Оригинални научни рад 331.105.24:342.738(439)

*Adrienn I. Lukács, Ph.D. Student*
*University of Szeged*
*Faculty of Law and Political Sciences and*
*University Paris 1 Pantheon-Sorbonne*
*Sorbonne Law School*
*lkcs.adrienn@gmail.com*

# The Monitoring of Employee's Use of Social Network Sites at the Workplace with Special Regard to the Data Protection Law of the European Union and Hungary

***Abstract***: *Facebook and other social media and social network sites have gained increasing importance in our everyday lives: the workplace does not constitute an exception. The use of social network sites during working hours can seriously compromise the employer's legitimate interest. The paper explores whether and how the employer is entitled to monitor employee's use of social media at the workplace – while still respecting their right to data protection. As the "traditional" monitoring of Internet use is already regulated both in the European Union and in Hungary, the main question is how these rules can be adequately applied to the case of monitoring the use of social network sites? To answer this question, the paper first presents the already existing data protection framework of Internet monitoring in the European Union and in Hungary and the changes brought by the EU's data protection reform, then discusses the new challenges relating to social network sites.*

***Keywords***: *social network sites, employee monitoring, data protection law.*

## 1. Introduction

Facebook and other social media and social network sites have gained increasing importance in our everyday lives. The most popular platforms have several millions of users,[1] – and employees use these sites just like any individual. The use of social network sites can cause several privacy and data protection law

[1] In August 2017, Facebook was the biggest "country" in the world with its 2 billion users, while Youtube had 1.5 billion, Twitter 328 million, LinkedIn 106 million *active* users worldwide, just to mention a few examples. Source: Most famous social network sites worldwide as of August

challenges when it comes to the employment context: from cyber-vetting candidates' social network profiles in the hiring phase to dismissing an employee because of a questionable Facebook post. If an employee spends his/her working time surfing on Facebook, it can seriously compromise the interests of the employer, who lawfully expects the employee to work during working hours. The paper discusses the phenomenon of the use of social network sites in the workplace – during working hours – and its regulation and monitoring by the employer.

The aim of the paper is to examine whether the personal use of social media at the workplace can be successfully addressed by the already existing regulation covering the regulation and monitoring of employees' personal use of the Internet or whether adjustments would be needed. The paper will focus on the data protection law of the European Union and of Hungary and will refer to the changes brought by the EU's recent data protection reform. First, the paper will present the already existing data protection framework governing monitoring of Internet use and the relevant legal documents in the field. Then, it will discuss whether this already existing framework could effectively regulate the use and monitoring of social network sites and addresses the new challenges brought by the technological development.

## 2. Regulation and monitoring of the personal use of Internet at the workplace

The traditional ways of employee monitoring are already regulated both in the European Union and in Hungary. Among these types of monitoring, the rules of CCTV monitoring, telephone, computer and Internet use or GPS monitoring, etc. are already elaborated.[2] The monitoring of the monitoring of the use of online social networks has a very close connection to the regulation and to the monitoring of personal Internet use, as these sites are Internet based platforms. However, as it will be discussed later, technological developments and the societal-cultural changes brought by them cause new types of challenges.

When it comes to employee monitoring, the balancing of the employee's rights and the employer's legitimate interests shall be made and the basic labour law principles can help to trace the line where to strike the balance between the two sides. The subjects of the employment relationship have various rights and obligations, and the interests of the employer to restrict the employees' right to

2017, ranked by number of active users (in millions). Available at: *https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/* Accessed: 22 September 2017.

[2] Regarding the EU regulation see more in: Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, 17/EN WP 249, 8 June 2017 and in the documents referred to in the Opinion. On the Hungarian regulation see more in Mariann Arany-Tóth, *Személyes adatok kezelése a munkaviszonyban*, Wolters Kluwer, Budapest 2016, 74-172

personality underlie the reinforcement of these rights and obligations.[3] An employment relationship necessarily comes with the limitation of certain rights and the autonomy of the employees.[4] It follows from the main labour law principles that employers have the contractually based right to determine the work and to control whether the employees perform their contractual obligations.[5] Obviously, the employees have the obligation to work and to follow the instructions of the employer. There is an interaction between these rights and obligations: what is a right on one side will be on obligation on the other side.[6]

The employer has the right to monitor whether the employee complies with his/her instructions. This monitoring necessarily comes with the processing of personal data and falls under the scope of the data protection legislation, meaning that the data protection requirements aiming to ensure the employees' right to personal data protection shall be respected during such monitoring. The monitoring of employees' Internet use is already regulated both at the level of the European Union and at Member State level, so Hungary, too, has already addressed this question and elaborated the detailed rules.[7]

## 2.1. The European Union's data protection regulation

At the time of writing this paper, the two most important legal documents establishing the general legal framework for the data protection regulation were the Data Protection Directive[8] (hereinafter referred to as DPD) (not in force anymore, but still applicable until 2018 May) and the General Data Protection Regulation (hereinafter referred to as: GDPR)[9] (in force, but applicable only from 2018 May). These two documents lay down the most important rules for data processing.

[3] József Hajdú, *A munkavállalók személyiségi jogainak védelme,* Pólay Elemér Alapítvány, Szeged 2005, 20

[4] ed. Kolos Kardkovács, *Az új Munka Törvénykönyvének magyarázata,* HVG-ORAC Lap- és Könyvkiadó, Budapest 2012, 40

[5] Frank Hendrickx, *Protection of workers' personal data in the European Union, Two studies*, EC, 2002, 97

[6] ed. Tamás Gyulavári, *Munkajog*, ELTE Eötvös Kiadó, Budapest 2013, 244

[7] Other international organisations have also addressed the question of employees' right to data protection, such as the International Labour Organization (*Protection of workers' personal data,* An ILO code of practice, 1997) or the Council of Europe (*Working document on the Protection of Personal Data used for Employment Purposes,* 1989; *Recommendation of the Committee of Ministers to Member States on the processing of personal data in the context of employment,* 2015).

[8] 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 1995.

[9] 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

The Article 29 Data Protection Working Party – an independent advisory board set up by Article 29 of the DPD – has addressed the question of employee monitoring in several of its documents. Among them, Opinion 8/2001 on the processing of personal data in the employment context, Working document on the surveillance of electronic communications in the workplace (2002) and Opinion 2/2017 on data processing at work shall be mentioned, which provide guidance regarding the regulation and monitoring of employees' Internet use.

In its *Opinion 8/2001 on the processing of personal data in the employment context*, the Working Party emphasizes the interconnectedness of data protection and labour law and the importance of the "general" data protection requirements.[10] Regarding the legal ground of the processing, it points out the highly questionable nature of the consent.[11] It also addresses in general the question of surveillance and monitoring, but does not address separately each type of monitoring.[12] The *Working document on the surveillance of electronic communications in the workplace* (hereinafter referred to as: Working Document) complements Opinion 8/2001.[13] This document also confirms that despite being in the workplace, the employees do not leave their rights at home, but these rights have to be balanced against the employer's legitimate interests.[14] Contrary to Opinion 8/2001, the Working Document specifically addresses the question of electronic monitoring of employees: the surveillance and monitoring of e-mail and Internet use. Regarding the monitoring of Internet access, the starting point is that the employer is free to decide whether he/she allows workers to use the Internet for personal purposes, and if so, to what extent. Though the employer is entitled to monitor whether employees comply with the regulation, certain restrictions shall be considered. The Working Party expressed its view that instead of monitoring, the emphasis should be placed on preventing the misuse of computers.[15] According to the basic principles, the least intrusion possible must be made, so it is advisable that the employer avoid automatic and constant monitoring.[16]

[10] 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, 13 September 2001, 3-4

[11] Ibid., 3

[12] Ibid., 24-25

[13] Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace,* 5401/01/EN/Final WP 55, 29 May 2002, 3

[14] Ibid., 4

[15] Ibid., 24 This could be achieved by using programs that remind the employee of the misuse (e.g. warning windows, which pop up and alert the employee). Source: Ibid., 5. According to the European Data Protection Supervisor – the EU's independent data protection authority –, it is more useful to watch the indicators (for example, volume of data downloaded) than the visited websites themselves and to take further steps only when there is a strong suspicion of misuse. Source: Giovanni Buttarelli, *Do you have a private life at your workplace? Privacy in the workplace in EC institutions and bodies*, 31st International Conference of Data Protection and Privacy, Madrid, November 4-6, 2009, 2

[16] Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace,* 5401/01/EN/Final WP 55, 29 May 2002, 17

The Working Party's most recent document in this field is *Opinion 2/2017 on data processing at work*. This Opinion takes into account the technological changes and emphasizes the significance of the protection of employees' right to privacy and to data protection in today's society.[17] Opinion 2/2017 mainly concerns the DPD but also takes into account the GDPR. It first highlights the general requirements regarding monitoring, then discusses nine types of data processing in the employment context. One of the nine items is entitled "Processing operations resulting from monitoring ICT usage at the workplace". In this item the Working Party states that the conclusions laid down in the Working Document still remain valid, "[…] there is a need to take into account technological developments that have enabled newer, potentially more intrusive and pervasive ways of monitoring."[18] The Working Party emphasizes the importance of proportionality, transparency (e. g. by means of adopting policies).[19] It follows from the requirement of subsidiarity that monitoring might not even be necessary, as the blocking of certain websites (in our case the blocking of social network sites) can prevent employees from personal use of Internet; emphasis should be put on prevention, rather than detention.[20]

In conclusion, according to the EU regulation, the employer is entitled to decide whether he/she allows employees to use social network sites during working hours at the workplace. He/she is also entitled to monitor whether employees comply with these restrictions. However, the monitoring cannot be limitless or excessive; the data protection requirements – such as necessity, proportionality, etc. – shall be respected.[21]

## 2.2. Hungary's data protection regulation

Hungary is a Member State of the European Union, meaning that it shall comply with the requirements set out by the DPD and the GDPR. Several rules of law declare the protection of the right to privacy and the right to data protection. The Hungarian constitution, the *Fundamental Law* guarantees the protection of

---

[17] Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, 17/EN WP 249, 8 June 2017, 9-10

[18] Ibid., 12

[19] Ibid., 14

[20] Ibid., 15

[21] Though this case relates to the European Court of Human Rights, the Bărbulescu case has a great significance. In this case the employee has violated the employer's instructions and used the work computer for private purposes, which the employer could prove through the monitoring of the employee's computer. Taking into consideration the exact circumstances of the monitoring, the Court found that Article 8 (ensuring the right to privacy) was infringed. See more in: European Court of Human Rights, *Bărbulescu v. Romania.* 5 September 2017, application no. 61496/08

the right to privacy and to data protection.[22] The *Civil Code* guarantees the protection of personality rights and identifies a list of personality rights, specifying the right to privacy and the right to data protection as a personality right.[23] These norms do not contain detailed dispositions regarding employee data protection, the *Labour Code*[24] and the *Privacy Act*[25] provide more detailed dispositions. The question of employee privacy and data protection is addressed in the form of very general dispositions, but the Hungarian National Authority for Data Protection and Freedom of Information's (hereinafter referred to as the Authority) practice gives guidance regarding the field of workplace data protection.

In recent years the Authority has published two important documents regarding workplace monitoring. The first document is the *Recommendation on the basic requirements of electronic monitoring at the workplace* (2013), which cleared possible misunderstandings arising from the new legal environment[26] and laid down the most important requirements regarding employee monitoring, contributing to the establishment of a uniform practice. Contrary to the previous Hungarian practice, the Authority stated – referring to the EU data protection regulation and the Working Party's documents – that employee monitoring can be independent from the employees' consent, as it follows from the very nature of the employment relationship and the employer's right to monitor that no consent is needed for such a monitoring.[27] It does not mean that monitoring can be limitless, a balancing of rights and interests shall be made, which still has to respect certain conditions.[28] In the second part of the document the Authority deals specifically with CCTV monitoring, however, the dispositions laid down in this document shall be adequately applied to the case of Internet monitoring, too.[29]

---

[22] Subsection (1) of Article VI and Subsection (2) of Article VI of the Fundamental Law

[23] Items b and e of Section 2:43 of Act V of 2013 on the Civil Code

[24] Sections 9-11 of the Labour Code in force state the protection of the rights relating to personality and contain dispositions regarding data protection and employee monitoring. Section 9 guarantees the protection of personality rights by declaring that for the employer's and employee's personality rights the dispositions of the Civil Code shall be applied and lays down the conditions for restricting these rights. Section 10 contains dispositions regarding employee statements and disclosure of information. Section 11 regulates employee monitoring, stating that the employee can only be monitored relating to work, limited by his/her right to dignity and his/her private life as it cannot constitute the subject of the monitoring.

[25] Act CXII of 2011 on the Right to Informational Self-Determination and on Freedom of Information

[26] The Fundamental Law and the Privacy Act came into force in 2012, while the Authority started its functioning in 2012, succeeding the Data Protection Commissioner.

[27] Hungarian National Authority for Data Protection and Freedom of Information, *Recommendation on the basic requirements of electronic monitoring at the workplace,* 23 January 2013. Case number: NAIH-4001-6/2012/V., 3

[28] Such as necessity, the employee's dignity and private life, information of employees and the respect of the basic data protection requirements. Source: Idem.

[29] M. Arany-Tóth, 106

The second document is the *Information notice on the basic requirements on data processing at work* (2016) which – similarly to the Working Party's Opinion 2/2017 – first discusses the general data protection requirements in relation to processing in the context of employment and then addresses several scenarios of processing. With respect to Internet monitoring, it points out that information shall be given to employees regarding first, which sites cannot be visited, and second, how the monitoring of compliance will be conducted. It is advisable for the employer to block the access to certain sites. However, the use of such blocking does not mean that he/she cannot monitor compliance, as employees can by-pass such blockings. The importance of the purpose limitation principle and transparency principle is also emphasized.[30]

### 2.3. The European Union's data protection reform

We are now witnessing the data protection reform, which has (will have) a huge impact on the Member States' data protection regulation. The EU legislator has decided to adopt a regulation instead of the previously used directive, unifying national data protection legislations. The GDPR introduces several important changes, here only the ones most relevant to workplace monitoring will be discussed.

In the employment relationship consent is highly questionable as an appropriate *legal ground* of processing. The GDPR even strengthens the condition for a valid consent: in order to ensure the free nature of consent, it should not constitute a valid legal ground of processing when a clear imbalance is present between the controller and the data subject.[31] In consistency with the documents of the Working Party, it is now reinforced that consent should not constitute a valid legal ground for the monitoring of social media use at the workplace.

A *data protection impact assessment* is required prior to processing when a processing is "likely to result in a high risk to the rights and freedoms of natural persons".[32] Employee monitoring will likely fall under the notion of "high risk" processing, placing obligation on controllers to conduct a data protection impact assessment.[33] In order to reinforce the implementation of data protection principles – such as data minimization or purpose limitation – the GDPR introduced the principles of data protection by design and data protection by default. *Data pro-*

---

[30] Monitoring can only cover the processing of necessary data. For example, it is enough for the employer to know which "forbidden" sites the employee has visited, it is not necessary to know what exactly the employee did on these sites. Source: Hungarian National Authority for Data Protection and Freedom of Information, *Information notice on the basic requirements on data processing at work,* 28 October 2016, 30-31

[31] GDPR, Recital 43

[32] GDPR, Article 35, 1

[33] Employee monitoring update, March 2017, Available at: *https://www.taylorwessing.com/globaldatahub/article-employee-monitoring-update.html* Accessed: 27 February 2018

*tection by design* means that already when planning and then when implementing data processing, the controller "shall implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles […] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."[34] The principle of *data protection by default* means that the controller is obliged to ensure that "by default, only personal data which are necessary for each specific purpose of the processing are processed".[35] These principles reinforce that the constant and automatic monitoring of employees' social media use during working hours is not reconcilable with the principles laid down in the GDPR.

Though having a regulation instead of a directive will lead to more uniformity, it does not mean that no differences will exist between Member State regulations. Article 88 of the GDPR contains *special provisions* regarding the processing in the employment context, stating that Member States can provide for more specific rules in order to ensure employees' right to data protection.[36] Such rules should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to, amongst others, monitoring systems at the workplace.[37] This will mean – as there is no unified "EU labour law" – that some differences between Member State regulations might still exist in the future in the field of employment monitoring, giving rise to national specificities.

The reform also introduced more severe consequences for controllers and processors in *the case of non-compliance* with the dispositions in the GDPR. In the most severe cases national data protection authorities can impose administrative fines up to 20 million euros or if it concerns an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year (the higher amount from these two).[38]

---

[34] GDPR, Article 25, 1.

[35] GDPR, Article 25, 2.

[36] GDPR, Article 88, Processing in the context of employment: *"1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship."*

[37] Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work,* 17/EN WP 249, 8 June 2017, 9

[38] GDPR, Article 83, 5.

## 3. Use of social network sites in the workplace and its monitoring

The above mentioned documents regulate the most important rules regarding the monitoring of employees' Internet use. However, the question arises whether the use of social network sites necessitates adjustments compared to these dispositions and what other, new factors shall be taken into account.

### 3.1. The proliferation of social network sites and its effect on employment

Both the Working Party's Opinion 2/2017 and the Authority's Information Notice mention social network sites. However, they do that by referring to their role in the hiring process (pre-employment screening) or the screening of employees' profiles in order to obtain information about them,[39] and they do not specifically address the monitoring of their use at the workplace.[40] Essentially, the already presented regulation is applicable to them: the employer can decide whether he/she allows employees to check social media and social networks at the workplace and can monitor whether employees comply with these restrictions. According to the Hungarian jurist *Janka Németh,* the employer can choose from among three scenarios: banning the use of Internet completely, only banning the personal use of Internet or not placing restrictions on the employees' use of Internet. Then, the scale of monitoring is influenced by which scenario was chosen by the employer.[41]

Prima facie, it seems convenient to completely block the access to social media sites. However, as a myriad of these platforms exists, the employer would probably be able to block only the most widely used ones (e. g. Facebook or Instagram), but not all these sites. Also, in spite of being free to decide whether employees can use social media at the workplace or not, it should be taken into account that in today's information society it might be unrealistic to completely ban its personal use. Today – whether we accept it or not – it has become a reality that individuals, especially younger generations, spend a considerable amount of time on social networks and they would not like to be completely cut off from these sites during working hours.[42] Also, due to the advancement of information

[39] Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work,* 17/EN WP 249, 8 June 2017,11-12; Hungarian National Authority for Data Protection and Freedom of Information, *Information notice on the basic requirements on data processing at work,* 28 October 2016, 18-19

[40] Not only their use itself can raise important questions, but also the content that employees post to these sites, even after the working hours. For lack of space, this paper discusses only the question of social media use at the workplace, at the expense of working hours.

[41] Janka Németh, "Internet és közösségi háló mint munkaeszköz", *Infokommunikáció és jog,* 2013/1, 38-39

[42] According to Social Media Today, an average user spends almost 2 hours (116 minutes) on social media every day, which amount of time is higher among teenagers. Forbes has revealed

communication technologies, the boundaries between work and private life are more and more blurred. As employees can receive a work-related mail during the weekend or can finish a task (from their own computer) at home in the evening, they might also wish to check their social media profiles during working hours, or just see on the newsfeed what happened to their contacts.[43] Today it seems unreasonable to completely cut off employees from social media during working hours. Checking these profiles occasionally for 5-10 minutes would not necessarily harm the employer. However, employees can also abuse their "rights" and can spend a considerable amount of time on these sites. An example can be brought from French case law, where an employee connected to not work-related sites – and among them to social media – more than 10000 times during a period of 18 days, and was dismissed because of these actions.[44]

If the employees do not meet the obligation of performing work, or despite the ban on the use of social networks they connect to these sites, they can face various consequences according to the labour law regulations. In serious cases they can even be dismissed from the workplace. If the employee infringes the regulation regarding the prohibition of personal use, it can serve as the basis for dismissal.[45] However, the circumstances of these cases are important, as the motivation of the termination shall be reasonable. The Supreme Court of Hungary ruled that the motivation of the termination shall not be considered reasonable if a long-term employee is dismissed because he/she arrived late at the workplace once.[46] In my opinion this provision shall adequately be applied to the case of using social network sites. There is a difference between infringing the employer's instructions and checking Facebook one time, for 5 minutes or spending there

that employees spend more and more time on Internet and social media for personal purposes. According to the results of the PAW (Privacy in the workplace) project in 2012, 39 % of the Hungarian employees participating in the survey check social networks at the workplace. Sources: Evan Asano, How Much Time Do People Spend on Social Media? [Infographic], 4 January 2017. Available at: *https://www.socialmediatoday.com/marketing/how-much-time-do-people-spend-social-media-infographic* Accessed: 17 December 2017; Cheryl Conner, Wasting Time At Work: The Epidemic Continues, 23 July 2015. Available at: *https://www.forbes.com/sites/cherylsnappconner/2015/07/31/wasting-time-at-work-the-epidemic-continues/#520a42741d94* Accessed: 17 December 2017, ed. Gergely László Szőke, *Privacy in the workplace. Data protection law and self-regulation in Germany and in Hungary*, HVG-ORAC Lap- és Könyvkiadó, Budapest 2012, 173. Regarding more details of the PAW project's survey, see more in Idem., 174-177

[43] Edit Kajtár, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* Vol. 56, No 4., 2015, 269

[44] Cour de cassation chambre sociale, 26 February 2013, N° 11-27372

[45] Gyula Berke *et al.*, *Kommentár a munka törvénykönyvéhez,* Wolters Kluwer, Budapest 2014, 62. The Hungarian Supreme Court ruled that infringing the employer's restrictions and using another employee's computer for this purpose constituted a serious breach of obligation. (BH2006.64)

[46] T. Gyulavári, 200

hours on a daily basis, and also there is a difference if a newly hired employee does that on his/her first week or an employee who has worked there for years.

Social network sites can also contribute to revealing another kind of activity at the expense of working time: in a number of cases employees on sick leave are caught on social media being a picture of perfect health.[47] In such a scenario, the employee infringes his/her obligation to be at the disposal of the employer and this conduct can even constitute the basis for layoff.[48] However, when using such posts for decision making, attention should be paid to the enforcement of the data quality principles.[49]

Transparency has key importance, as employers have the obligation to inform employees on the details of the monitoring.[50] An increasingly more common way for employers is to regulate these issues in internal social media policies or *social media guidelines*. Drafting such a document can not only ensure compliance with the employer's obligations but, by informing the employees regarding the permitted and not permitted conducts, it can also contribute to the prevention of misuse by clarifying the conducts to be followed by employees. It is crucial for employees to be aware of the rules they have to respect: the employer has to inform them whether the use of social media at the workplace is prohibited; or – in the case of a permissive regulation – what the limits of social media use are (e. g. 20 minutes daily). Also, notice on how and what kind of monitoring takes place shall be provided to employees. In accordance with the previously presented: constant and systematic monitoring is not advisable. Also, instead of monitoring the content of the visited website, a misuse could also be detected by determining the time spent on these sites.

### 3.2. Challenges posed by smartphones

A challenge brought by technological development is that social network sites can not only be used on computers, but also on mobile devices such as smartphones or tablets. These days more and more people have their own smartphones, which they take with themselves everywhere – to the workplace too. It is also very

---

[47] See, for example, the case of a Swiss woman who said she was sick, complaining to have migraine and that she needed to rest in a dark room without using any computer: then her colleagues reported her seen active on Facebook and changing her status, or the case of a French employee who posted when returning from sick leave: "after two weeks and three days of holiday it's going to be very hard…" Sources: Ildikó Rácz, A közösségi média és a munkajog kereszttüzében, 20 August 2017, Available at: *http://arsboni.hu/kozossegi-media-es-munkajog-kereszttuzeben/* Accessed : 27 February 2018 and Cour d'appel d'Amiens, 21 May 2013, n° 12/01638

[48] Linda Horváth, Anikó Gelányi, „Lájkolni vagy nem lájkolni? A közösségi oldalak használatának munkajogi kérdései", *Infokommunikáció és jog*, 2/2011, 61

[49] Hungarian National Authority for Data Protection and Freedom of Information Case number: NAIH/2016/4386/2/V.

[50] GDPR, Article 12

common that individuals have their own mobile Internet subscription, so the blocking of social network sites by the employer is not an option in these cases. Though the employer has the right to regulate and monitor the use of social network sites on *his/her* computer, the scenario is different when the device constitutes the property of the employee.

As one of the employee's main obligations is being at the employer's disposal and performing work, the employer can prohibit the employee from using his/her own device for personal purposes. However, break time might cause a challenge. Hungarian labour law professor, *Attila Kun* pointed out a very unique phenomenon, namely that (even the permitted) use of social media can have an indirect effect on work, by disintegrating employees' attention. The mass of ever changing information on social media might result in the fact that the employee receives more information than he/she can process, causing fatigue and reducing concentration.[51] As concerns the break time and the use of social media, it also has to be taken into consideration that the employer has the obligation to ensure safe working environment, and the employer has to monitor whether workplace safety rules are respected. Therefore, if an employee works with a computer and spends his/her break looking at the screen of his/her smartphone, the workplace safety regulations are infringed, as the employer has to ensure breaks for the employee from staring at a screen.[52]

It is one thing to be able to restrict employees' personal social media use, but can the employer monitor whether employees comply? In cases when the smartphone is the employee's property, the employer is limited in monitoring their use, he/she cannot have access to the content/pages visited on these devices. In these cases the activity of employees checking their Facebook can easily stay invisible. An exception can be when the employee posts something during working hours – despite the ban of social media use – and the time of the post reveals to the employer that the employee has infringed the limitation.

## 4. Conclusion

The proliferation of social media amongst employees has a profound effect on the world of work too, creating new challenges that still need to be addressed. Social media has a huge impact on several phases of the employment relationship, starting from-cyber vetting in the hiring phase to dismissing an employee because of a Facebook comment. Though more and more legal articles address these issues, there is not yet a uniform regulation exhaustively dealing with the question of social media and privacy/data protection at the workplace. From among the areas

[51] Attila Kun, "Közösségi média és munkajog – avagy „online" munkaidőben és azon túl", *Munkaügyi Szemle*, 3/2013, 13

[52] J. Németh, 40

where social media can affect work, the article presented the case of using social media at the workplace during working hours.

The main question that the paper intended to answer was whether the already existing regulations – both in the EU and in Hungary – regarding employees' personal Internet use at the workplace can be applied to the case of personal social media use at the workplace. As social media and social network sites are Internet based sites, the rules for Internet use at the workplace can be adequately applied to these questions. However, the appearance of mobile devices raises some new challenges. They seemingly exempt from the employer's monitoring, however, their excessive use and the loss of productivity and working time would give away the employee even without the employer being able to monitor these devices.

The employer has the right to decide whether he/she allows employees to check their personal social media account and can monitor whether employees respect that decision or not. In my opinion, a complete ban on the use of social media at the workplace would be unrealistic, as today social media and social network sites play a growing role in everyday life. Permitting employees to access social media from work would not mean that they would spend their whole day on these sites: the employer would be able to decide how much time they can spend on it (e. g. 20 minutes daily) and can easily monitor – while respecting the data protection requirements of proportionality and necessity – how much time employees truly spend on these sites. Transparency is a very important requirement, which can also prevent the misuse of the employer's equipment. The employer is obliged to inform the employees regarding the rules of the company's equipment and its monitoring. Despite the new challenges raised by the development of information communication technologies, if reasonableness is present from both sides, the employer and the employees, too, can effectively enforce their rights and interests. Through regulation and monitoring the employer can ensure that there is no considerable amount of working time or productivity loss, while the employees can retain their right to privacy and to data protection and still be able to check their Facebook profiles.

*Адриен И. Лукач, студент докторских студија*
*Универзитет у Сегедину*
*Правни факултет и*
*Универзитет Пантеон-Сорбона (Париз 1)*
*Правни факултет у Паризу*
*lkcs.adrienn@gmail.com*

# Надзор над коришћењем друштвених мрежа на радном месту од стране запосленог са посебним освртом на регулативу у вези са заштитом података о личности у праву Европске уније и праву Мађарске

***Сажетак**: Фејсбук, али и друге друштвене мреже, данас играју значајну улогу у човековој свакодневници, те с тога, ни радно место не представља изузетак. Но, коришћење друштвених мрежа у току трајања радног времена негативно утиче на остваривање интереса послодавца у радном односу. Управо зато, главна тема овог чланка јесте да ли и под којим условима послодавац може да врши надзор над коришћењем друштвених мрежа на радном месту од стране запосленог, а да при томе не крши правила о заштити података о личности. Како је надзор над "традиционалном" употребом интернета већ уређен у праву Европске уније и праву Мађарске, главно питање овде јесте како та правила на адекватан начин применити и у случају надзора над коришћењем друштвених мрежа од стране запосленог? У одговору на ово питање, аутор је најпре изложио постојећа правила у вези са заштитом података о личности приликом надзора над коришћењем интернета у праву Европске уније и праву Мађарске, потом је елаборирао реформу у домену заштите података о личности у праву Европске уније, да би на крају, сагледао савремене изазове у вези са коришћењем друштвених мрежа.*

***Кључне речи:** друштвене мреже, надзор над радом запосленог, заштита података о личности.*