIENN LUKÁCS*

*Nowadays social media have a growing importance in several areas of our lives. They are used for numerous objectives: self-expression, keeping in touch with acquaintances, communication or obtaining information about the latest events and news. During their use the individual shares a significant amount of personal data. This conduct can have serious implications for employment. The (prospective) employer is interested in the surveillance of these sites for several reasons, as he/she can easily gain insight into the individual's private life and obtain, without costs, detailed information about him/her. The legal problem arising is that the employee's fundamental rights – namely the right to privacy and the right to data protection – collide with the employer's legitimate interests.*

*The aim of the paper is to highlight the different rights and interests present on the two sides of the parties in the employment relationship; focusing on the employee's right to data protection and on the employer's legitimate interests in monitoring employees. As a result of the paper, I will draw attention to the legal problems lying behind social network background checks and monitoring. I will provide recommendations on how users and employers can continue using these sites while still preserving privacy.*

## KEY WORDS

*Privacy, Data Protection, Social Network Sites, Employment Law, Employee Monitoring*

* lkcs.adrienn@gmail.com, Ph.D. student, University of Szeged, Hungary and University Paris 1 Panthéon Sorbonne, France.

## 1. INTRODUCTION

Social media are of increasing importance in our everyday lives, they have become one of the main forms of communication and self-expression. It is easy to see that during their use an enormous amount of personal data is shared, which can have serious implications for the professional life of the individual. The aim of the paper is to analyse what data protection rights the employees dispose during the use of social network sites, what their interests are in using these sites and how these interests and rights collide with the employer's desire to monitor Facebook in order to enforce his/her legitimate interests. The paper focuses on the subject from the view of the European Union law, with special regard to the data protection directive and the data protection regulation. The original contribution of the paper is that it gives clarity to the present understanding of the problem and it examines exhaustively the data protection challenges arising during the use of social network sites, focusing specifically on the characteristics of the employment context. The overarching research question that I intend to answer is what special data protection questions arise during the different phases of the employment relationship and how the employee's right to data protection can be respected during employee monitoring.

As regards methodology, I conducted desktop research and I applied descriptive and analytical approach to examine the research subject. First, I am going to examine what the main interests and rights underlying the employee use of Facebook are, then I am going to examine why the (prospective) employer is interested in monitoring the (prospective) employee's activity on online social networks. In the next part I am going to review the main data protection problems and challenges regarding social network background checks and monitoring conducted by the employer, and in the last part of my paper I am going to provide possible solutions and recommendations towards the privacy friendly use of social network sites.

## 2. WHY DO EMPLOYEES USE FACEBOOK?

Nowadays we can experience the growing popularity of social network sites (hereinafter referred to as: SNS). In order to address the question of SNS use and privacy, first, I am going to examine our subject in a broader

context and I am going to look into the reasons that drive the individual to use these sites. Then I am going to present the legal framework applicable to privacy and data protection.

## 2.1 REASONS UNDERLYING THE USE OF SOCIAL NETWORK SITES

The first SNS – SixDegrees – appeared in 1997[1], and since then several others have followed.[2] *Boyd* and *Ellison* define SNSs as

> *"web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."*[3]

Through the use of SNSs, users can create their own content, stay in touch with their friends, watch and share photos or videos, etc. – depending on the particular properties of the given SNS. All these activities come with the share of personal data. In my paper I will mostly use the example of Facebook, instead of SNSs in general, as it is the most popular SNS today, with the highest number of users worldwide.[4] All generations are present on Facebook,[5] meaning that employees and prospective employees use these sites just like any other individual.

SNSs have a significant role in our everyday lives. *Grimmelmann* argued that nowadays SNSs constitute an important tool for social interaction, as they can fulfil basic human needs like self-expression, communication and being part of a community.[6] *Clark* and *Roberts* note that technology has always had a significant impact on how people communicate

---

1 Boyd, D. M. and Ellison, N. B. (2008) Social Network Sites: Definition, History and Scholarship. *Journal of Computer Mediated Communication*, 13 (1), p. 214.

2 On the (not exhaustive) list of SNSs see *List of social networking websites.* [online] Wikipedia. Available from: https://en.wikipedia.org/wiki/List_of_social_networking_websites [Accessed 9 November 2016].

3 Boyd, D. M. and Ellison, N. B. (2008) Social Network Sites: Definition, History and Scholarship. *Journal of Computer Mediated Communication*, 13 (1), p. 211.

4 Facebook had 1.79 billion monthly active users worldwide in 2016. Source: *Number of monthly active Facebook users worldwide as of 3rd quarter 2016 (in millions).* [online] Statista. Available from: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [Accessed 17 January 2017].

5 On the distribution of users of different ages see these statistics of 2014: *Distribution of active Facebook users worldwide as of 4th quarter 2014, by age.* [online] Statista. Available from: https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/ [Accessed 17 January 2017].

6 Grimmelmann, J. (2009) Saving Facebook. *Iowa Law Review*, 94 (4), p. 159.

(e.g. telegraph, telephone, the Internet, etc.) and SNSs should be considered as a next step of human interaction, therefore they shall receive adequate protection.[7] The individual can express himself/herself through different ways on these sites. It ensues from the very nature of these sites that, in order to use them properly, the sharing of personal information is needed.[8] SNSs seem to have changed what society considers to be private, as users from all over the world share personal data in a quantity and quality never seen before.[9] It is not only the SNSs themselves which encourage the user to use their services (and to share more and more data[10]), but the (informational) societal pressure is also an important factor. If everyone is present on these sites, staying away from them – in the age of information, when our life is centered on information – can entail serious disadvantages, as the user would not be able to use certain services and have the same possibilities as the other users.[11]

From a legal perspective, the *Council of Europe's Committee of Ministers* emphasized the importance of the Internet and SNSs in promoting the exercise and enjoyment of human rights and fundamental freedoms, stating that they can also enhance participation in social and political life and promote democracy and social cohesion.[12] The president of the French data protection authority, *Falque-Pierrotin* also emphasized the role of the Internet in promoting the exercise of individual and public liberties – especially freedom of expression and right to information – and argued that the exercise of these rights is inseparable from the question of privacy protection.[13] One employment specific example can be the exercise

[7] Clark, L. A. and Roberts, S. J. (2010) Employer's Use of Social Networking Sites. A Socially Irresponsible Practice. *Journal of Business Ethics*, 95 (4), pp. 508–509, 518.

[8] *Herbert* describes the phenomenon of electronic exhibitionism, which means *"the increasing worldwide phenomenon of individuals eviscerating their own privacy by affirmatively or inadvertently posting and distributing private and intimate information, thoughts, activities and photographs via email, text messaging, blogs, and social networking pages."* See Herbert, W. A. (2011) Workplace Consequences of Electronic Exhibition and Voyeurism. *IEEE Technology and Society Magazine*, 30 (3), p. 26.

[9] International Working Group on Data Protection in Telecommunications (2008) *Report and Guidance on Privacy in Social Network Services "Rome Memorandum"*, 3-4 March. Rome, Italy, 675.36.5., Available from: http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf [Accessed 26 May 2017], p. 1.

[10] See for example González Fuster, G. and Gutwirth, S. (2008) Privacy 2.0? *Revue du droit des Technologies de l'Information,* (32), p. 352.

[11] Cseh, G. (2013) A közösségi portálok árnyoldalai. *Infokommunikáció és jog*, 10 (2), p. 90.

[12] Council of Europe (2012) *Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services.* CM/Rec(2012)4, 4 April 2012.

[13] Falque-Pierrotin, I. (2012) La Constitution et l'Internet. *Les Nouveaux Cahiers du Conseil Constitutionnel*, (36, June), pp. 34–35.

of collective labour rights, as communication on SNSs might also serve the activity of trade unions, etc.

## 2.2 THE RIGHT TO PRIVACY AND THE RIGHT TO DATA PROTECTION ON SOCIAL NETWORK SITES

We could see that nowadays the use of SNSs has become a part of everyday life and they are useful tools in communication, self-expression and the exercise of certain fundamental rights. We could also see that the use of SNSs naturally comes with the share of personal data, so in my opinion if we accept SNSs as the new form of communication and self-expression, we cannot *automatically* say any more that the user himself/herself contributes to the destruction of his/her own privacy.[14] Therefore, SNSs deserve effective legal protection. Still, during the use of SNSs serious legal issues arise: namely, issues regarding the right to privacy and the right to data protection. The protection of the right to privacy and to data protection shall by all means be respected on these sites and not only because their insurance is a condition for being able to fully enjoy the possibilities given by SNSs. If users are afraid to use SNSs because of the fear that someone – in our case the employer – might use the information available on these sites, the freedom and fundamental rights of the individual will be impaired.[15]

The right to privacy and the right to data protection are not synonymous concepts, and in my article I will mainly focus on the data protection aspect. However, a very brief discussion of the right to privacy is also needed as data protection can be retraced to the right to privacy. Although privacy itself has its origins as early as in ancient societies, it only became a generally accepted right in the 19th–20th century.[16] More precisely, the right

[14] For example, in the case that Simms calls self-presentation, sharing should not count as privacy self-destruction, considering the changed social norms. On the difference between self-presentation and self-disclosure see Simms, M. (1994) Defining Privacy in Employee Health Screening Cases: Ethical Ramifications Concerning the Employee/ Employer Relationship. *Journal of Business Ethics*, 13 (5), pp. 315–325. Cited in: Clark, L. A. and Roberts, S. J. (2010) Employer's Use of Social Networking Sites. A Socially Irresponsible Practice. *Journal of Business Ethics*, 95 (4), p. 512.

[15] See more on why SNSs should be protected: Clark, L. A. and Roberts, S. J. (2010) Employer's Use of Social Networking Sites. A Socially Irresponsible Practice. *Journal of Business Ethics*, 95 (4), pp. 507–525.

[16] On the subject of the history and definition of the right to privacy see more in: Lukács, A. (2016) What is Privacy? The History and Definition of Privacy. In: Keresztes, Gábor (ed.): *Tavaszi Szél 2016 Tanulmánykötet I,* Budapest, 15- April. Budapest: Doktoranduszok Országos Szövetsége, pp. 256–265. Available from: http://www.dosz.hu/dokumentumfile/ TSZ_I_kotet_161114_574o.pdf [Accessed 4 May 2017].

to privacy appeared at the end of the 19th century, in the famous article of *Warren* and *Brandeis* in 1890, entitled "The Right to Privacy". To date, there is no uniform definition on what (the right to) privacy[17] is, in spite of the fact that numerous legal scholars made an attempt to define it: *Warren* and *Brandeis* defined the (right to) privacy in the above mentioned article as

> *"the right to be let alone".*[18]

*Posner* argued that

> *"one aspect of privacy is the withholding or concealment of information."*[19]

*Westin* stated that privacy is

> *"the claim of an individual to determine what information about himself or herself should be known to others",*[20]

while *Fried* defined privacy as

> *"[…] the control we have over information about ourselves."*[21]

*Máté Dániel Szabó* argued that

> *"privacy is the right of the individual to decide about himself/herself."*[22]

In the 1960s, with the appearance of computers, new legal protection was needed and the right to data protection appeared. Despite the high amount of attention paid to data protection, to date, there is still no uniform standpoint on the relation between the right to data protection and the right to privacy.[23] In my article I will stick to the opinion of *Jóri*, who interpreted the right to data protection as

---

[17] The protection of privacy can appear in different aspects: the protection of information, human body, communication, location. (See Hajdú, J. (2005) *A munkavállalók személyiségi jogainak védelme.* Szeged: Pólay Elemér Alapítvány, p. 10.) In my article I will focus on informational privacy.

[18] Warren, S. D. and Brandeis, L. D. (1890) The Right to Privacy. *Harvard Law Review*, 4 (5), p. 193.

[19] Posner, R. A. (1978) The Right of Privacy. *Georgia Law Review*, 12 (3), p. 393.

[20] Westin, A. F. (2003) Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59 (2), p. 431.

[21] Fried, C. (1968) Privacy. *The Yale Law Journal*, 77 (3), p. 482.

[22] Szabó, M. D. (2005) Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. *Információs Társadalom*, 5 (2), p. 46.

*"a unique legal way to protect the private sphere of the individual",*[24]

so it also aims to protect privacy, but this right can effectively ensure the protection of privacy in our digital era.[25]

Several *international documents* acknowledge the right to respect for private life and personal data protection both at the universal and at the regional level.[26] In the *European Union* the Charter of Fundamental Rights of the EU acknowledges as a fundamental right both the right to privacy (Article 7) and to data protection (Article 8). The right to data protection is further elaborated in Article 16 of the Treaty on the Functioning of the European Union and in the data protection directive (hereinafter referred to as: DPD)[27] and data protection regulation (hereinafter referred to as: GDPR).[28, 29] The requirements laid down in these documents are general dispositions, meaning they shall also be applied

---

[23] Purtova, N. (2010) Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights. *Netherlands Quarterly of Human Rights*, 28 (2), p. 181. See more on this subject Kokott, J. and Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3 (4), pp. 222–228.; Gellert, R. and Gutwirth, S. (2013) The legal construction of privacy and data protection. *Computer Law and Security Review*, 29 (5), pp. 522–530.

[24] Jóri, A. (2009) *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése.* Ph.D. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola, p. 9.

[25] Ibid.

[26] Regarding the right to privacy, Article 12 of the *Universal Declaration of Human Rights* (United Nations, 1948), Article 17 of the *International Covenant on Civil and Political Rights* (United Nations, 1966), Article 8 of the *European Convention of Human Rights* (Council of Europe, 1950) and Article 7 of the *Charter of Fundamental Rights of the European Union* (2000) state that the right to privacy is a fundamental human right and everyone has the right for his/her private and family life, home and correspondence to be respected, and they have the right to protect themselves against an unlawful interference.

Regarding the right to data protection, the *Guidelines for the Regulation of Computerized Personal Data Files* (United Nations, 1990), the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) and *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013) and the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Council of Europe, 1981) shall be mentioned.

[27] 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. O*fficial Journal of the European Union*. (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281: FULL&from=EN [Accessed 4 May 2017].

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017].

[29] It is not the aim of the present paper to distinguish between these two norms. Throughout my paper I will refer very briefly to both documents, as the GDPR already entered into force in 2016, but the DPD is still applicable till 2018.

to the case of SNSs and to data processing conducted by the employer. Focussing specifically on the employment context, several norms deal especially with the question of employee privacy/data protection.[30] Also, the European Court of Human Rights has an important case law in which the body acknowledged and developed the rules regarding employee privacy protection.[31]

Users are entitled to the right to privacy and to data protection during the use of SNSs. However, these rights are not absolute, the employer disposes certain legitimate interests which can prevail over the rights of the employees or can limit the use of SNSs. Before addressing the data protection challenges regarding the monitoring of employee SNS use, I am going to examine what kind of interests the employer has in monitoring the (prospective) employee's activity on SNSs.

## 3. WHY DO EMPLOYERS USE FACEBOOK?

Regarding the question of data protection and the employer's legitimate interests, it is obvious that employers would like to know as much as possible about their employees. This is not a new phenomenon, as one of the early examples the Ford Motor Company can be cited, where Henry Ford investigated the employees' lifestyles in detail at the beginning of the 20th century.[32] Since then, technology has become more sophisticated and made it easier to have access to all kinds of information about employees: it is enough to think of telephone and computer monitoring (e-mail and the Internet surveillance). On SNSs users share an enormous amount of personal data, from which the employer can draw consequences regarding the employees' professional aptitudes, loyalty, etc. By obtaining all this information, the employer can enforce different legitimate business interests. This is not a new phenomenon; SNSs only put the already existing interests into a different light by providing an unprecedented quantity

[30] See for example *"Protection of workers' personal data."* An ILO code of practice (International Labour Organization, 1997), *Recommendation no. R (89) 2 of the Committee of Ministers to member states on the protection of personal data used for employment purposes* (Council of Europe, 1989) and *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment* (Council of Europe, 2015).

[31] See for example the *Niemietz v. Germany* (1992), Application no. 13710/88, European Court of Human Rights, 16 December *Halford v. the United Kingdom* (1997), Application no. 20605/92, European Court of Human Rights, 25 June or the very recent *Bărbulescu v. Romania* (2016), Application no. 61496/08, European Court of Human Rights, 12 January.

[32] Sprague, R. (2011) Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. *University of Louisville Law Review*, 50 (1), p. 6.

and quality of personal data available online. Also – unlike the traditional methods of monitoring – new ways of monitoring (like SNSs) aim to monitor activities conducted outside the workplace and beyond working hours.[33] In my opinion, this is the characteristic that distinguishes most SNS monitoring from the traditional types of monitoring, and makes a more severe intrusion into the private sphere of the employee possible.

The starting point is that the employer aims to provide employment in order to achieve his/her economic goals, maximizing productivity and profitability. This has different aspects during the different phases of the employment relationship. It shall not be forgotten that during the enforcement of these interests the employees still dispose the right to privacy and to data protection. So the legal issue arising with regard to employee monitoring is that a collision can be found between the employee's rights and the employer's legitimate interests. There are fundamental rights and significant interests on both sides, so a balance of their enforcement must be found and respected during the creation of regulations and the application of monitoring.[34] I will present three phases, although they cannot be distinguished sharply: before, during and after the employment relationship.

### 3.1 BEFORE THE EMPLOYMENT RELATIONSHIP

During the hiring phase, the employer has the right to choose between the candidates and he/she is interested in contracting with the best candidate. He/she has the right to decide with whom to contract. By conducting an SNS background check, the employer can enforce this interest, as information available on SNSs can contribute to making the hiring decision. Information like inappropriate texts or comments, criticism of the previous employer, unsuitable photos, spelling mistakes, sharing of false information, or membership in certain groups can be very revealing.[35] Also, personality traits and moral convictions can influence the performance of work.[36]

---

[33] Kajtár, E. (2015) Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship. *Acta Juridica Hungarica*, 56 (4), p 269.

[34] Hajdú, J. (2005) *A munkavállalók személyiségi jogainak védelme.* Szeged: Pólay Elemér Alapítvány, p. 20.

[35] Sprague, R. (2011) Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. *University of Louisville Law Review*, 50 (1), p. 5.

[36] Abril, P. S., Levin, A. and Del Riego, A. (2012) Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. *American Business Law Journal*, 49 (1), p. 70.

Also, this information can be obtained in a very easy and inexpensive manner, especially when the candidate does not use the privacy settings. With the appearance of SNSs, the employer needs only a few clicks to access information which would not have been available for him/her (or only with great efforts and expenses, such as hiring a private detective) in the pre-Internet age. Another important issue is also evoked as not legitimate interests can be enforced, too: in practice, the employer might use these sites to discriminate among the candidates by basing the decision on protected characteristics.[37]

### 3.2 DURING AND AFTER THE EMPLOYMENT RELATIONSHIP

*During the existence of the employment relationship*, the employer might monitor SNS use at the workplace during working hours and outside the workplace beyond working hours. *During working hours* the use of SNSs can represent a huge loss of working time and productivity. While the employer has the obligation to pay the salary and to ensure proper working conditions, the employee has the obligation to perform the work. Naturally, the employer is interested in employing someone who performs the work satisfactorily,[38] and he/she has rights to ensure effective management. Ensuing from the nature of the employment contract, the employer is entitled to monitor whether the employee carries out his/her task and fulfils his/her duties correctly. Furthermore, he/she is interested in ensuring productivity and profitability.[39] So naturally he/she wants to control and monitor whether the employee is really working or hanging out on Facebook instead. This case is very similar to the problems regarding the use of the employer's computer for private purposes. For example, the European Court of Human Rights has recently confirmed the dismissal of an employee for personal use of the employer's

---

[37] See, for example Manant, M., Pajak, S. and Soulié, N. (2014) *Online social networks and hiring: a field experiment on the French labor market*. [in press] *Munich Personal RePEc Archive*. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2458468 [Accessed 2 February 2017].

[38] Miller, S. and Weckert, J. (2000) Privacy, the Workplace and the Internet. *Journal of Business Ethics*, 28 (3), p. 257.

[39] Persson, A. J. and Hansson, S. O. (2003) Privacy at Work – Ethical Criteria. *Journal of Business Ethics*, 42 (1), p. 65; Sprague, R. (2007) From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace. *The John Marshall Journal of Information Technology & Privacy Law*, 25 (1), p. 4.

equipment (violating the company's internal regulation) in the *Bărbulescu v. Romania* case.[40]

The novelty of SNSs is that they make it possible to monitor – unlike the "traditional" monitoring of computer or the Internet use for personal purposes at the workplace – the activities of the employee conducted *outside the workplace and beyond working hours*. After working hours, the employees' online activity can also represent risks for the employer. The employer's reputation can be at stake either directly through too sharp posts or comments, or indirectly if the employee's not appropriate lifestyle can be associated with the employer's image. An example for too sharp criticism can be found in a French ruling, where an employee was dismissed because she insulted her supervisor in an abusive manner in a Facebook comment.[41] As regards not appropriate lifestyle, see for example the case of the American high school teacher, Ashley Payne, who was dismissed for posting pictures of herself holding a pint of beer and a glass of wine in her hand during her trip to Europe.[42] As *Abril et al.* pointed out:

> *"[c]onventional wisdom dictates that an employee is a representative of his/her organization in all areas of life."*[43]

The divulgation of trade secrets can also be an issue. The employees shall respect the reputation and the business secrets of the employer. Besides taking the necessary steps against these infringements (e.g. removing the content, etc.), the employer is also interested in making certain of the loyalty of his/her employees. Information obtained from SNSs can help the employer to make human resourcing decisions; the information acquired can help him/her to decide on promotions or dismissals.

*After the termination of the employment relationship* the interest in protecting the reputation and business secrets still exists, as the former employee can harm the employer's reputation or violate his/her trade secrets. SNSs can also play a role in monitoring whether the former

---

[40] *Bărbulescu v. Romania.* (2016) Application no. 61496/08. European Court of Human Rights, 12 January.

[41] *Barbera v. Sté Alten Sir.* (2010) Application no. 10/00853. Conseil de Prud'hommes de Boulogne-Billancourt, 19 November.

[42] Oppenheim, R. (2013) *High School Teacher Files an Appeal in Case of Social Media Related Resignation.* [online] California Business Litigation Blog. Available from: https://www.californiabusinesslitigation.com/2013/05/high_school_teacher_files_an_a.html [Accessed 4 May 2017].

[43] Abril, P. S., Levin, A. and Del Riego, (2012) Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. *American Business Law Journal*, 49 (1), p. 89.

employee respects the potential non-compete obligation or non-solicitation clause.[44]

These interests are acknowledged in the labour law regulation, too. Although they are not absolute, during their enforcement the employer shall respect the fundamental rights of the employees. However, during the enjoyment of these rights the employee shall also respect the employer's legitimate interest: a balance shall be found between the two parties. In the next part I am going to review the main data protection challenges arising during this collision of rights and legitimate interests.

## 4. QUESTIONS AND PROBLEMS

Although the collision of the employee's fundamental rights and the employer's legitimate interests has already existed, the appearance of SNSs raises new types of issues both on the employee's and the employer's side. These problems and questions shall be addressed before striking the balance between the employee's fundamental rights and the employer's legitimate interests. First, I am going to examine these challenges from the employee's perspective and then from the employer's view.

### 4.1 CHALLENGES POSED REGARDING THE EMPLOYEE'S RIGHTS

From the employee's side, attention shall be drawn to *the right to informational self-determination.* The right to informational self-determination requires that the individual is aware who processes his/her data, what kind of data and for what purposes.[45] The problem with SNS monitoring is that the employee loses control over his/her personal data for various reasons.

First, SNS background checks are invisible, it is quasi impossible for the employee to prove (or know) that the decision was based

[44] See for example Anderson, D. R. (2011) Restricting Social Graces: The Implications of Social Media for Restrictive Covenants in Employment Contracts. *Ohio State Law Journal*, 72 (4), pp. 881-908. and Warren, M. and Pedowitz, A. (2011) Social Media, Trade Secrets, Duties of Loyalty, Restrictive Covenants and Yes, the Sky is Falling. *Hofstra Labor and Employment Law Journal*, 29 (1), pp. 99–113.

[45] The right to informational self-determination first appeared in Germany with the famous population census judgement of the Federal Constitutional Court in 1983. In its decision the Court has adopted basic data protection principles, which later appeared in the DPD, too, as key principles. Source: Hornung, G. and Schnabel, C. (2009) Data protection in Germany I: The population census decision and the right to informational self--determination. *Computer Law and Security Review*, 25 (1), p. 87.

on the content found on SNSs, especially in the hiring phase.[46] Therefore the employee will not know what data the employer has access to, how he/she will interpret that information, the requirement of prior information and the principle of transparency guaranteed by the EU regulation will be infringed.[47] According to the principle of transparency, the employee shall be informed of the existence of the processing and be aware of the characteristics of the processing, and it shall be done in a concise, easily understandable manner.[48] This means that when the employer conducts a background check of candidates, or monitors the online activity of employees, he/she should inform them in advance that such processing will take place.

Second, it follows from the invisible nature of these searches that the employee cannot participate in the data processing and cannot exercise his/her rights. Both the DPD and the GDPR acknowledge the rights of the data subject (e.g. the right of access, right to information, right to objection, to rectification, to erasure).[49] The right of access guarantees that the employee has access to personal data concerning him/her, therefore

---

[46] Kajtár, E. (2015) Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship. *Acta Juridica Hungarica*, 56 (4), p. 278.

[47] 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. *Official Journal of the European Union.* (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=EN [Accessed 4 May 2017], Section IV; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Article 5.1.(a), Article 12–14.

[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Recital 60, 58.

[49] See more on the rights of the data subjects: 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. *Official Journal of the European Union.* (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=EN [Accessed 4 May 2017], Sections IV-VII.; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Chapter III.

he/she can be aware of the processing and verify its lawfulness.[50] We will see in the next section that information obtained from SNSs are not reliable, therefore it is crucial to ensure the participation of the data subject in the processing, by guaranteeing the exercise of the above mentioned rights. The reliability of the information is closely connected to the data quality principles, which will be presented in the next section.

Third, it is also a problem that, although in a lot of cases personal data were made available by the user himself/herself, it is still possible that third persons post data about the individual. Thus it is not necessarily the user who contributes to the destruction of his/her own privacy, but third persons can also share content about the data subject without his/her consent; or even worse, without his/her knowledge.[51] In such cases the employee loses control over his/her e-reputation. Furthermore – although in a legal way it does not exempt the user – it constitutes a problem that users may not be aware of the functioning of SNSs and may be mistaken regarding the public or private nature of the published content,[52] publishing something presuming that it would be accessible only to a narrow circle of users – e.g. only to friends – but not to the employer. At the same time, considering that it is not uncommon for a user to have several hundreds of "friends", the content might be available to hundreds or thousands of users, depending on the chosen privacy settings.

A differentiation between the methods of obtaining data from SNSs shall be also made. The most obvious way of access is when the employer accesses the data when the data protection settings are set to public so he/she can have public access to the candidate's profile (either from outside the SNS or from the company's profile). However, the other practices cannot be forgotten: the employer can have access by logging

[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Recital 63.

[51] Clark, L. A. and Roberts, S. J. (2010) Employer's Use of Social Networking Sites. A Socially Irresponsible Practice. *Journal of Business Ethics*, 95 (4), p. 516.; Smith, W. P. and Kidder, D. L. (2010) You've been tagged! (Then again, maybe not): Employers and Facebook. *Business Horizons,* 53 (5), p. 495.

[52] See more Sprague, R. (2011) Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. *University of Louisville Law Review*, 50 (1), p. 15.; Kajtár, E. and Mestre, B. (2016) Social networks and employees' right to privacy in the pre-employment stage: some comparative remarks and interrogations. *Hungarian Labour Law E-journal*, (1), pp. 24–25.

into another user's profile, or even by hacking, by requiring password, by making the employee change the privacy settings, or making him/her add the employer to his/her contacts, observing the profile in his/her presence, etc.[53] The hierarchal relation between the employee and the employer shall also be mentioned. The employer might take advantage of his/her position to gain access to certain content posted by the employees. For example, in the US case *Pietrylo v. Hillstone Restaurant* the employer accessed a private chat room where employees had a discussion, by obtaining the login credentials of one of the employee, who gave them to the employer in the fear of getting in trouble in the case of not complying with the request.[54] Also, as there are not yet clear social conventions about social media use[55] – for example, what should the employee do if the employer adds him/her as a friend? Can the employee ignore the friend request without consequences or is he/she "obliged" to accept it?

## 4.2 CHALLENGES POSED REGARDING THE ENFORCEMENT OF THE EMPLOYER'S LEGITIMATE INTERESTS

SNSs pose a risk not only for the employee, but also for the employer. From the employer's perspective, the main question regarding the respect of the employee's right to data protection is why the employer would *not* want to consult all this freely and easily accessible vast amount of data made available in most cases by the user himself/herself? The employer as a data controller shall comply with the obligations laid down by the data protection regime. It should not be forgotten that the application of these data protection requirements in practice depends on the exact circumstances of the given job.

---

[53] Engler, P. and Tanoury, P. (2007) Employers Use of Facebook in Recruiting. In: Dan McIntosh, Ralph Drabic, Kristina Huber, Igor Vinogradov and Michael Bassick (eds.), *The Ethical Imperative in the Context of Evolving Technologies.* University of Colorado Leeds School of Business, pp. 65–66. Available from: http://www.ethicapublishing.com/ethical imperative.pdf [Accessed 13 July 2016].; Park, S. (2014) Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy. *American Business Law Journal*, 51 (4), p. 790.

[54] *Pietrylo v. Hillstone Restaurant Group.* (2009) Civil Case No. 06–5754 (FSH). United States District Court, D. New Jersey, 25 September.

[55] Van Eecke, P. and Truyens, M. (2010) Privacy and social networks. *Computer Law and Security Review*, 26 (5), p. 536.

Considering only the aspects which are the most problematic in relation to our topic: every data processing shall have a *finality*, meaning that data shall be collected

> *"for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".*[56]

We could see in Part 3 *why* employers can be interested in monitoring activities on SNSs, in this section it will be examined *how* they can process employee personal data and what other requirements need to be respected. The data processing has to be *legitimate/lawful*, meaning that it has to have one of the legal grounds defined in Article 7 of the DPD or in Article 6 of the GDPR. In the case of the employment relationship, the consent as a legal ground can be problematic, as there is a hierarchal relationship between the parties, which can question the voluntary nature of the consent.[57] The legal ground that might apply in most cases is the legitimate interest of the controller. It means that the employer can process employees' personal data when the processing is necessary for the enforcement of his/her economic interests, except if the employees' rights override these interests.[58] So basically the employer's legitimate interests must be balanced with the employee's right to data protection.

The most important *principles of processing* which have relevance to our subject are that the data collected cannot be excessive and it shall be

---

[56] 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. *Official Journal of the European Union.* (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=EN [Accessed 4 May 2017], Article 6.1.(b); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Article 5.1.(b).

[57] Article 29 Data Protection Working Party (2001) *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*, 5062/01/EN/Final WP 48, 13 September, p. 23.

[58] 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. *Official Journal of the European Union.* (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=EN [Accessed 4 May 2017], Article 7.(f); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Article 6.1.(f).

adequate, relevant,[59] accurate and, when necessary, kept up to date.[60] These requirements are not satisfied in the case of SNS monitoring. First, the requirements of relevancy and non-excessiveness aim to ensure that as little data are collected as possible.[61] So the employer is entitled to process personal data that is directly related to the employment relationship. On SNSs a part of the personal information available does not have a (direct) connection to employment and is purely private, as mostly "private" SNSs (e.g. Facebook, Instagram, Twitter) are destined for private use, unlike the "professional" SNSs (e.g. LinkedIn). Typically, this information would not have been available (or only with great effort) to the employer in the pre-Internet age. The problem is that this "legally consultable" data and data which the employer cannot process legitimately (e.g. information related to protected characteristics) are inseparable on the profile of the user. Second, the principle of accuracy can be very important regarding identification, in order to avoid situations where the (prospective) employee is mistakenly associated with the SNS activity of someone else – especially if the employee has a very common name and/or there is no other publicly available personal data which can help to correctly identify him/her.[62] Completeness requires that the data

[59] 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. *Official Journal of the European Union.* (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=EN [Accessed 4 May 2017], Article 6.1.(c); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Article 5.1.(c).

[60] 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. *Official Journal of the European Union.* (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=EN [Accessed 4 May 2017], Article 6.1.(d); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Article 5.1.(d).

[61] Kajtár, E. and Mestre, B. (2016) Social Networks and Employees' Right to Privacy in the Pre-employment Stage: Some Comparative Remarks and Interrogations. *Hungarian Labour Law E-journal*, (1), p. 33.

[62] Tenenbaum, J. M. (2012) *Posting Yourself Out of a Posting: Using Social Networks to Screen Job Applicants in America and Germany.*[pre-print]. Available from: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2062462_code1805294.pdf?abstractid=2020477&mirid=1 [Accessed 14 July 2016], p. 13.

processed should give a true picture of the individual.[63] Assessing information obtained from these sites might be misleading, as very often the information originally posted was intended for a different audience (e.g. inside jokes among friends), so it might be taken out of context, thereby giving a false impression of the user. The employee might not have been the author of the given content – a profile can be hacked by a third party,[64] or even friends can post, as a prank, in the name of the employee if the employee leaves his/her device unattended. Third, regarding the up-to-datedness, we must see that the Internet does not forget – it is also true in the case of SNSs. A decision should not be based on out-dated information, but on SNSs information from the past years of the individual is often available. This means that users cannot escape from their past mistakes and, for example, a funny photo taken in high school years ago can have an impact on the future carrier options, even if it is not relevant anymore.[65] In my opinion, for these reasons, information obtained from SNSs cannot be considered reliable. Although traditionally the vulnerability of the employee is the case, nowadays we also have to count with the *reversed vulnerability* of the employer. Employees can do a lot of damage to the employer during the use of the Internet and SNSs.[66] Because of the open nature of these sites, the possible audience of a negative or false comment on the employer can be quickly available to millions of people, causing serious damage to the employer's reputation. See, for example, the prank made by two employees of Domino's Pizza, which could seriously compromise the company's reputation in a few days.[67] The unforgiving nature of the Internet can cause issues for the employer, too, as these contents can remain available even after they are not relevant any more.

---

[63] Péterfalvi, A. (ed.) (2012) *Adatvédelem és információszabadság a mindennapokban.* Budapest: HVG-ORAC, p. 83.

[64] See the scenario described in Sanders, S. D. (2012) Privacy is Dead: The Birth of Social Media Background Checks. *Southern University Law Review*, 39 (2), p. 243.

[65] On the importance of forgetting see Mayer-Schönberger, V. (2011) *Delete – The Virtue of Forgetting in the Digital Age.* Princeton and Oxford: Princeton University Press.

[66] Balogh, Zs. Gy., Polyák, G., Rátai, B. and Szőke, G. L. (2012) Munkahelyi adatvédelem a gyakorlatban. *Infokommunikáció és Jog*, 9 (3), pp. 96–97.

[67] Clifford, S. (2009) *Video Prank at Domino's Taints Brand.* [online] The New York Times. Available from: http://www.nytimes.com/2009/04/16/business/media/16dominos.html [Accessed 10 November 2016].

## 5. POSSIBLE SOLUTIONS

Regarding the possible solutions, it should be emphasized that the DPD and the GDPR are applicable to employee monitoring, the question is how these dispositions should be applied to the case of SNSs? The solution is twofold; it requires efforts both from the employer and the employee.

### 5.1 EMPLOYERS

First, it would be unrealistic to expect employers not to use this cheap, invisible and easy tool of obtaining information at all,[68] but it would be welcomed if the employer could realize that it is also in his/her own interests to comply with the data protection regulation for two reasons. On the one hand, in the case of non-compliance with the GDPR, employers can face administrative fines (in which field the GDPR became more severe)[69], and on the other hand, by respecting the employees' data subject rights and other safeguards, they can eliminate the risks associated with unreliable data. In the next section I will examine how the principles and the rights presented in the previous part of the paper can be complied with.

First of all, internal SNS policies might be adequate instruments to comply with the principle of transparency and the obligation of prior information. The Information Commissioner's Office in the UK issued a document in which, *inter alia*, the importance of policies and impact assessments was emphasized. These policies could serve the purpose of informing (prospective) employees on how their data would be processed. Depending on the given phase of the employment relationship, the content of this document can differ (see below), but it can be stated that the employees should be informed – in plain language, if relevant, illustrated with examples – regarding what data will be processed, by whom, for what reason, what their rights as data subjects are, how they can exercise them, etc. Employers should also conduct *impact assessments* –

---

[68] Kajtár, E. (2015) Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship. *Acta Juridica Hungarica*, 56 (4), p. 278.

[69] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Article 83.

which instrument also appears in the GDPR[70] – to decide whether and how to conduct the monitoring. This assessment should include identifying the purposes of the monitoring, weighing the possible adverse effects, taking into consideration alternatives (e.g. traditional job interviews, period of probation, etc.), considering how the employer will comply with the obligations arising from the monitoring (e.g. the data protection obligations) and considering whether the monitoring is truly justified. A universal model cannot be established, as the monitoring also depends on the given particularities of the employer.[71] Training the employees on SNS use might also be an option.[72]

In my opinion, the use of data obtained from SNS monitoring should not be a general method because of the risks and challenges presented in Part 4. The employer's legitimate interests do not automatically outweigh the employee's right to data protection. As we could see, interests and rights shall be balanced, the processing of personal data must be truly necessary and appropriate guarantees/safeguards should be ensured. Conducting an impact assessment can also help to determine whether the monitoring is truly necessary. Laying down the rules of processing can facilitate compliance with the data protection regulation by making the processing organized/planned and transparent. I have mentioned that it is crucial to inform the current and the prospective employees that such a monitoring would occur, and to provide them with the possibility to exercise their rights as data subjects. Although it is often the employee who decides to share his/her personal data on SNSs (maybe without using the privacy settings), it does not mean that he/she has consented to the free processing of that data. The Hungarian National Data Protection Authority stated in a case regarding hiring – but it can also be applied to the cases of other decision making processes – that it would be unrealistic to expect employers not to consult the publicly available data on Facebook, but if they

---

[70] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 4 May 2017], Article 35.

[71] Information Commissioner's Office (2011) *The Employment Practices Code.* Available from: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf [Accessed 1 February 2017], pp. 61–63.

[72] Proskauer Rose LLP. (2014) *Social Media in the Workplace. Around the World 3.0.* 2013/14 survey. Available from: http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf [Accessed 2 February 2017], p. 23.

use that data during the decision making, the data protection requirements shall apply (especially the requirement of prior information and the data subject's rights).[73] By ensuring these rights, the misinterpretation of the data could also be avoided and the use of SNS data could truly contribute to the promotion of the employer's interests.

Beyond the above presented general statements, in the *phase of hiring*, SNS background checks should only be conducted when they are necessary, for example, when the nature of the given job or the type of employer justifies it (e.g. it is more probable that background checks can be justified if the position comes with high responsibility). These checks should be conducted in a uniform manner and in the late stage of the selection process.[74] The employer shall inform employees that a SNS background check will be conducted during the selection process, state precisely which sites will be checked and what is the lawful information that the employer aims to obtain. The employer can only use data which is publicly available, he/she should not ask for the candidate's password or log into his/her account with other methods or friend a candidate.[75] In order to solve the problem of the inseparability of private and work related information, it might be a solution if a third party – who will not participate in the decision making – conducts the background check and transmits only the work related information to the decision makers.[76]

Concerning the SNS use *during working hours* – a distinction shall be made between whether the employee uses the employer's or his/her own device. Regarding the employer's equipment – by analogy with the already regulated the Internet and e-mail monitoring at the workplace – the employer has the right to decide whether he/she allows the use of SNSs. The Article 29 Data Protection Working Party provides more detail in its *Working document on the surveillance of electronic communications in the workplace* regarding the Internet and e-mail monitoring

[73] Hungarian National Authority for Data Protection and Freedom of Information (2016), NAIH/2016/4386/2/V, August, pp. 3–4.

[74] Information Commissioner's Office (2011) *The Employment Practices Code.* Available from: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf [Accessed 1 February 2017], p. 23.

[75] Mikkelson, K. (2010) Cybervetting and Monitoring Employees' Online Activities: Assessing the Legal Risks for Employers. *The Public Lawyer*, 18 (2), p. 6.

[76] Peebles, K. A. (2012) Negligent Hiring and the Information Age: How State Legislatures Can Save Employers from Inevitable Liability. *William and Mary Law Review*, 53 (4), pp. 1428-1429.; Sprague, R. (2011) Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. *University of Louisville Law Review*, 50 (1), p. 32.

at the workplace, which dispositions, in my opinion, should adequately be applied to the case of SNSs. In this document they emphasize that monitoring whether the employee complies with this restriction shall respect the data protection regulation, and the emphasis should be laid on prevention rather than on detection. For example, it is possible to ban these sites or to use warning windows which alert the employee, or check the time spent on these sites. The content itself should be accessed only in very exceptional cases.[77] Regarding the use of SNSs from the employees' own device is a different case. As a main rule, the employer can prohibit the use of these sites as the employee's obligation is to perform work and not to surf on these sites. However, in this case the monitoring of the device can be quite problematic.[78] In my opinion, the restriction should not concern the case of periods of rest, when the employee can use SNSs on his/her own device.

With regard to activities on SNSs *after working hours*, taking into account how severely one post can harm the employer's reputation and economic interests, the employer is entitled to restrict the employee's conduct on SNSs and has the right to control whether the employee complies. Again, the conditions for this should be laid down in an SNS policy, by taking into consideration the particularities of the workplace and giving clear examples to employees of what conduct is admissible and what is not. The restriction and monitoring cannot be limitless, the employer is obliged to respect the data protection requirements and other rights (e.g. the right to freedom of expression) during establishing the limitations and the way how to monitor compliance. The employer should educate or inform the employees regarding how they can lawfully formulate their opinion and what is not permissible, by providing clear and concrete examples.[79]

## 5.2 EMPLOYEES

Although the employees are entitled to legal protection, they can also make further steps in order to knowingly monitor their digital representations

[77] See more in Article 29 Data Protection Working Party (2002) *Working document on the surveillance of electronic communications in the workplace*, 5401/01/EN/Final WP 55, 29 May, p. 15, 24.

[78] Proskauer Rose LLP. (2014) *Social Media in the Workplace. Around the World 3.0.* 2013/14 survey. Available from: http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf [Accessed 2 February 2017], pp. 7–8.

[79] Proskauer Rose LLP. (2014) *Social Media in the Workplace. Around the World 3.0.* 2013/14 survey. Available from: http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf [Accessed 2 February 2017], p. 23.

and to actively practice their right to informational self-determination. First, they should use the privacy settings in order to control which audiences can have access to the content on their profiles.[80] For example, Facebook gives users the possibility to use differentiated privacy settings – in theory it is possible that every friend of the user has access to a different content on the profile. By effectively using the privacy settings, it would be possible to shape the online identity into an "employer friendly" version, where the employer (or users with whom the employee is not friends) can only have access to one part of the information. Second, the user should also control his/her digital identity by monitoring what information is available regarding him/her on the Internet – for example, typing his/her name into a search engine or monitoring whether third persons have posted information relating to him/her.[81] If he/she is aware of the content which the employer might have access to, he/she can make the necessary steps to remove that content.[82]

Third – not forgetting about the open nature of SNSs – choosing the appropriate form of communication is absolutely crucial. Before sharing something, the employee should think over what the right form for the given content is: would he/she want to share – for example, holiday pictures – in an album accessible to all Facebook users, or "only" to all of his/her friends, or in a private group destined for communication with the closest friends, or in a private message? They should also consider what to post, as they might be confronted with that information in a different situation – for example, the employer might access those holiday pictures during the recruitment process.[83] There exists a so-called Grandmother rule, which can help users to post appropriate material to SNSs, as according to this rule, users should only share information on SNSs that they would feel comfortable to share with their grandmother.[84]

---

[80] CNIL (2011) *Maîtriser les informations publiées sur les réseaux sociaux.* [online] 10 January 2011. Available from: https://www.cnil.fr/fr/maitriser-les-informations-publiees-sur-les-reseaux-sociaux [Accessed 26 February 2017].

[81] CNIL (2011), *L'e-réputation en questions.* [online] 24 August 2011. Available from: https://www.cnil.fr/fr/le-reputation-en-questions-0 [Accessed 24 January 2017].

[82] Byrnside, I. (2008) Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants. *Vanderbilt Journal of Entertainment and Technology Law*, 10 (2), p. 474.

[83] 30th International Conference of Data Protection and Privacy Commissioners (2008), *Resolution on Privacy Protection in Social Network Services.* Strasbourg, 17 October 2008, p. 2.

[84] Byrnside, I. (2008) Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants. *Vanderbilt Journal of Entertainment and Technology Law*, 10 (2), p. 474.

Last, I have to mention the content itself. Although, as we could see, employees are entitled to the right to data protection during SNS use, it must be emphasized that it does not mean that they are free to post anything, they still have to respect certain rules. Naturally, the employees are obliged to respect, e.g. the reputation and trade secrets of the employer, so they have to keep in mind that they are not completely free to post anything they want. Acting with rationality and with prudence is crucial;[85] as the French professor, *Ray* noted, an individual in the 21st century must also dispose a digital IQ.[86] Therefore employees should ask themselves the question "to post or not to post" and think twice before hitting the post button.

## 6. CONCLUSION

The paper discussed the question of SNS use in the employment context with regard to the right to personal data protection. The aim of the research was to examine what special data protection questions or challenges arise during the different phases of the employment relationship, what factors and how should be considered during the balancing of the employer's legitimate interests and the employee's right to data protection.

Answering the question where the balance should be struck between the employer's interests and the employee's rights: in the phase of hiring the prospective employee's rights should prevail. The question of SNS monitoring during working hours is relatively well regulated by analogy with computer/the Internet monitoring – with the employer entitled to determine the rules of SNS use. With respect to the activity conducted beyond the workplace – in the light of the employee's obligations and the severity of the possible damage that can be done to the employer – the balance should be tipped in favour of the employer's legitimate interests.

In my opinion, one of the greatest challenges regarding the subject is the invisibility of SNS monitoring. As the employer might (and often will) check the employee's profile without even notifying him/her, the guarantees set out in the regulations may not be enforced and important data protection rights might be impaired. Regarding the (prospective)

[85] Nivelles, V. (2014) Les entreprises à l'épreuve des réseaux sociaux. *Jurisprudence Sociale Lamy*, (377–378, 23 December), p. 13.

[86] Ray, J.-E. (2011) Facebook, le salarié et l'employeur. *Droit Social*, (2), p. 133.

employee, we could see that this might cause negative consequences to him/her. At the same time, this invisibility generates the biggest controversy in the subject, as it is very noble to define all these data protection rights that the individual is entitled to, but let us be honest: why the employer would want to trouble himself/herself with respecting these regulations when he/she can – "in secret" – gain access to a vast amount of useful information easily and freely? We could see that during the inspection of SNSs not only the individual's rights might be impaired, but not respecting the regulation might also lead to the processing of unreliable, inaccurate, out-of-date data, which is also contrary to the interest of the employer. Employers should realize that they are also interested in the lawful and fair processing of data, and after this "general acknowledgement", both the employer and the employee can and should make further efforts – as I presented in Part 5.

This is a very complex subject, which can be examined from different angles, and I chose to present the arising challenges linked to the different phases of the employment relationship. However, numerous unanswered questions still exist: these can and should serve as a basis for future research and be elaborated in detail in time. Due to space limitations I had to draw the limits here, but even the data protection issues of each phase could constitute a separate paper. Also, matters not discussed in this paper should be analysed in the future, for example, the "soft" impacts of SNS monitoring (e.g. erosion of trust) or questions related to the practice of collective labour law rights.

## LIST OF REFERENCES

[1] 30th International Conference of Data Protection and Privacy Commissioners (2008), *Resolution on Privacy Protection in Social Network Services.* Strasbourg, 17 October 2008.

[2] Abril, P. S., Levin, A. and Del Riego, A. (2012) Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. *American Business Law Journal*, 49 (1), pp. 63–124.

[3] Anderson, D. R. (2011) Restricting Social Graces: The Implications of Social Media for Restrictive Covenants in Employment Contracts. *Ohio State Law Journal*, 72 (4), pp. 881–908.

[4] Article 29 Data Protection Working Party (2001) *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*, 5062/01/EN/Final WP 48, 13 September.

[5] Article 29 Data Protection Working Party (2002) *Working document on the surveillance of electronic communications in the workplace*, 5401/01/EN/Final WP 55, 29 May.

[6] Balogh, Zs. Gy., Polyák, G., Rátai, B. and Szőke, G. L. (2012) Munkahelyi adatvédelem a gyakorlatban. *Infokommunikáció és Jog*, 9 (3), pp. 95–104.

[7] *Barbera v. Sté Alten Sir.* (2010) Application no. 10/00853. Conseil de Prud'hommes de Boulogne-Billancourt, 19 November.

[8] *Bărbulescu v. Romania.* (2016) Application no. 61496/08. European Court of Human Rights, 12 January.

[9] Boyd, D. M. and Ellison, N. B. (2008) Social Network Sites: Definition, History and Scholarship. *Journal of Computer Mediated Communication*, 13 (1), pp. 210–230.

[10] Byrnside, I. (2008) Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants. *Vanderbilt Journal of Entertainment and Technology Law*, 10 (2), pp. 445–477.

[11] Clark, L. A. and Roberts, S. J. (2010) Employer's Use of Social Networking Sites. A Socially Irresponsible Practice. *Journal of Business Ethics,* 95 (4), pp. 507–525.

[12] Clifford, S. (2009) *Video Prank at Domino's Taints Brand.* [online] The New York Times. Available from: http://www.nytimes.com/2009/04/16/business/media/16dominos.html [Accessed 10 November 2016].

[13] CNIL (2011) *Maîtriser les informations publiées sur les réseaux sociaux.* [online] 10 January 2011. Available from: https://www.cnil.fr/fr/maitriser-les-informations-publiees-sur-les-reseaux-sociaux [Accessed 26 February 2017].

[14] CNIL (2011) *L'e-réputation en questions.* [online] 24 August 2011. Available from: https://www.cnil.fr/fr/le-reputation-en-questions-0 [Accessed 24 January 2017].

[15] Council of Europe (2012) *Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services.* CM/Rec(2012)4, 4 April 2012.

[16] Cseh, G. (2013) A közösségi portálok árnyoldalai. *Infokommunikáció és jog*, 10 (2), pp. 90–95.

[17] 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. *Official Journal of the European Union.* (1995: L 281) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF /?uri=OJ:L:1995: 281:FULL &from=EN [Accessed 4 May 2017].

[18] *Distribution of active Facebook users worldwide as of 4th quarter 2014, by age.* [online] Statista. Available from: https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/ [Accessed 17 January 2017].

[19] Engler, P. and Tanoury, P. (2007) Employers Use of Facebook in Recruiting. In: Dan McIntosh, Ralph Drabic, Kristina Huber, Igor Vinogradov and Michael Bassick (eds.), *The Ethical Imperative in the Context of Evolving Technologies.* University of Colorado Leeds School of Business. Available from: http://www.ethicapublishing.com/ethical imperative.pdf [Accessed 13 July 2016], pp. 61–74.

[20] Falque-Pierrotin, I. (2012) La Constitution et l'Internet. *Les Nouveaux Cahiers du Conseil Constitutionnel*, (36, June), pp 31–44.

[21] Fried, C. (1968) Privacy. *The Yale Law Journal*, 77 (3), pp. 475–493.

[22] Gellert, R. and Gutwirth, S. (2013) The legal construction of privacy and data protection. *Computer Law and Security Review*, 29 (5), pp. 522–530.

[23] González Fuster, G. and Gutwirth, S. (2008) Privacy 2.0? *Revue du droit des Technologies de l'Information,* (32), p. 351–361.

[24] Grimmelmann, J. (2009) Saving Facebook. *Iowa Law Review*, 94 (4), pp. 1137–1206.

[25] Hajdú, J. (2005) *A munkavállalók személyiségi jogainak védelme.* Szeged: Pólay Elemér Alapítvány.

[26] Herbert, W. A. (2011) Workplace Consequences of Electronic Exhibition and Voyeurism. *IEEE Technology and Society Magazine*, 30 (3), pp. 25–33.

[27] Hornung, G. and Schnabel, C. (2009) Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law and Security Review*, 25 (1), pp. 84–88.

[28] Hungarian National Authority for Data Protection and Freedom of Information (2016) case NAIH/2016/4386/2/V., August.

[29] Information Commissioner's Office (2011) *The Employment Practices Code.* Available from: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_ practices_code.pdf [Accessed 1 February 2017].

[30] International Working Group on Data Protection in Telecommunications (2008) *Report and Guidance on Privacy in Social Network Services "Rome Memorandum"*, 3-4 March. Rome, Italy, 675.36.5., Available from: http://www.datenschutz-berlin.de/attachments/ 461/WP_ social_network_services.pdf [Accessed 26 May 2017].

[31] Jóri, A. (2009) *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése.* Ph.D. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola.

[32] Kajtár, E. (2015) Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship. *Acta Juridica Hungarica*, 56 (4), pp. 268–280.

[33] Kajtár, E. and Mestre, B. (2016) Social Networks and Employees' Right to Privacy in the Pre-employment Stage: Some Comparative Remarks and Interrogations. *Hungarian Labour Law E-journal*, (1), pp. 22–39.

[34] Kokott, J. and Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3 (4), pp. 222–228.

[35] *List of social networking websites.* [online] Wikipedia. Available from: https://en.wikipedia.org/wiki/List_of_social_networking_websites [Accessed 09 November 2016].

[36] Lukács, A. (2016) What is Privacy? The History and Definition of Privacy. In: Keresztes, Gábor. (ed.): *Tavaszi Szél 2016 Tanulmánykötet I*, Budapest, 15-17 April. Budapest: Doktoranduszok Országos Szövetsége, pp. 256–265. Available from: http://www.dosz.hu/dokumentumfile/TSZ_I_kotet_161114_574o.pdf [Accessed 4 May 2017].

[37] Manant, M., Pajak, S. and Soulié, N. (2014) *Online social networks and hiring: a field experiment on the French labor market.* [in press] Munich Personal RePEc Archive. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2458468 [Accessed 2 February 2017].

[38] Mayer-Schönberger, V. (2011) *Delete – The Virtue of Forgetting in the Digital Age.* Princeton and Oxford: Princeton University Press.

[39] Mikkelson, K. (2010) Cybervetting and Monitoring Employees' Online Activities: Assessing the Legal Risks for Employers. *The Public Lawyer*, 18 (2), pp. 3–7.

[40] Miller, S. and Weckert, J. (2000) Privacy, the Workplace and the Internet. *Journal of Business Ethics*, 28 (3), pp. 255–265.

[41] Nivelles, V. (2014) Les entreprises à l'épreuve des réseaux sociaux. *Jurisprudence Sociale Lamy*, (377–378, 23 December 2014), pp. 9–13.

[42] *Number of monthly active Facebook users worldwide as of 3rd quarter 2016 (in millions).* [online] Statista. Available from: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [Accessed 17 January 2017].

[43] Oppenheim, R. (2013) *High School Teacher Files an Appeal in Case of Social Media Related Resignation.* [online] California Business Litigation Blog. Available from: https://www.californiabusinesslitigation.com/2013/05/high_school_teacher_files_an_a.html [Accessed 4 May 2017].

[44] Park, S. (2014) Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy. *American Business Law Journal*, 51 (4), pp. 779–841.

[45] Peebles, K. A. (2012) Negligent Hiring and the Information Age: How State Legislatures Can Save Employers from Inevitable Liability. *William and Mary Law Review*, 53 (4), pp. 1397–1433.

[46] Persson, A. J. and Hansson, S. O. (2003) Privacy at Work – Ethical Criteria. *Journal of Business Ethics*, 42 (1), pp. 59–70.

[47] Péterfalvi, A. (ed.) (2012) *Adatvédelem és információszabadság a mindennapokban.* Budapest: HVG-ORAC.

[48] *Pietrylo v. Hillstone Restaurant Group.* (2009) Civil Case No. 06–5754 (FSH). United States District Court, D. New Jersey, 25 September.

[49] Posner, R. A. (1978) The Right of Privacy. *Georgia Law Review*, 12 (3), pp. 393–422.

[50] Proskauer Rose LLP. (2014) *Social Media in the Workplace. Around the World 3.0.* 2013/14 survey. Available from: http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf [Accessed 2 February 2017].

[51] Purtova, N. (2010) Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights. *Netherlands Quarterly of Human Rights,* 28 (2), pp. 179–198.

[52] Ray, J.-E. (2011) Facebook, le salarié et l'employeur. *Droit Social,* (2), pp. 128–140.

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union.* (2016: L 119) 4 May. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119: FULL&from=EN [Accessed 4 May 2017].

[54] Sanders, S. D. (2012) Privacy is Dead: The Birth of Social Media Background Checks. *Southern University Law Review*, 39 (2), pp. 243–264.

[55] Smith, W. P. and Kidder, D. L. (2010) You've been tagged! (Then again, maybe not): Employers and Facebook. *Business Horizons*, 53 (5), pp. 491–499.

[56] Sprague, R. (2007) From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace. *The John Marshall Journal of Information Technology & Privacy Law*, 25 (1), pp. 1–36.

[57] Sprague, R. (2011) Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. *University of Louisville Law Review*, 50 (1), pp. 1–34.

[58] Szabó, M. D. (2005) Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. *Információs Társadalom*, 5 (2), pp. 44–54.

[59] Tenenbaum, J. M. (2012) *Posting Yourself Out of a Posting: Using Social Networks to Screen Job Applicants in America and Germany.* [pre-print]. Available from: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2062462_code1805294.pdf?abstractid=2020477&mirid=1 [Accessed 14 July 2016].

[60] Van Eecke, P. and Truyens, M. (2010) Privacy and social networks. *Computer Law and Security Review*, 26 (5), pp. 535–546.

[61] Warren, M. and Pedowitz, A. (2011) Social Media, Trade Secrets, Duties of Loyalty, Restrictive Covenants and Yes, the Sky is Falling. *Hofstra Labor and Employment Law Journal*, 29 (1), pp. 99–113.

[62] Warren, S. D. and Brandeis, L. D. (1890) The Right to Privacy. *Harvard Law Review*, 4 (5), pp. 193–220.

[63] Westin, A. F. (2003) Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59 (2), pp. 431–453.