universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Employee monitoring in the digital age”

Monitoring of social networking sites

verfasst von / submitted by

Christoph Pixner

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Univ.Prof.Dr.Dr.hc. Peter Fischer

Table of Contents

ABSTRACT

1. The workplace has drastically changed over the last decade. The emergence of social media has created new ways for people to communicate with each other. During their use however, the individual shares an unprecedented amount of personal data. This conduct can have serious implications for the employer.[1] The employment relationship is historically defined as a relationship where one party, the employee, performs the work while the other party, the employer, remunerates him/her for that work. Naturally, the employer has an interest in monitoring that the work he bestows upon his/her employees is being performed. To ensure employee productivity and to reduce the risk of reputational loss, the employers are increasingly relying on new information and communications technologies to monitor their employees. The adoption of new forms of infrastructures, applications and smart devices enables employers to collect and connect each other with enormous quantities of employees' personal data and to do so within a reasonable time and with inexpensive means.[2] The new types of systematic data processing at work are less visible than traditional ones such as overt CCTV cameras but are more invasive of the private life of employees. It is not surprising that social media monitoring poses privacy concerns for the employees and creates significant challenges for privacy and data protection.

2. The aim of this paper is to establish the data protection legal framework that applies to the employment relationship. The paper will try to establish to what extent the employee enjoys privacy protection with regards to his/her social media usage. A legal problem that will be analysed in this paper is the collision between the employee's right to privacy and right to data protection and the employer's legitimate interest. Since there are fundamental rights and significant interests on both sides, a balance in enforcement must be found. Where that balance lays and how it should be approached depends on the phase of the employment relationship and the method of communication.

[1] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 185.
[2] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 2.

ZUSAMMENFASSUNG

3. Der Arbeitsplatz hat sich in den letzten Jahren stark verändert. Das Aufkommen von Sozialen Medien hat neue Kommunikationsmöglichkeiten geschaffen. Doch, während dessen Benutzung teilt der Benutzer eine unglaubliche Menge an persönlichen Daten. Die Benutzung von Sozialen Medien durch Mitarbeiter kann auch starke Folgen haben für den Arbeitgeber. So kann die Benutzung von Sozialen Medien während der Arbeitszeit Einfluss haben auf die Arbeitsleistungen der Mitarbeiter. Auch der gute Ruf des Unternehmens kann durch negative Kommentare der Mitarbeiter im Netz beeinflusst werden.

4. Es ist klar das der Arbeitgeber ein berechtigtes Interesse darin hat die Benützung von Sozialen Medien durch Mitarbeiter zu überwachen, sowohl während als nach der Arbeitszeit. Diese Überwachung kann aber nicht unbegrenzt stattfinden. Sowohl Internationale Verträge als Europäische Vorschriften begrenzen die Autorität des Arbeitgebers. Der Fokus dieser Arbeit liegt hauptsächlich bei der Datenschutz-Grundverordnung (DSGVO). Da diese Verordnung aber nicht speziell für das Arbeitsverhältnis geschaffen ist untersucht diese Arbeit ob und in wie fern die DSGVO anwendbar ist.

5. Im Arbeitsverhältnis kommt es zu einer Kollision von zwei gegensätzlichen Interessen. Auf der einen Seite gibt es das berechtigte Interesse des Arbeitgebers um die Produktivität seiner Mitarbeiter zu kontrollieren und das Unternehmen vor einem Imageverlust zu beschützen. Auf der anderen Seite steht das Recht des Mitarbeiters auf Privatsphäre und Datenschutz. Da auf beiden Seiten Grundrechte und wichtige Interessen bestehen, muss ein Gleichgewicht bei der Durchsetzung gefunden werden. Wo dieses Gleichgewicht liegt und wie es ausgelegt werden sollte, hängt von der Phase des Arbeitsverhältnisses und der Kommunikationsmethode ab.

INTRODUCTION

6. There has always been a natural tension between an employee's desire to 'mind their own business' by keeping some parts of their working day private and an employer's legitimate interest to be aware of what is going on at the workplace.[3] An employer's supervisory capacity is fundamental to concepts such as an employer's duty of care to protect employees' health and safety, their duty to promote an employee's dignity at work and – most obviously – ensuring that appropriate work is being performed.[4] While most employees may believe in subordination to their employer for lawful instruction, many would also believe that non-work-related issues should be beyond the purview of their employer.[5] These competing interests meet on a daily basis – in every workplace across the globe – and require a balance to be struck between the employer's need for information and the employee's need for privacy.

7. Traditionally, this balance weighed heavily in favour of employers as the 'right' to supervise was accepted to be one of the key characteristics of an employment relationship. However, in the past, a balance was automatically achieved because the employers' ability to supervise employees was tempered due to logistical constraints. It was often simply physically impossible for the employer to supervise his employees. In practice, these 'blind spots' in the employer's supervisory system automatically became the 'private zones' for employees.[6]

8. Over the last decade, the digital transformation and the introduction of new technologies completely upset this traditional balance. Most of the 'blind spots' that used to exist are gone. Business organizations are now able to use hardware and software to electronically monitor a wide variety of employee behaviours both in and out of the workplace.[7] Monitoring tools have become a staple method for protecting business interests, limiting possible legal liabilities and ensuring employee productivity.

9. The increasing use of electronic monitoring in the modern workplace have exacerbated privacy concerns in the employment context. Consequently, the question on how to balance the competing

---

[3] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 355.
[4] S. HONEYBALL, *Honeyball & Bowers' Textbook on Employment Law, Oxford University Press*, Oxford, 2008, 445; A. OLSOVSKÁ and M. SVEC, "How To Monitor Employees But Protect Employee Privacy?", *Silesian Journal of Legal Studies,* 2016, (81) 81.
[5] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 355.
[6] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 355.
[7] J. FORD, L. WILLEY, B.J. WHITE and T. DOMAGALSKI, "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethical and Regulatory Issues,* 2015, Vol. 18(1), (51) 52.

interests involved arises once again. Considering that the traditional limitations on an employer's ability to monitor are no longer applicable, a balance can only be struck by limiting the employer's authority.[8]

10. This paper sets out to discuss the employer's authority to restrict and monitor his/her employee's social media usage during the different phases of the employment relationship. To achieve this goal the paper starts by interpreting the applicable legal framework. The right to privacy and data protection are not only protected on a European level. Some thought will also be given to recent case law of the European Court of Human Rights and how it effects the employment relationship. After establishing the general legal framework for privacy and data protection, an entire chapter will be devoted to a recent attempt by the European Union to provide guidance on data processing in the employment context.

11. The last Chapter will focus mostly on employee social media monitoring. This Chapter will elaborate the notion that employers have a legitimate interest in social media monitoring, both inside and outside the workplace. Naturally, the employers right to monitor is limited by data protection requirements such as proportionality, necessity and transparency. Additionally, this Chapter will present some challenges raised in social media monitoring as well as point out some regulatory shortcomings. To do all this in an organized manner, Chapter IV makes a distinction between employee social media monitoring according to the different stages of the employment relationship.

[8] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 356.

CHAPTER I: RECENT TRENDS IN EMPLOYEE MONITORING

SECTION I. THE RISE OF SOCIAL NETWORKING SITES

12. Social media has become a global phenomenon. It is one of the most exciting and challenging technological developments in modern times.[9] It is estimated that by 2021, over three billion people will be active on social media worldwide.[10] In today's world, it is harder to find someone who is not on social media than vice versa. Social media platforms such as Facebook, LinkedIn and Twitter have become integral parts of people's daily lives. At first, social media networks were used for private purposes. These networks started as a way for people to connect with each other within an online platform. Over the last years however, social media has also come to play a major role in the workplace as a means of communication and conducting business.[11] Businesses and corporations now make extensive use of social media to advertise, promote and conduct business.[12] Social media has fundamentally changed how the workplace operates and how employers and employees interact with each other.[13] Despite the advantages for businesses, social media use has also created new financial and legal challenges for employers. In considering these challenges, employers' resort to electronic monitoring to protect their business interests and to minimize or prevent exposure to the potential risk of legal liability arising from the misuse of online services by employees.[14] The increased use of electronic monitoring by employers has considerably raised potential privacy threats for employees.

SECTION II. ONLINE MONITORING

13. The modern workplace has become increasingly reliant on the use of online monitoring in an effort to maintain employee productivity and to avoid legal liabilities and business injuries which stem from employee misconduct. However, employee monitoring is not a new phenomenon. Employers have always gathered employee personal data, either to determine whether a candidate

[9] J.C. DUVENHAGE, "Social media in the workplace: Legal challenges for employers and employees", *Masterthesis,* University of Notre Dame Australia, 2017, *https://researchonline.nd.edu.au/theses/164/*, 1.
[10] Statista, *Number of Social Media Users Worldwide From 2010 to 2020* (2016), *https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.*
[11] M. SILVERMAN, E. BAKHSHALIAN and L. HILLMAN, "Social Media and Employee Voice: The Current Landscape", *CIPD Research Report, https://www.cipd.co.uk/knowledge/work/technology/employee-voice-report,* 2013, (1) 8-9.
[12] J. IRETON, "Social Media: What Control Do Employers Have Over Employee Social Media Activity in the Workplace?", *Houston Business and Tax Law Journal,* 2014, (144) 144-145.
[13] J.C. DUVENHAGE, "Social media in the workplace: Legal challenges for employers and employees", *Masterthesis,* University of Notre Dame Australia, 2017, *https://researchonline.nd.edu.au/theses/164/*, 2.
[14] K. EIVAZI, "Computer use monitoring and privacy at work", *Computer Law and Security Review: The International Journal of Technology and Practice,* Vol 27(5), 2011, (516) 516.

was the perfect fit for a job or task, or to comply with legal and administrative requirements.[15] Before the rise of social network sites employers relied mostly on the recording and review of telephone conversations or voicemail messages and the video recording of employees to assess job performance.[16] Since 2007 we can observe a shift in the monitoring techniques used by employers.[17] Organizations are increasingly monitoring new technologies such as social network sites and blogs in order to improve business efficiency and productivity. This rise in the use of information and communication technology in the modern workplace to monitor the online behaviour of employees has blurred the once so clear boundaries between an employee's personal and professional life.[18] In fact, the use of electronic monitoring, facilitated by information and communication technology, not only appears to be a powerful tool in the invasion of an employee's privacy, but can also lead to the potential serious abuse of an employee's personal data, specifically as such technology facilitates the unlimited collection, storage and management of data.[19] Moreover, the collection of personal data is not even limited to the employment relationship. In fact, the Article 29 Working Party[20] recognizes that data collection of employees happens prior to and following the employment relationship, thus further increasing the related privacy risks.[21]

14. To summarize, although the employer has a legitimate interest in collecting an employees' personal data, the problem with new monitoring techniques is that such practices are no longer contained to the work environment but are now also being applied to the 'online' world, albeit in the employment context.[22] Specifically the use of information found online, particularly in connection to social networking sites, is increasingly playing a role in employers' decisions.

---

[15] S. WALLACH, "Who's Info is it Anyway? Employees' Right to Privacy and Protection of Personal Data in the Workplace", *Int'l J. Comp. Lab. L. & Indus. Rel. 23,* 2007, (195) 224-225.
[16] J. FORD, L. WILLEY, B.J. WHITE and T. DOMAGALSKI, "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethical and Regulatory Issues,* 2015, Vol. 18(1), (51) 53.
[17] J. FORD, L. WILLEY, B.J. WHITE and T. DOMAGALSKI, "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethical and Regulatory Issues,* 2015, Vol. 18(1), (51) 54.
[18] G. LASPROGATA, N.J. KING and S. PILLAY, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 1.
[19] K. EIVAZI, "Computer use monitoring and privacy at work", *Computer Law and Security Review: The International Journal of Technology and Practice,* Vol 27(5), 2011, (516) 517.
[20] Explained in detail in Chapter III, Section II.
[21] Article 29 Working Party, WP 48, Opinion 8/2001 on the processing of personal data in the employment context, adopted 13 September 2001, 8, available at: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf* (Accessed 14 February 2019).
[22] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 5.

CHAPTER II: THE FUNDAMENTAL RIGHTS APPROACH

15. When the General Data Protection Regulation[23] (hereafter: GDPR) finally went into force on the 25 May 2018, it was quickly hailed as a major win for individuals as it strengthened their rights and increased the obligations on organizations.[24] Although the GDPR is without a doubt the most famous piece of privacy regulation at the moment, it is far from the only one. Several international documents acknowledge the right to respect for private life and personal data protection, both at the universal and at the regional level.[25]

16. In Europe an employee's privacy rights (*Right to respect for private and family life*) have been laid down in Article 8 of the Council of Europe's *Convention for the Protection of Human Rights and Fundamental Freedoms* of 1950 (hereafter: ECHR).[26] This article provides that:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*[27]

17. The European Court of Human Rights (hereafter: ECtHR), which enforces the rights established under the Convention, interprets the protection of "private life" to include the workplace and extends protection of privacy in correspondence to communications from it.[28] In *Niemietz v. Germany*[29], the ECtHR held that:

---

[23] 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), 2016, *OJ* L199, 1-88.

[24] See for example the Irish Data Protection Commission, "GDPR & You", *http://gdprandyou.ie* (Accessed 22 March 2019).

[25] 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) 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.

[26] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 16 and 18; A. OLSOVSKÁ and M. SVEC, "How To Monitor Employees But Protect Employee Privacy?", *Silesian Journal of Legal Studies,* 2016, (81) 82.

[27] Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome, 4 November 1950, *https://www.echr.coe.int/Documents/Convention_ENG.pdf* (Accessed 1 March 2019).

[28] G. LASPROGATA, *et al.*, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 12.

[29] ECtHR 16 December 1992, nr. 13710/88, *Niemietz v. Germany*, para. 29.

Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not.

18. By extending the *Right to respect for private and family life* to the workplace, the Court practically limits the employer's ability to interfere with an employee's privacy, particularly with regards to monitoring and surveillance tools. Furthermore, it has been established that this right should be understood as keeping with technological developments and to be applicable to any new form of communication.[30] Consequently, this would indicate that the right to privacy should be interpreted as being applicable to online communications, including those that are publicly available and easily found online.[31]

19. Recent caselaw helps further define the boundaries regarding employee privacy in the European workplace. In its *Bărbulescu v. Romania*[32] decision, the Court held that a Romanian employee's legally protected right to privacy was violated when his employer monitored personal messages he sent from a company account, reversing a previous decision by the ECHR in this case that had expanded employers' rights to monitor employees.[33] *Bărbulescu* is the Court's first case concerning the monitoring of an employee's electronic communications by a private employer.[34] In the case concerned, Mr Bărbulescu was employed by a Romanian private company as a sales engineer and was asked to open a Yahoo Messenger account for professional purposes. On two occasions the applicant was notified by his employer that his communications would be monitored; however, the extent of the monitoring was not defined. Mr Bărbulescu was fired after having reportedly made use of the Yahoo Messenger account for personal reasons, despite the relevant strict prohibition. More precisely, he was informed that his communications had been

[30] S. WALLACH, "Who's Info is it Anyway? Employees' Right to Privacy and Protection of Personal Data in the Workplace", *Int'l J. Comp. Lab. L. & Indus. Rel. 23,* 2007, (195) 197-198.
[31] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 13.
[32] ECtHR 5 September 2017, nr. 61496/08, *Bărbulescu v. Romania.*
[33] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 53-54; N.L. STERLING and E.R. FEDELES, "Introductory note to Barbulescu v. Romania (Eur. Ct. H.R.)", *International Legal Matters*, 2018, (80) 81 (Accessed 29 March 2019).
[34] The *Halford v. UK* and *Copland v. UK* decisions, which were not overruled by the Court, both involved public rather than private employers; N.L. STERLING and E.R. FEDELES, "Introductory note to Barbulescu v. Romania (Eur. Ct. H.R.)", *International Legal Matters*, 2018, (80) 81 (Accessed 29 March 2019).

monitored and that conduct contrary to internal regulations had been recorded. Although Mr Bărbulescu denied having used the account for non-professional communication, he was presented with a transcript of his communications which refuted his denial. Subsequently, the employment contract of Mr Bărbulescu was terminated, leading him to challenge his employer's decision before the courts.[35] The majority in the Grand Chamber agreed on appeal to overrule the Chamber's earlier decision[36] in holding that Mr. Bărbulescu's communications – even though they occurred in the workplace using workplace equipment – were covered by the concepts of private life and correspondence and thus Article 8 was engaged.[37] Consequently, the question than arises what value should be contributed to Mr Bărbulescu's employer' policies which tried to exclude the right, i.e. whether or not an employee's privacy rights at work can be excluded by virtue of an agreement between the employer and the employee.[38] The Court answered this question negatively, stating that 'an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.'[39] Well, if the employee's privacy right cannot be completely excluded, the questions arises again where the boundary between privacy and legitimate intrusion should be drawn. The Court – while acknowledging that states and employers should have a wide discretion to determine the acceptable level of intrusion – held that it is up to domestic authorities to ensure that any introduction of measures to monitor communications should be accompanied by adequate and sufficient safeguards against abuse.[40] The Court provided for six guiding factors for domestic authorities and employers to take into consideration when assessing the acceptable levels of intrusion:[41]

- Prior notification of monitoring: this should be clear as to the purpose and extent of the monitoring of communications and should be given in advance of the monitoring occurring.

[35] Facts as described on *https://strasbourgobservers.com/2017/10/19/barbulescu-v-romania-and-workplace-privacy-is-the-grand-chambers-judgment-a-reason-to-celebrate/* (Accessed 1 April 2019).
[36] The Fourth Section of the ECtHR held in January 2016 – in a six to one majority – that while Bărbulescu's Article 8 right were engaged, there was no violation as a fair balance had been struck between the respect for his private life and correspondence and his employer's interest. The court was influenced by the argument that the employer had only accessed the contents of Mr Bărbulescu's communications after he had stated that the Yahoo messenger had only been used for work-related purposes. Therefore, the access was legitimate as the employer claimed to be expecting to find only work-related contents.
[37] ECtHR 5 September 2017, nr. 61496/08, *Bărbulescu v. Romania,* para 81.
[38] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 357.
[39] ECtHR 5 September 2017, nr. 61496/08, *Bărbulescu v. Romania,* para 80.
[40] ECtHR 5 September 2017, nr. 61496/08, *Bărbulescu v. Romania,* para 120.
[41] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 357-358.

- The extent of the monitoring: it must be clear whether or not the monitoring is of the contents of communications, as distinct from just monitoring the identities of the senders/recipients. Whether or not all communications are monitored or are there limitations, e.g. only random emails are monitored or all emails are monitored for limited time periods in a sporadic fashion. Measure should also be taken of the extent to which the information gleaned is published, i.e. how widely is the information disseminated.
- Justification: the reasons proposed for carrying out the monitoring must be proportionate to the level of monitoring. The court noted that as 'monitoring of the content of communications is by nature a distinctly more invasive method, it requires weightier justification'[42].
- Necessity: if the purpose of the monitoring could be achieved by a less invasive method, then that method should be pursued.
- Consequences for employee: there cannot be unintended consequences for an employee, i.e. the information gleaned can only be used in furtherance of the stated goals of the monitoring; e.g. if the goal is to ensure that sensitive information is not being shared through email with competing entities and an employer discovers that an employee has used the email system to discuss private matters, this information is of a different nature to that being sought by the monitoring. Consequently, this information cannot be used to discipline the employee for using the email system to discuss private matters.
- Adequate safeguards: the employee should be afforded as many safeguards as possible; in particular, the employer should not access the content of messages without specifically notifying the employee – in advance – that such an eventuality may occur.

20. When these criteria were applied to the situation of Mr Bărbulescu, the court held that his employer – and subsequently the Romanian state authorities – had not taken sufficient care to protect his privacy at work. The merit of this case is that it unambiguously sets out that an employee can expect a right to privacy in the workplace and that, as a matter of practice, an employer must put thought into designing their system of supervision in such a way as to respect that right.[43] As will be more broadly discussed in the next Chapter, these guiding principles set out by the Grand Chamber of the ECtHR are almost indistinguishable from the provisions and obligations set out by the GDPR.[44]

[42] ECtHR 5 September 2017, nr. 61496/08, *Bărbulescu v. Romania,* para 121 (iii).
[43] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 358.
[44] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 362-363.

21. Now, since the European Convention on Human Rights is not a legal framework provided by the European Union it is useful – especially for non-jurists – to examine how the European Union and its Member States have observed the fundamental rights laid down in the Convention. Although the European Union still has not acceded to the Convention as set out by Article 6(2) of the Treaty of the European Union (hereafter: TEU), the rights found in the Convention are generally recognised by the European Union and its Member States are fully expected to respect them.[45] In this regard, the jurisprudence concerning the European Convention on Human Rights and the interpreting judgements, including the rulings held in *Niemitz v. Germany* and *Bărbulescu v. Romania*, are directly enforceable in the European Union's Member States and should be regarded as general principles of European Community law.[46]

22. The right to privacy can however also be found in legislation promulgated by the European Union itself. The Charter of Fundamental Rights of the EU[47] acknowledges as a fundamental right both the right to privacy (Article 7) and to data protection (Article 8).[48] Article 7 of the Charter substantially reproduces Article 8 (1) of the ECHR.[49] That being so, it is evident that Article 7 contains rights corresponding to those guaranteed by Article 8 (1) of the ECHR, and therefore by virtue of Article 52 (3) should be given 'the same meaning and scope' as Article 8 (1) of the ECHR.[50] While Article 7 reinforces an individual's privacy rights, the European Union's Charter includes a further provision which may be more suitable to protect an employee's informational privacy in the modern workplace, specifically with regards to the increased use of personal data collected via electronic monitoring.[51] Under Article 8 the Charter provides for the protection of personal data by stating that:

---

[45] G. LASPROGATA, N.J. KING and S. PILLAY, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 5.

[46] See Article F(2) of the Treaty of Maastricht 1992; M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 13-14.

[47] Charter of Fundamental Rights of the European Union, 2012/C 326/02, available at: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT* (Accessed 2 April 2019).

[48] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 18; G. LASPROGATA, N.J. KING and S. PILLAY, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 5; A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 191.

[49] As observed by the ECJ in its judgement of 29 January 2008, *Productores de Música de España (Promusicae) v. Telefónica de España SAU,* C-275/06, para 64; M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 22.

[50] M. OTTO, *The Right to Privacy in Employment: A Comparative Analysis, Hart Publishing,* Portland, 2016, 108.

[51] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 14.

1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

23. The provision includes a series of principles that are staple to the European Union's approach to data protection and which have been better defined in the European Union's data protection legislation, such as the GDPR.[52] These principles will be discussed in detail in the next chapter.

24. The right to privacy and the right to data protection are thus not synonymous concepts. While the right to privacy first appeared at the end of the 19th century, it was not until the appearance of computers in the 1960s that new legal protection was needed and the right to data protection appeared.[53] There is still no uniform standpoint on the relation between the right to data protection and the right to privacy.[54] A. LUKÁCS, referring to the opinion of A. JÓRI, interprets the right to data protection as *"a unique legal way to protect the private sphere of the individual"*, so it also aims to protect privacy, but this right can effectively ensure the protection of privacy in the digital era.[55] Following the entry into force of the Treaty of Lisbon (including the Charter of Fundamental Rights of the EU) in December 2009, the right to the protection of personal data became a fundamental right.

25. The protection afforded to the right to privacy and to the right to data protection, as both the ECtHR and ECJ case law clearly imply, is not absolute and interference with these rights might be justifiable under the right conditions.[56] In the employment context, the employer disposes certain legitimate interests which can prevail over the rights of the employees. What these interests can be and how they should be used will be subject of discussion in the last chapter.

[52] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 14.
[53] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 189-190.
[54] N. PURTOVA, "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights"*, Netherlands Quarterly of Human Rights,* 28 (2), 2010, (179) 181.
[55] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 190-191.
[56] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 19; M. OTTO, *The Right to Privacy in Employment: A Comparative Analysis, Hart Publishing,* Portland, 2016, 119.

CHAPTER III: RIGHT OF DATA PROTECTION IN THE GDPR

SECTION I. RIGHT TO DATA PROTECTION IN THE GDPR

26. On the 25th of May 2018 the General Data Protection Regulation came into force.[57] This new and improved piece of regulation – which repeals the former Data Protection Directive[58] (hereafter: DPD) – regulates how natural persons should be protected with regards to the processing of their personal data.[59] The GDPR applies to the data collection performed by private marketing companies as well as to research by private companies or public universities, in very similar ways in all Member States, all sectors (public or private) and all purposes (commercial and non-commercial).[60] The GDPR has two main goals[61]: The first goal is to protect the fundamental rights and freedoms of the data subjects by creating a protective regiment with regards to the processing of personal data. The second goal is to create the optimal conditions so that the free flow of personal data – in parallel to the free movement of goods and services – can take place within the EU, supporting the creation of the European Single Market.

27. Before I proceed to analyse how the GDPR will affect the data processing of employees and more specifically their social network usage, it is important to make clear the fundamental terms and ideas of this piece of law. Consequently, in this Chapter I will present the GDPR's concepts and principles that are the most relevant for employment related data retrieval and processing.

28. The GDPR defines the right to protection of personal data as one of the fundamental rights and freedoms of natural persons (art. 1 (2) GDPR).[62] Since fundamental rights protection is the raison d'être of data protection legislation[63], the level of protection of personal data, or in a broader view,

---

[57] J. POHLE (ed.), "Data Privacy Legislation in the EU Member States – Part Two of the Practical Overview. How EU Member States have adjusted their domestic data privacy law to the GDPR – Update", *Computer Law Review International,* 2018, (133) 133.
[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. L 281*, 1995, available at *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML* (Accessed 2 April 2019)
[59] W. BERNING and L. KEPPELER, "Datenschutz im Konzern"*, HMD Praxis der Wirtschaftsinformatik*, 2017, (1021 1022; A. KOTSIOS, M. MAGNANI, L. ROSSI, I. SHKLOVSKI and D. VEGA, "An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research", *Cornell University Journal,* 2019, (1) 2.
[60] A. KOTSIOS, *et al.*, "An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research", *Cornell University Journal,* 2019, (1) 2.
[61] A. KOTSIOS, *et al.*, "An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research", *Cornell University Journal,* 2019, (1) 2.
[62] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 4.
[63] F. BIEKER, *et al.*, "A process for data protection impact assessment under the European General Data Protection Regulation", *Lecture Notes in Computer Science,* 2016, Vol. 9857, (21) 36.

the right to privacy of natural persons, guaranteed by the GDPR, must be interpreted in the context of the Charter of Fundamental Rights of the EU. The scope of the right to privacy and the right to protection of personal data, as described in legal acts of European scope, is defined in specific terms in case law of the ECtHR and the European Court of Justice, as discussed in the previous Chapter.

29. What constitutes 'personal data' is defined quite broadly in the GDPR as any information that does or may lead to the identification of a natural person (art. 4 (1) GDPR).[64] The term 'processing' is defined similarly broadly as "any operation or set of operations on personal data or sets of personal data" (art. 4 (2) GDPR), including data collection.[65] These definitions cast a very wide scope. The Article 29 Working Party has clarified in its Opinion 8/2001[66] what this means in the employment context. This Opinion pertained to the DPD, but the statements made remain true for the GDPR. The Article 29 Working Party clarified that "personal data" in the employment context means all data that pertains to the employee, such as names, addresses and similar, as well as email communication and internet access, if it can be linked to a specific individual. Similarly, processing sound and image data concerning an individual employee would also fall within the scope.[67]

30. A very wide type of processing is profiling. Just like the previous two, this term covers an equally broad definition. The GDPR defines profiling (art. 4 (4) GDPR) as "any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements".

31. The GDPR distinguishes between three types of actors in data protection law. On the one side, the process of data processing involves a data controller who is fully responsible for the

[64] M. ARANY-TÓTH, *Arbeitnehmerdatenschutz in Ungarn im Rahmen des europäischen Datenschutzrechts, Peter Lang,* Frankfurt am Main, 2011, 14.
[65] A. KOTSIOS, *et al.*, "An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research", *Cornell University Journal,* 2019, (1) 4.
[66] Article 29 Working Party, WP 48, Opinion 8/2001 on the processing of personal data in the employment context, adopted 13 September 2001, 13, available at: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf* (Accessed 12 June 2019).
[67] G. LASPROGATA, N.J. KING and S. PILLAY, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 11; M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 25.

correctness of the data processing.[68] In the employment relationship, the employer is the data controller. The employer as a data controller must comply with the obligations laid down by the data protection regime.[69] There can also be a processor who processes the personal data on behalf of the controller. The difference between the controller and the processor is that the latter's scope of responsibility does not include making decisions both on the purposes and on the means of data processing. The third actor in the data processing process is the data subject him/herself. It is his/her data that is being processed, either by the controller directly or by the processor on behalf of the controller. In our case, the employee is the data subject. It is he/she who enjoys the protection of his/her privacy and data under privacy and data protection rules set out by the GDPR and fundamental rights.

32. The GDPR has not replaced the personal data processing rules that were introduced by the DPD but has updated and significantly reinforced them. The data protection regime is still based on the fundamental principles, such as the purpose limitation principle, data minimisation principle or storage limitation principle. The data minimisation principle is particularly relevant in the GDPR since digital transformation and data exchange have evolved making frequent data collection for a variety of treatments.[70] These principles aim to ensure that monitoring processes are not overly intrusive on an employee's privacy rights. This is especially true in the employment context where these principles have to be balanced against the legitimate interests of the employer.[71]

33. Additionally, the controller is still required to specify the legal basis of the processing, however, this requirement has been made more stringent in relation to sensitive data. In general, the GDPR lists six lawful basis for processing of personal data (art. 6 GDPR): (a) the data subject has given its consent; (b) it is necessary for the performance of the contract; (c) it is necessary in order for the controller to comply with a legal obligation; (d) it is necessary in order to protect individuals' vital interests; (e) it is necessary for the performance of a task carried out in the public interest; (f) it is necessary for the purposes of legitimate interests pursued by the controller as long as these interest are not overridden by interests and fundamental rights and freedoms of the data subjects.[72]

---

[68] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 144.
[69] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 199.
[70] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 8.
[71] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 26.
[72] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 65-88.

All these legal bases are equivalent: the processing of data is lawful if any of these conditions is met. Demonstrating compliance with one of them is therefore enough.[73]

34. The European Union model of data protection recognises "data subject" a positive freedom to control and intervention.[74] This so called right to informational self-determination (*recht auf Informationelle selbstbestimmung[75])* requires that the individual is aware who processes his/her data, what kind of data and for what purposes.[76] To support this right to informational self-determination, the GDPR introduces seven principles that must be adhered to when processing personal data. Chapter II[77] states that personal data shall be processed lawfully, fairly and in a transparent manner; data shall be collected for specified, explicit and legitimate purposes only. The data may be processed only if they are adequate, relevant and limited to what is necessary with regards to the purpose of processing and the data must be accurate and up to date to be processed. Moreover, controllers must do an analysis and risk assessment to define the appropriate measures (physical, logical and organizational) to assure integrity and security of data. The purpose limitation principle applies (alongside the lawfulness and fairness principles), among others, to the surveillance of employees and public places.[78]

35. In its third Chapter, the GDPR hands the data subjects, i.e. the employees, the necessary tools to enforce their rights. This chapter codifies the data subjects' rights to receive transparent information, communication and modalities for the exercise of their rights (art. 12 GDPR). It also reaffirms the data subjects' rights to information and access to personal data (art. 13-15 GDPR). These fundamental conditions let individuals decide which kind of personal data could be processed thanks to the recognition of the right to rectification, erasure, restriction of processing and the rights to data portability (art. 16-20 GDPR).[79] Not all these tools are new. However, the

[73] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 65.
[74] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 8.
[75] This concept first appeared in Germany with the famous population census judgement of the Federal Constitutional Court in 1983; Volkszählungsurteil (BVferG), 15 December 1983, 1 bVr 209/83.
[76] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 52; A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 196.
[77] Article 5 and 6 GDPR.
[78] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 53.
[79] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 9.

elements of this structure have been modernised to respond to the growing influence of the internet and new technologies on the protection of personal data.[80]

36. A new demanding obligation under the GDPR is the requirement to notify a personal data breach to the supervisory authority and to the data subject (art. 33 and 34 GDPR).[81] The Independent EU Advisory Body on Data Protection and Privacy outlines that this new requirement strengthens data subjects' rights since communicating a "data breach" to individuals allows them "to protect themselves from its potential consequences".[82]

37. Finally, the European legislator has included Article 88 in the GDPR that provides EU Member States with the ability to "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".[83] The article contains a list of situations for which the national States can extend the employee's personal data protection in the employment context. In accordance with Article 88 (2), any such rules should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, specifically with regards to transparency of processing, transfers of personal data, and monitoring systems at the workplace.[84] According to S. SIEMENS, this would suggest that any subsequent rules provided for by Member States may not weaken the rights provided for by the GDPR.[85]

---

[80] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 5.
[81] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 6.
[82] See WP29 *Guidelines on Personal data breach notification under Regulation 2016/679,* October 2017, 3.
[83] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 600; C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 20-21.
[84] Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, adopted on 8 June 2017, 9, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 12 June 2019).
[85] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 31.

SECTION II. DATA PROCESSING IN THE EMPLOYMENT CONTEXT

38. Despite the great importance of individual rights in the employment context, the European Union has not managed in stating a set of particular uniform rules for workers' data protection across the entire EU.[86] There is currently no EU directive or regulation that speaks directly to electronic monitoring of employees in the workplace.[87]

39. To understand how privacy protection should be understood in the employment context we will look at Opinion 2/2017 *on the processing of personal data in the employment context*[88], as adopted on 8 June 2017 by the group known as the Article 29 Data Protection Working Party.[89] Although the Opinion was adopted under and is primarily based on the old DPD regime, it is somewhat prescient by being cognisant of the obligations placed on employers by the GDPR[90] and can thus offer welcome insight in how data protection in the employment context is to be looked at.

§1. The Article 29 Working Party

40. The Article 29 Working Party (hereafter: WP29) was an independent EU advisory body on data and privacy protection, established by Article 29 of the DPD.[91] It was a European level body comprised of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the EU Commission.[92] Following the GDPR reform, the WP29 was replaced by the European Data Protection Board, composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives (Article 68 GDPR).[93]

---

[86] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 3.
[87] G. LASPROGATA, N.J. KING and S. PILLAY, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 13.
[88] Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, adopted on 8 June 2017, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 10 April 2019).
[89] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 359; C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 10-11.
[90] As stated in the Executive Summary of Opinion 2/2017, available at *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 10 April 2019).
[91] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 596.
[92] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 359.
[93] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 5; C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 10.

41. The WP29 publishes opinions on various data-related issues. In doing so, the Working Party tries to harmonise the application of data protection rules throughout the EU. As the WP29 was a stand-alone entity with an advisory role, its opinions were not directly enforceable against employers. Although the WP29' Opinions don't carry more weight than traditional 'soft law', they can however still be a useful mechanism for determining where the balance lies between an employer's right to monitor his workforce and an employee's right to privacy, especially when considering that the European Data Protection Board has not yet offered an opinion to replace that of the WP29.[94]

42. The Opinion intends to provide practical use to both employers and employees by providing a clear template for dealing with contentious issues. To do this, the Opinion takes an unusual approach by focussing on nine specific scenarios where modern technology has increased the ability of the employer to monitor employees.[95] This Chapter however will not focus on these scenarios but will discuss the provisions of broader application instead.[96]

43. As already hinted at in the beginning of this Chapter, neither the GDPR nor any other piece of EU data protection legislation reserves any kind of special protection for the employee against any one "data subject".[97] Regarding data processing at work, Article 9 of the GDPR merely provides for an exemption from the prohibition on processing sensitive data in the labour field and Article 88 is limited to allow Member States to define specific rules to protect employees' right to personal data.[98]

44. The Opinion 2/2017 stresses that consent cannot legitimate data processing in the employment context due to the nature of the labour relationship.[99] The legal basis for data processing in the employment context could normally be: (1) "Performance of a contract" (meeting obligations

[94] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 359.
[95] Recruitment, in employment screening, ICT usage at work, ICT usage outside the workplace, time and attendance, video monitoring, vehicles, disclosure of employee data to third parties, and international transfer of HR and employee data.
[96] For more on these scenario's see: C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017.
[97] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 10.
[98] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 11.
[99] «Employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Unless in exceptional situations, employers will have to rely on another legal ground than consent – such as the necessity to process the data for their legitimate interest. However, a legitimate interest in itself is not sufficient to override the rights and freedoms of employees»

under labour contract such as paying a salary, requiring the processing of personal data)[100]; (2) "Legal obligations" imposed on the employer by employment law (where law constitutes a legal basis for data processing)[101] and (3) Employer's "legitimate interest"[102].

45. This final legal basis for processing implies specific mitigation measures to ensure a proper balance between the employer's legitimate interest and employees' fundamental rights and freedoms: monitoring limitation (geographical, data oriented and time-related) and appropriate technical and organizational measures.[103] This also implies a proportionality test to assure that the chosen method of data processing is proportional to the business needs. If these mitigation measures are in place, Opinion 2/2017 outlines that in most cases, the legitimate interest of companies can be invoked to process employees' data.[104]

A. Private zones at work

46. Opinion 2/2017 notes unequivocally that employees enjoy a right to private zones even in the workplace, stating that 'it should be ensured that employees can designate certain private spaces to which the employer may not gain access unless under exceptional circumstances'.[105] These private spaces can be physical as well as virtual, e.g. designated areas in the workplace or private sections in electronic calendars or other shared repositories.[106] The Opinion also notes that the right to these private zones cannot be excluded by 'agreement' between the parties – e.g. in an agreed set of employment policies – because: 'Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances'.[107] The Opinion makes it very clear that an employee is entitled to a basic level of privacy at work, which cannot be excluded. Consequently, it is important that we identify where the Opinion sets the boundaries of that right.[108]

---

[100] Article 7 (b) GDPR.
[101] Article 7 (c) GDPR.
[102] Article 7 (f) GDPR.
[103] A. KOTSIOS, *et al.*, "An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research", *Cornell University Journal,* 2019, (1) 10; C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 12.
[104] M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 85.
[105] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 360.
[106] Opinion 2/2017 (n 5) s 5.3., p. 15.
[107] *Ibid,* ch 6.2., p. 23.
[108] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 360.

47. When figuring out how to balance the interests' involved it is important to mention that the WP29 in its 2017 Opinion favours avoiding breaches of privacy through forward planning rather than amending them afterwards. The essence of this approach can be summed up by the phrase: 'prevention should be given much more weight than detection'.[109] This prevention is based on two pillars: first and foremost, on comprehensive practical employment policies and second, in some situations, a data protection impact assessment is needed.[110]

1. Comprehensive Practical Employment Policies

48. Opinion 2/2017 emphasizes that employers must formulate and implement acceptable employment policies, outlining the permissible use of the organization's network and equipment, and strictly detailing the processing taking place.[111] Although the Opinion offers some general advice on how to formulate these policies, the ultimate determinant of the details of these policies will be the context of the work itself.[112] To ensure a long-term success of the policies, the Opinion 2/2017 notes that employees or their representatives should be involved in designing an employment policy,[113] thus ensuring not only 'buy in' by both employers and employees, but also a deeper understanding of each other's perspective.[114]

49. The Opinion suggests three basic elements which should be at the core of all employment policies:

1) Transparency: Effective communication should be provided to employees concerning any kind of monitoring that takes place. Suitably formulated policies must be made freely available to all employees, including specific details of the 'who/what/why' of the monitoring and the means by which an employee can avoid being monitored.[115] A transparency requirement avoids the risk that "the legitimate interest of employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive

[109] Opinion 2/2017 (n 5) s 5.3., p. 15; E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 360.
[110] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 360; C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 12.
[111] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 15.
[112] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 360.
[113] Opinion 2/2017 (n 5) s 6.3., p. 23.
[114] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 360.
[115] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 360.

monitoring.[116]"[117] The key point is that the employee must always be aware of when they are being monitored, even if monitoring cannot be avoided. Covert monitoring may never occur.

2) Proportionality: The employer should always approach monitoring from a minimalist point of view. The level of monitoring must stand in proportion to the risk faced by the employer. An employer must use the least intrusive means possible to achieve a stated goal. F.e. if the goal is to prevent internet misuse, then the system should be based on filters to block inappropriate internet sites, rather than monitoring all the web activity of employees.[118]

3) Data minimisation: Where the stated goal cannot be achieved without intrusion into the private sphere of an employee, then the minimum amount of data should be gathered, shared only with those who need to know and deleted as soon as possible.[119]

50. It is clear that the Opinion, when it comes to formulating employment policies, puts the burden on the employer to prove the necessity of the intrusion rather than on the employee to claim their right to privacy. According to E. KEANE this proposes a default position that all data is private unless the employer can show that a legitimate specific goal of the enterprise can only be satisfied by acquiring that particular data.[120]

2. Data Protection Impact Assessment

51. The GDPR not only included and enhanced the requirements of the DPD, it also introduced new obligations for all data controllers, including employers. The second pillar for preventing excessive monitoring of employees is a new concept that was introduced by Article 35 of the GDPR, the Data Protection Impact Assessment (hereafter: DPIA). A DPIA is an instrument that aims to identify and analyse the main risks of a project with respect to the rights of data subjects concerning their personal data.[121] It is a systematic process to elicit threats to the privacy of individuals, identify the procedures and practices in place to mitigate these threats, and document

[116] *Ibid,* ch. 4, p. 9.
[117] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 24.
[118] *Ibid,* ch. 6.4, p. 23.
[119] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 361.
[120] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 361.
[121] F. BIEKER, M. FRIEDEWALD, M. HANSEN, H. OBERSTELLER and M. ROST, "A process for data protection impact assessment under the European General Data Protection Regulation", *Lecture Notes in Computer Science,* 2016, Vol. 9857, (21) 21-22.

how the risks were addressed in order to minimise harm to data subjects.[122] In the employment context, a DPIA may require employers to carry out an assessment as to whether or not a system of data processing is likely to result in a high risk to the rights and freedoms of employees.[123] A DPIA is not mandatory for all personal data processing activities of a company.[124] The regulation stipulates that a DPIA is necessary when the processing operation, in particular using new technologies, and taking into account the nature, scope and context and purpose of the processing itself is "likely to result in a high risk to the rights and freedoms of natural persons".[125] Applied to the employment context, it is likely that a DPIA would be required where employees and/or their communications are directly monitored, due to the potential sensitive information involved.[126]

52. When discussing the requirements for a DPIA it must be noted that the GDPR itself merely provides a minimum standard for carrying out a DPIA, as stipulated in Article 35 (7) GDPR.[127] In order to facilitate the implementation of the DPIA requirements, the WP29 provided, in a separate opinion, for a detailed guidance on how to carry out an effective DPIA. To qualify the sensitivity of a project, the WP29 proposes in its *Guidelines on Data Protection Impact Assessment (DPIA)*[128] a list of criteria.[129] The WP29 recommends carrying out a DPIA if two of these criteria are met, but, in some cases, only one criterion may suffice[130]. These criteria include, inter alia, large scale data processing, profiling, matching or combining datasets, data processing

[122] R. ALNEMR, E. CAYIRCI, L. DALLA CORTE, A. GARAGA, R. LEENES, R. MHUNGU, S. PEARSON, C. REED, A. SANTANA DE OLIVEIRA, D. STEFANATOU, K. TETRIMIDA and A. VRANAKI, "A Data Protection Impact Assessment Methodology for Cloud", *Lecture Notes in Computer Science,* 2016, Vol. 9484, (60) 60; Y. VAN DER SYPE, "De gegevensbeschermingseffectbeoordeling voor de verwerking van werknemersgegevens, *Or.* 2018, afl 1, (2) 3; C. VANDE VORST en L. VAN GOETHEM, "Wanneer is het verplicht om een gegevensbeschermingseffectbeoordeling uit te voeren?", *TPP* 2018, afl. 1, (14) 14-15.

[123] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 361.

[124] J. SARRAT and R. BRUN, "DPIA: How to carry out one of the key principles of accountability", *Lecture Notes in Computer Science,* 2018, Vol. 11079, (172) 172.

[125] Article 35 GDPR; F. BIEKER, *et al.*, "A process for data protection impact assessment under the European General Data Protection Regulation", *Lecture Notes in Computer Science,* 2016, Vol. 9857, (21) 24; C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 12; J. SARRAT and R. BRUN, "DPIA: How to carry out one of the key principles of accountability", *Lecture Notes in Computer Science,* 2018, Vol. 11079, (172) 172.

[126] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 361.

[127] F. BIEKER, *et al.*, "A process for data protection impact assessment under the European General Data Protection Regulation", *Lecture Notes in Computer Science,* 2016, Vol. 9857, (21) 25.

[128] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, wp248rev.01, adopted on 4 April 2017, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 15 April 2019).

[129] J. SARRAT and R. BRUN, "DPIA: How to carry out one of the key principles of accountability", *Lecture Notes in Computer Science,* 2018, Vol. 11079, (172) 174.

[130] A single criterion can be considered when the stakes require it. The is particularly the case for sensitive personal data processing operations.

of vulnerable data, automated-decision making with legal of similar significant effect, and systemic monitoring of a data subject.[131] When it comes to the employment context, the WP29 outlines that a DPIA is likely to be required if «a company systematically monitor(s) its employees' activities, including the monitoring of the employees' work station, internet activity» since it implies a «systematic monitoring and data concerning vulnerable data subjects»[132].[133]

53. While the Guidance Paper of the WP29 provides some welcome insight on how and when to perform a DPIA, it is important to note that, just like the Opinion 2/2017, the guidance itself is not directly enforceable against employers. The Guidance Paper provides that if a DPIA is to meet the standard of a proper DPIA for the purposes of the Regulation, it must include[134]:

- A systematic description of the monitoring, including the scope of the monitoring, the hardware/software used and the period for which the data will be stored.

- Details of the necessity and proportionality of the monitoring, including the relevancy of the specific purpose, the level of intrusion into the private sphere of the employee, the potential recipients of the data and details of how the rights of employees will be upheld (e.g. right to access, rectify, erase or limit the portability of the data).

- Details of how the risks to the rights and freedoms of data subjects are managed, including the identification of the sources of risks, the potential impacts and if/how those risks can be resolved or reduced.

- The involvement of interested parties, including not just the relevant employees but the employer's Data Protection Officer and, if any high risks cannot be eliminated, the national data protection authority.

54. Whenever a DPIA is required, the above-mentioned requirements certainly impose quite a heavy obligation on an employer. It is however in the employers' interest to comply with these standards for a proper DPIA since a well implemented DPIA can be regarded as an early warning system enabling all actors to systematically address potential deficiencies in a process at the

[131] For the other criteria, see WP 29, Guidelines on Data Protection Impact Assessment, p. 9-11.
[132] *Ibid,* p. 11.
[133] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 13.
[134] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 361-362.

implementation stage and thus reduce the risk of infringing on the data subjects' rights *a priori*.[135] Controllers, i.e. employers, can foresee risks and their causes and are thus enabled to distribute responsibilities and competences accordingly in order to implement data protection at the core of the operations.[136] When combined with the requirement for agreed employment policies, these measures mean that the employer must give significant forethought to the system of monitoring that he wishes to use.[137] This way the GDPR hopes to *prevent* data subjects' rights infringements rather than *amend* them.

55. **CONCLUSION.** It can be concluded that the WP29' approach in its Opinion 2/2017 is very similar to ruleset set out by the ECtHR in its *Bărbulescu v. Romania* decision. Both the WP29 and the ECtHR seem to agree that employees enjoy a right to private zones, even in the workplace, and, that this right to private zones cannot be excluded by the employer by way of an agreement between the parties. Off course this does not mean that an employer cannot monitor his employees at all. But if he wants to implement monitoring measures, he must implement sufficient safeguards to prevent abuses by the employer. As to not exceed the acceptable level of intrusion, both the WP29 and the ECtHR attach great importance to transparency towards the monitored subject and proportionality of the monitoring measures. At all times must an employee be aware if and to what extent his communications are being monitored.

56. In this chapter we have looked at what rules do apply to employee monitoring in general and what the employer can do to prevent breaches of data protection rules. The next chapter will focus on an employee's use of Social Networking Sites, why this recent development brings along new issues for the employment relationship and how an employer can cope with them.

[135] F. BIEKER, *et al.*, "A process for data protection impact assessment under the European General Data Protection Regulation", *Lecture Notes in Computer Science,* 2016, Vol. 9857, (21) 35.
[136] F. BIEKER, *et al.*, "A process for data protection impact assessment under the European General Data Protection Regulation", *Lecture Notes in Computer Science,* 2016, Vol. 9857, (21) 35.
[137] E. KEANE, "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), (354) 362.

CHAPTER IV: MONITORING THE EMPLOYEE'S USE OF SOCIAL NETWORK SITES AT THE WORKPLACE

57. In the previous chapter we have discussed the substantive legal framework concerning an employee's privacy protection. This chapter will discuss the implications these rules have in practice and how both employers and employees should approach their rights and obligations. This Chapter will take a more pragmatic approach to data protection law by focussing specifically on the recent monitoring trend and its implications in the employment context. The focus will mainly be on monitoring of social network sites. In this chapter we will try to answer the question as to whether or not this existing framework can effectively regulate the use and monitoring of social network sites.[138]

SECTION I. THE PROLIFERATION OF SOCIAL NETWORKING SITES

58. The global scale and evolution of information technologies have changed the data processing environment and brought new challenges. These result in particular from the widespread online processing of data, the ubiquity of devices with access to the internet, the common use of social networking services, and the growing capacity of data processing hardware and software.[139] Especially the wide spread use of social network sites[140] (hereafter: SNS) creates a wide array of new challenges. SNSs have quickly developed into widely used communication channels whose importance on our everyday lives can hardly be overstated.[141]

59. As a general rule, SNSs allow a user to create a public or semi-public profile, articulate a list of other users with whom they share a connection, and view other users' profiles in the system.[142]

---

[138] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 594.

[139] N.N. GOMES DE ANDRADE and S. MONTELEONE, "Digital natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications" in S. GUTWIRTH, R. LEENES, P. DE HERT and Y. POULLET (eds.), *European Data Protection: Coming of Age*, *Springer Dordrecht*, 2013, (119) 119; M. KRZYSZTOFEK, *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 10.

[140] The concept of 'Social Media' will be used interchangeably with 'Social Networking Sites'throughout this paper as they mostly pertain to the same thing.

[141] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 185; D. PERAS, R. MEKOVEC and R. PICEK, "Influence of GDPR on social networks used by omnichannel contact center", *MIPRO* 2018, Opatija, (1132) 1132.

[142] V. BROWN and E. VAUGHN, "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions", *Journal of Business and Psychology,* 2011, Vol. 26 (2), (219) 220; D.J. KUSS and M.D. GRIFFITHS, "Online Social Networking and Addiction – A Review of the Psychological Literature", *Int.J.Environ.Res.Public Health* 2011, (3528) 2528-3529; M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 7.

The idea behind these sites is to connect people, for instance friends or alumni, with one another on an informal basis and make communication more effective. Users of SNSs step outside their immediate family circle and enter the realm of virtual social interactions; they introduce themselves by sharing information; connect and communicate with each other. SNSs differ from physical places in many respects: they are mediated, and potentially global, searchable, and the interactions may be recorded or copied and also these sites may have invisible audiences or audiences not present at the time of the conversation.[143] The use of SNSs is not only heavily encouraged by the SNSs themselves, but the societal pressure is also an important factor.[144] With a large part of the population 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.[145]

60. SNSs can be used for numerous objectives, ranging from self-expression and keeping in touch with acquaintances to targeted advertising. During their use of SNSs, individuals share large amounts of personal data. This data can become a valuable commodity for external users and entities that have lucrative and non-lucrative objectives.[146] This was even recognised by the WP29. In its Opinion on Online Social Networking, the WP29 stated that "the personal information a user posts online, combined with data outlining the user's actions with other people, can create a rich profile of that person's interests and activities. Personal data published on SNSs can be used by third parties for a wide variety of purposes, including commercial purposes, and may pose major risks".[147]

61. It is obvious that during their use an enormous amount of personal data is shared on SNSs, which can have serious implications for employment.[148] For Example, accounts of employees discrediting themselves and their employers via postings on SNS and media sites have become

[143] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 269.
[144] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 188.
[145] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 188.
[146] R. FARAHBAKHSH, H. XIAO, A. CUEVAS and N. CRESPI, "Analysis of publicly disclosed information in Facebook profiles", *2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,* 2013, (699) 699.
[147] Article 29 Working Party, WP 163, Opinion 5/2009 on Online Social Networking, adopted on 12 June 2009, 4, available at: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf* (Accessed 23 April 2019).
[148] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 185; R. SPRAGUE, "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship", *University of Louisville Law Review,* 2011, Vol. 50, (1) 22-23.

ubiquitous.[149] For example, in Belgium, an employee was dismissed after criticising the employer's company policy on Facebook.[150]

62. While SNS can surely have impressive benefits to individuals and businesses, in the employment context, their (mis)use can also be a threat to an organization's confidentiality and reputation.[151] Members of SNS expose not only their personal information, but also details about the organizations for which they work.[152] This in turn has urged employers to increasingly rely on online monitoring, not only to observe what employees do on the job but – more importantly – to review their electronic communications, in a move to limit their exposure to liability or security risks.[153]

SECTION II. EMPLOYER'S INTERESTS AND EMPLOYEE'S RIGHTS COLLIDE

63. Until this point, the main focus of this paper was on employees' rights in the employment relationship, namely his/her right to privacy and data protection. Although the default position is that the employee enjoys the right to privacy, this right is not absolute. The employer also enjoys some rights that stem directly from the employment contract.[154] 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.[155] Once an employee agrees to the employment contract, he/she is under a contractual obligation to perform the work and to follow the instructions of the employer. To ascertain that the employee actually performs his tasks properly, the employer has a right to monitor whether the employee complies with his/her instructions. This monitoring necessarily comes with the processing of personal data and falls

[149] P.S. ABRIL, A. LEVIN and A. DEL RIEGO, "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee", *American Business Law Journal,* Vol. 49, 2012, (63) 68.
[150] Arbh. Brussel 3 September 2013, nr. 2012/AB/104, *Juristenkrant* 2013, afl. 278, 6; *JTT* 2013, afl. 1173, 497; *Ors.* 2014, afl. 3, 20; *Or.* 2013, afl. 9, 231; *Rev.trim.dr.fam.* 2014, afl. 3, 711; *RW* 2013-14, afl. 40, 1586.
[151] P.S. ABRIL, A. LEVIN and A. DEL RIEGO, "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee", *American Business Law Journal,* Vol. 49, 2012, (63) 69-70; R. SPRAGUE, "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship", *University of Louisville Law Review,* 2011, Vol. 50, (1) 35-36.
[152] M. FIRE, R. PUZIS and Y. ELOVICI, "Organization Mining Using Online Social Networks", *Networks and Spatial Economics,* 2013, (1) 1.
[153] G. LASPROGATA, N.J. KING and S. PILLAY, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 2.
[154] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 268-269.
[155] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 595.

under the scope of the data protection legislation, meaning that the monitoring of employees, especially their internet use and behaviour, is subject to the rules set out in the GDPR.

64. Ensuring employee productivity is a major consideration to support the monitoring processes.[156] But employers have also long been aware of the risk of legal liability or loss to which their organizations may be exposed as a result of inappropriate employee activities online.[157] Traditionally, the employee is seen as the weaker party but nowadays we also have to take the *reversed vulnerability* of the employer into consideration. Employees can do a lot of damage to the employer by using the internet and SNSs. 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.[158] This risk of reputational loss is strengthened by the long-lasting availability of content posted online, causing issues for the employer even after the content is not relevant anymore.[159]

65. It is obvious that employers have an interest in knowing as much as possible about their employees and thus have an interest in monitoring their employees' activities. However, SNSs put the already existing interests into a different light by providing an unprecedented quantity and quality of personal data available online from which the employer can draw consequences regarding the employees' professional aptitudes, loyalty, etc. Additionally, the new monitoring techniques are no longer contained to the work environment.[160] The monitoring of SNSs expands inspection to activities conducted outside the workplace and beyond working hours.[161] According to A. LUKÁCS, it is this characteristic that distinguishes most SNS monitoring from the traditional types

[156] G. LASPROGATA, N.J. KING and S. PILLAY, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, (1) 2.
[157] J. FORD, L. WILLEY, B.J. WHITE and T. DOMAGALSKI, "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethical and Regulatory Issues,* 2015, Vol. 18(1), (51) 51.
[158] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 202; R. SPRAGUE, "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship", *University of Louisville Law Review,* 2011, Vol. 50, (1) 35-36.
[159] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 202.
[160] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 5.
[161] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 269; A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 193.

of monitoring and makes a more severe intrusion into the private sphere of the employee possible.[162]

66. In this Section so far, we have established that the employer enjoys a certain level of legitimate interest to monitor the behaviour of his employees. Naturally, this also includes the right to monitor the proper use of the employer's property by the employee, compliance with any internal policies and quality requirements, and to a certain extent, compliance with professional and organizational behaviour standards.[163] It is important that we recognize the legitimate interests that employers have in the employment relationship – legitimate interests that also extend to the processing of personal data accumulated through the monitoring of employees – since it is one of the lawful grounds for processing personal data under the GDPR.[164] As the WP29 stated, "the employer has a legitimate interest in processing personal data of his workers for lawful and legitimate purposes that are necessary for the normal development of the employment relationship and the business operation."[165]

67. All the Member States of the European Union agree that the employment relationship between the employer and the employee is legally to be regarded as a subordinate relationship, by which the employee agrees, via a contract, to perform certain tasks, for certain wage under the authority of the employer.[166] Thus, it is argued, by signing an employment contract, the employee has consented to work under instructions and control of the employer.[167] By entering into an employment relationship, the employee agrees and is prepared to have his or her fundamental rights to privacy and data protection restricted.[168] However, it is important to stress this once again, the employer's right to control and to manage in the employment setting is not an absolute

[162] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 193.
[163] F. HENDRICKX, *Protection of workers' personal data in the European Union, European Commission,* 2002, 97.
[164] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 17.
[165] Article 29 Working Party, WP 48, Opinion 8/2001 on the processing of personal data in the employment context, adopted 13 september 2001, 19, available at: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf* (Accessed 23 April 2019).
[166] F. HENDRICKX, *Protection of workers' personal data in the European Union, European Commission,* 2002, 12-13; M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 17.
[167] P. DE HERT and H. LAMMERANT, "Protection of Personal Data in Work-related Relations", *Study for the CCLS and the CEPS,* 2013, 49-50, available at: *http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-LIBE_ET(2013)474440* (Accessed 25 April 2019)
[168] S. WALLACH, "Who's Info is it Anyway? Employees' Right to Privacy and Protection of Personal Data in the Workplace", *Int'l J. Comp. Lab. L. & Indus. Rel. 23,* 2007, (195) 203.

right.[169] When setting up a system of online employee monitoring, the employer must take into account that even in the employment relationship, an employee still maintains his or her fundamental rights and human dignity, and, in the case of employee monitoring, it would guarantee a certain level of protection for privacy and against wrongful use of personal data.[170]

68. We have established that there are fundamental rights and significant interests on both sides.[171] Consequently, the discourse concerning employee monitoring does not concern itself with the legality of monitoring practices, as employers have an entitlement to certain information for the well-being and efficiency of their companies, but rather with the threshold and severity of the intrusion into the respective fundamental right.[172] The WP29 also identified this aspect in stating that "the question...is never whether data processing at the workplace per se are lawful activities or not. The real question is what are the limits that data protection imposes to such activities or, the other way around, which are the reasons that may justify the collection and further processing of personal data of any given worker."[173] A balance in the enforcement of both colliding fundamental rights and interests must be found and respected during the creation and application of monitoring systems.[174]

69. In the next two sections, I will try to find out how this balancing exercise should be approached in the different phases of the employment relationship and where the thresholds lay in each phase. For this purpose, I will differentiate between the pre-employment screening phase and the employment phase which is then again divided into SNS monitoring inside the workplace and SNS monitoring outside the workplace.

---

[169] [169] P. DE HERT and H. LAMMERANT, "Protection of Personal Data in Work-related Relations", *Study for the CCLS and the CEPS,* 2013, 49-50, available at: *http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-LIBE_ET(2013)474440* (Accessed 25 April 2019).

[170] F. HENDRICKX, *Protection of workers' personal data in the European Union, European Commission,* 2002, 90; M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 18.

[171] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 193.

[172] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 18.

[173] Article 29 Working Party, WP 48, Opinion 8/2001 on the processing of personal data in the employment context, adopted 13 September 2001, 19, available at: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf* (Accessed 25 April 2019).

[174] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 193.

SECTION III. SNS MONITORING BEFORE THE EMPLOYMENT RELATIONSHIP

70. These days, most hiring professionals use SNSs to aide in screening and selecting applicants.[175] This screening procedure affords several benefits to organizations[176]: SNSs provide a readily available public forum to research candidates while incurring minimal cost, allowing even small businesses to engage in such practices. The information on SNSs may provide further evidence related to the veracity of information presented on an applicant's resume (e.g., education and work experience). In addition, potential employers may have access to detailed information that would allow them to draw conclusions or make inferences about the applicant's character or personality that might not be as easily or economically obtained through traditional means.

71. Information on social network sites can both help applicants get hired as well as hinder an applicant from getting hired.[177] Applicants posting inappropriate photographs or information, displaying poor communication skills or revealing information that falsifies qualifications listed in a resumé are all good reasons for employers to not hire an applicant.[178] On the contrary, applicants' profiles may enhance their chances of being hired or selected for consideration by providing supportive evidence of their listed qualifications, portraying a profile indicative of being a good fit with the employer, and displaying creativity and positive communication skills.[179]

72. During the hiring phase, it is a legitimate interest for the employer to want to select the best possible candidate.[180] After all, the employer has the right to decide with whom to contract. If he/she wants to avoid vicarious liability and "negligent hiring" claims, the future employer has to take reasonable action to examine the candidate's background, to gain relevant information, verify documentations.[181] By conducting a SNS background check, the employer can enforce his

[175] V. BROWN and E. VAUGHN, "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions", *Journal of Business and Psychology,* 2011, Vol. 26 (2), (219) 219.
[176] V. BROWN and E. VAUGHN, "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions", *Journal of Business and Psychology,* 2011, Vol. 26 (2), (219) 220.
[177] J. FORD, L. WILLEY, B.J. WHITE and T. DOMAGALSKI, "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethical and Regulatory Issues,* 2015, Vol. 18(1), (51) 54.
[178] R. SPRAGUE, "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship", *University of Louisville Law Review,* 2011, Vol. 50, (1) 6.
[179] V. BROWN and E. VAUGHN, "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions", *Journal of Business and Psychology,* 2011, Vol. 26 (2), (219) 220.
[180] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 271.
[181] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 271; R. SPRAGUE, "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship", *University of Louisville Law Review,* 2011, Vol. 50, (1) 9.

legitimate interest, as information available on SNSs can contribute to making the right hiring decision.[182]

73. Employers who choose to use SNSs as an informal method of predicting applicant employability must consider that this kind of data processing can be potentially damaging for applicants.[183] WP29 confirms in Opinion 2/2017 that the «use of social media by individuals is widespread and it is relatively common for users profiles to be publicly viewable depending on the settings chosen by the account holder».[184] However, the mere fact that an individual's social media profile is publicly viewable does not imply that the potential employer is allowed to process those data for his/her own purposes. Even if employers rely on a legitimate interest as a legal ground for processing, they are «only allowed to collect and process personal data relating to job applicants to the extent that the collection of those data is necessary and relevant to the performance of the job which is being applied for»[185] Opinion 2/2017 further states that data collected during the recruitment process should generally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the individual concerned.[186] The individual must also be correctly informed of any such processing before they engage with the recruitment process (for example in the job advert).[187] A big issue of SNS background checks is that they are invisible. Due to the invisible nature of SNS background checks it is quasi impossible for applicants to prove or even know that a decision made in the hiring phase is based on content found on SNSs.[188] To cope with this challenge and comply with the principle of transparency it is essential that applicants are informed in advance of any online monitoring that will take place.

---

[182] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 193.
[183] V. BROWN and E. VAUGHN, "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions", *Journal of Business and Psychology,* 2011, Vol. 26 (2), (219) 220.
[184] Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, adopted on 8 June 2017, 11, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 26 April 2019).
[185] *Ibid,* p. 11.
[186] In cases where the employer wishes to retain the data with a view to a further job opportunity, the data subject should be informed accordingly and be given the possibility to object to such further processing, in which case it should be deleted.
[187] Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, adopted on 8 June 2017, 11, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 26 April 2019); C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 14.
[188] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 278; A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 197; R. SPRAGUE, "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship", *University of Louisville Law Review,* 2011, Vol. 50, (1) 41.

74. The WP29 in its Opinion clearly refers back to some basic principles of data protection law. On the one side the WP29 holds that employers screening the SNSs of potential employees must keep in mind the data minimisation principle. This principle, which is defined in Article 5(1)(c) of the GDPR, entails the obligation to ensure that personal data are "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Additionally, the employer must adhere to the transparency and storage limitation principles by telling the potential employees when their SNSs will be screened and deleting the gathered information as soon as the storage of the data is no longer necessary for the purposes for which they are processed. In the case of pre-employment screening, the purpose of the data retention disappears as soon as it becomes clear that no job offer will be made or is not accepted by the individual concerned. It is advisable for employers who want to prevent possible lawsuits to have a written policy that specifies what information or sites will be consulted before the decision is made, who will conduct the review and what records will be maintained and for how long.[189] Additionally, throughout the entire recruitment process, employers must always ask themselves if the search they do fulfils the general requirements of data processing (necessity, proportionality, etc.).

75. To sum up, any employer who, during the recruitment of new staff, wants to check the social network profiles of candidates and wants to include information from these network sites (or any other publicly available information) in the screening process may only do so if it is necessary for the job to review information about a candidate on social media[190] and the candidate is made well aware that his SNSs are being screened. Only if these conditions are fulfilled will the employer be able to rely on the legal basis of Article 7(f) to review publicly available information about candidates.

[189] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 278.

[190] For example in order to be able to assess specific risks regarding candidates for a specific function; Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, adopted on 8 June 2017, 11, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 9 June 2019).

SECTION IV. SNS MONITORING DURING THE EMPLOYMENT RELATIONSHIP

§1. During working hours

76. During working hours, the employee has the obligation to perform his work for the employer. Naturally, the employer wants to check whether the persons employed by him are actually performing the work set out by him and whether they perform the work satisfactorily. It follows from the nature of the employment contract that the employer is entitled to monitor whether the employee carries out his/her task and fulfils his/her duties correctly.[191] Employers have to make sure that their company meets certain productivity and profitability standards. In order to reach these goals, it is only natural that the employer wants to control and monitor whether his employees are really working or just spending their time on various SNS.

77. There are several ways for an employer to go about social media monitoring. The chosen scenario will in turn influence the scale of monitoring.

78. Firstly, the employer can resort to a complete block of SNSs in the workplace. While this scenario might seem like a convenient and simple solution for the employer, it might be unrealistic to completely ban the use of SNSs during working hours. Off course, the employer can easily block access to SNSs when employees use the employer's equipment. The WP29 even acknowledges this by emphasising that prevention, i.e. the blocking or banning of certain websites, should be given more weight than detection. These days however, most people have smartphones which they take everywhere, including the workplace, and from which they can easily access a plethora of SNSs. A smartphone mostly goes along with a mobile internet subscription, so the blocking of social network sites by the employer is just practically not an option in these cases. While an employer has the right to regulate and monitor the use of SNSs on his/her own equipment, the scenario is different for devices that are property of the employee.[192] So in the case an employer would instruct a complete ban on SNSs, the employer will be faced with a major enforcement problem as the activity of employees checking their Facebook accounts on their mobile phones can easily stay invisible.

[191] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 194.
[192] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 601.

79. Since a simple block of social media sites seems unrealistic due to the advancement of information communication technologies the employer can also choose not to block SNS but to restrict their usage. This scenario would also seem more in line with ECtHR case law as employee's have the right to private zones at work where they can then technically resort to the usage of SNSs. Nonetheless, in this case as well as in the previous scenario, the employer will benefit from regulating his employee's social media usage and his/her monitoring of that usage in internal social media policies or social media guidelines.[193] These policies that attempt to define the limits of permissible employee online activity and identify forms of impermissible online activity that might expose the organization to legal liability or loss play a key role in compliance with data protection regulation, especially the transparency[194] principle that holds that employers have the obligation to inform employees on the details of the monitoring.[195] I would even argue that social media policies are quintessential for every modern organization. Data protection regulation provides for a plethora of rights data subjects enjoy (e.g. the right to access, right to objection, to rectification, to erasure) when their data is being processed.[196] This participation of the data subject in the processing however presupposes that he/she is aware of the processing, this is where employment policies play an important role.

80. It would be naïve to expect employers not to use SNS monitoring at all as it provides for a cheap, invisible and easy tool of obtaining information. However, employers must also realise that it is in their interest to comply with data protection regulation as non-compliance with the GDPR can result in hefty fines for the organisation involved. A written document containing internal SNS policies can not only help the organisation ensure its compliance with data protection regulation (which in turn protects the organisation against future liability actions of workers), it can also contribute to the prevention of misuse by clarifying the conducts to be followed by employees (by giving clear guidelines on what employees can and cannot say about the organisation).[197]

---

[193] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 38.
[194] Article 12 GDPR.
[195] J. FORD, L. WILLEY, B.J. WHITE and T. DOMAGALSKI, "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethical and Regulatory Issues,* 2015, Vol. 18(1), (51) 52; A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 603.
[196] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 203.
[197] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 277; A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 603.

81. The employer's social media policy needs to be written in a clear and comprehensible manner so that every employee can understand it. The content of these policies will depend on the phase of the employment relationship and the position of the employee within the workplace hierarchy[198]. A one size fits all solution does not exist here. E. KAJTÁR provides some suggestions to make a well-rounded social media policy[199]:[200] The employer has to inform his employees whether the use of social media at the workplace is prohibited. In case it is allowed, the employer must provide guidelines on the limits of social media usage in the workplace (e.g. time limits on daily use). Employers should give clear examples of what will be regarded as gross misconduct (e.g. posting derogatory or offensive comments on the internet about the company or a work colleague) and provide information about the possible consequences. To support this, it is advisable for the employer to define what he considers responsible, "normal" use of social media (he can reference bullying and harassment policies to support what is seen as acceptable behaviour). This policy should also include a notice on how and what kind of monitoring takes place and how frequently the internet use will be monitored. An employer should however definitely refrain from constant and systematic monitoring of employees as this will certainly be regarded as disproportionate and lead to an infringement of data protection rules (which can in turn lead to liability of the organisation).

82. When drafting these policies, employers should make sure that employees are involved in the process and that a continuous dialogue with the social partners is achieved.[201] Additionally, successful organisations regularly update their policies and review the enforcement of those policies to ensure that they remain in compliance of data protection regulation.[202]

83. In addition to the use of policies, employers who want to resort to employee monitoring can, and, in case employee communications will be directly monitored, must, undertake a DPIA prior to the introduction of any monitoring technology to decide whether and how to conduct monitoring. The assessment that was explained above (*supra* p. 22 ff.) should "include identifying the purposes of the monitoring, weighing the possible adverse effects, taking into consideration

[198] As a "higher-up" will likely enjoy a higher level of autonomy in relation to internet use.
[199] E. KAJTÁR refers to the guidelines offered by the ACAS, a non-departmental public body of the Government of the United Kingdom whose purpose it is to improve organisations and working life through the promotion and facilitation of strong industrial relations practice.
[200] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 277.
[201] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 277.
[202] J. FORD, L. WILLEY, B.J. WHITE and T. DOMAGALSKI, "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethical and Regulatory Issues,* 2015, Vol. 18(1), (51) 52.

alternatives, considering how the employer will comply with the data protection obligations arising from the monitoring and considering whether the monitoring is truly justified.[203] This DPIA obligation exemplifies the principle of data protection *by design* which holds that already when planning and implementing a system of data processing must the controller "implement appropriate technical and organisational safeguards […] in order to meet the requirements of the GDPR and protect data subjects' rights.[204]

84. **CONCLUSION.** During the employment relationship and within working hours, the employer has the right to decide whether he/she allows employees to check their personal social media accounts and can monitor whether employees respect that decision or not.[205] Employers that want to be in compliance with data protection regulation (which they should since they can incur hefty fines if they are not) should put some thought into employment policies prior to the monitoring. Social media policies can be a great way for employers to inform employees about the extent of their allowed social media usage during working hours and the way this will be monitored. It is evident that under the current data protection regime a system of constant and systematic monitoring cannot be justified as it is clearly disproportionate. I share E. KAJTÁR'S opinion that the use of SNSs during working time in itself may only serve as ground for dismissal if the employer previously explicitly notified the employee that these activities are prohibited or restricted and the nature of the work as well as the content of the action justifies such a prohibition.[206] Therefore, *a contrario*, if the employee was not notified in advance of any prohibition or restriction on the usage of SNSs during working hours, the employee's actual access of SNSs during working hours cannot serve as a basis for dismissal.

85. The appearance of mobile smart devices raises some new challenges as employers are simply practically unable to monitor these devices, even during working hours.[207] Even if they were able to monitor these private devices, for example by deploying software packages, a whole new lane of data protection issues would open up as the processing involved in these technologies cannot

[203] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 203-204.
[204] Article 25 (1) GDPR.
[205] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 605.
[206] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 277.
[207] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 605.

distinguish between private and business use of the device and will therefore most certainly be regarded as disproportionate. It is then very unlikely to have a legal ground under legitimate interest.[208] The excessive use of these mobile smart devices, which are seemingly exempt from the employer's monitoring could lead to a loss in productivity and working time and therefore have a negative impact on the employer and his/her organisation. The question on how this challenge will be tackled by legislation in the future remains open, that there is a need for it is not.

§2. Outside the workplace and beyond working hours

86. According to A. LUKÁCS, the great novelty of SNSs is that they make it possible to monitor the activities employees conducted outside the workplace and beyond working hours.[209] The employer, due to the employment contract, gains the right to monitor whether the work he instructs the employer to do is actually being performed. What happens outside of the workplace has historically been outside the purview of the employer. In Section II of this Chapter we have established that these days the employer can be subject to reversed vulnerability. By (ab)using their social media, employees can do a lot of damage to the employer's reputation which, due to the long-lasting nature of content on the internet, can cause issues for the employer's image even long after the content is not relevant anymore. That the open nature of SNSs can make a negative or false comment quickly available to millions of people, hereby causing serious harm to the employer's reputation, was acknowledged by the sub district court in Arnhem[210] (so called "Blokker" case) that held that a message posted on Facebook, even on a private profile, can be "retweeted" by so called 'friends' and therefore end up in the public domain. The court effectively pointed out the relativeness of the private nature of Facebook.[211]

87. Until now we have looked at social media usage either prior to the working relationship or during the working relationship but within working hours. Outside of the workplace, the employee's privacy rights regain their full potential. Although the employer has a legitimate interest in collecting an employees' personal data, the problem with new monitoring techniques is that such practices are no longer contained to the work environment but are now also being applied to the

[208] C. OGRISEG, "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, (1) 16-17.
[209] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 195.
[210] Kantonrechter Arnhem 19 march 2012, *LJN BV* 9483.
[211] *https://leidenlawblog.nl/articles/think-before-you-post*.

'online' world, albeit in the employment context.[212] The question must then be raised whether the employer's legitimate interest to monitor his employees also resorts to postings made outside the workplace.

88. Monitoring of employee's usage of SNSs outside the workplace and beyond working hours makes for a more severe intrusion into private sphere. Whereas the balancing exercise of rights and interests involved weighs somewhat in favour of the employer during the working hours as employees are under an obligation to perform the work, the pendulum should swing more towards the employees' side when it comes to employee monitoring outside the workplace. The employer can for obvious reasons not rely on the purpose of ensuring employee productivity to monitor their employee's social media sites outside the workplace. What we see in practice is that the employers monitor their employee's SNSs beyond working hours for the purpose of reducing the risk of reputational loss for the organisation. While this is a legitimate reason for monitoring employees, in this stage of the employment relationship, the threshold for employee monitoring should be much higher.

89. At this point I would like to refer back to the sub district court's decision in the Blokker case. This case is very interesting as it shows the attitude of courts towards SNSs. The court ruled that the word "friend" on Facebook is a relative value. The conclusion to be drawn from this case is that on the internet, even on pages that are accessible only by a selected audience, privacy is of a relative value. The court held that employees need to be aware that their remarks might reach a wider audience than they intended.[213] The same line of legal reasoning can be found in Germany. The Higher Labour Court in Hamm[214] qualified a negative message about the employer as a relevant offence and emphasised that the use of Facebook made the comment available to the public. If we accept that everything that is posted online, no matter the privacy settings, is likely to end up in the public domain and therefore not protected by privacy anymore I fear we are moving towards dangerous turf. I fully join A. LUKÁCS' opinion that if we accept SNSs as the new form of communication and self-expression, we cannot automatically say that the user himself/herself contributes to the destruction of his/her own privacy.[215] Although it is often the

[212] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 5.
[213] *https://leidenlawblog.nl/articles/think-before-you-post*.
[214] Verdict by the Higher Labour Court Hamm 10 October 2012, 3 Sa 644/12.
[215] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 189.

employee who decides to share his/her personal data on SNSs, this does not mean that he/she consented to the free processing of that data.[216]

90. Even if we consider that information that was provided on SNSs relating to a specific individual is to be regarded as publicly available information[217], this information still constitutes personal data under art. 4 (1) of the GDPR and is therefore protected by privacy regulation. Data protection principles were introduced as safeguards against overly intrusive monitoring procedures and the expansion of the employer's right to control vis-à-vis an employee's privacy rights.[218] Taking into account how severly one post can harm the employer's reputation and economic interests, during the working relationship, the employer is entitled to restrict the employee's conduct on SNSs and has the right to control whether the employee complies, even after working hours.[219] However, the restriction and monitoring cannot be limitless. The employer is obliged to respect the data protection requirements (i.e. necessity, proportionality) and other rights (e.g. the right to freedom of expression).[220] It is thus advisable, for the employer to be in line with data protection regulation, to lay down conditions on SNS monitoring outside the working hours in a SNS policy as well. The legitimate interests of an employer can justify certain limitation to the privacy of employees, however such justifications can never trump over data protection principles.[221] The right balance of rights and interests here depends on the degree of harm to the employer, the potential size of the audience, the method of communication and finally the relationship between the employee and the audience.[222]

91. To end this Chapter I would like to quickly address the employees. We have discovered that employees are entitled to privacy protection not only under European data protection legislation but also under international fundamental rights. However, for an employee to have the mindset that everything that is posted on social media is protected from his/her employer is just foolish.

---

[216] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 204.
[217] According to M. SIEMENS, publicly available information is interpreted to mean any information that is readily available on web pages to the ordinary Internet user, without the impediment of passwords, pay-walls or subscriptions and memberships. Basically any information that can be readable following an Internet search or upon accessing a specific website.
[218] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 21.
[219] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 206.
[220] A. LUKÁCS, "To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, (185) 206.
[221] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 35.
[222] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 275.

Unfortunately, I still come across this mindset way too often. Even with a decent data protection framework in place, employers can resort to covert monitoring techniques and the employee would never even know that he is being monitored. I think it is important that the employee considers that things they wouldn't tell someone to their face are sometimes best left unsaid on the internet too.

CONCLUSION

92. The aim of this paper was to examine what data protection rules are applicable to the monitoring of social networking sites in the employment context. As social networking sites have become omnipresent, we have to accept that their usage can have serious implications for the employment relationship as well. Although more and more legal articles address these issues, we have not yet managed in stating a set of particular uniform rules for workers' data protection across the entire EU.[223]

93. It was argued that the General Data Protection Regulation provides data subjects, i.e. employees, with rights and that these rights can also be used in the employment context to protect an employee's informational privacy. However, it was also recognised that an employee cannot fully enjoy his/her privacy rights due to the nature of an employment contract. The employee's rights must be balanced and weighed against the legitimate interest of the employer to manage his/her business, including the right to conduct monitoring on employees.[224] The General Data Protection Regulation provides a viable tool to balance the interests of employers and employees[225] but the balancing exercise is different depending on the phase of the employment relationship.

94. If the employer wants to check the social network profiles of candidates during the recruitment phase and he/she wants to include information from these network sites in the screening process, he/she may only do so if it is necessary for the job to review information about a candidate on social media[226] and the candidate is made well aware that his SNS are being screened. Only if these conditions are fulfilled will the employer be able to rely on the legal basis of Article 7(f) to review publicly available information about candidates.

95. During the employment relationship the employer has the right to decide whether he/she allows employees to check their personal social media accounts and can monitor whether employees

[223] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 604.
[224] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 40.
[225] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 33.
[226] For example in order to be able to assess specific risks regarding candidates for a specific function; Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, adopted on 8 June 2017, 11, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169* (Accessed 9 June 2019).

respect that decision or not.[227] Employers that want to be in compliance with data protection regulation should put some thought into employment policies prior to commencing the monitoring as they can be a great way for employers to inform employees about the extent of their allowed social media usage during working hours and the way this will be monitored. Transparency is a very important requirement under the current data protection regime.

96. The employer does even have a legitimate interest to monitor his/her employees' social media after working hours as what they post can directly affect the employer's image. The right balance here depends on the degree of harm encountered by the employer, the potential size of the audience and the method of communication used by the employee. There is no one size fits all solution and a reasonable employer who wants to avoid liability under data protection legislation should include clear and comprehensible rules on social network site monitoring beyond working hours in SNS policies.

97. E. KAJTÁR described social media as a double-edged sword.[228] On the one side it undeniably provides for new and effective ways to communicate. This can also benefit employers as many firms these days advertise their products on social media. On the other side, there is clearly a dark side to social media as well. All these new communication technologies make it easy to access large quantities of personal information. They provide the employer with additional opportunities to monitor and inspect the employees' conduct. The main question of this paper was whether, and if so, how, the existing data protection framework deals with the problem of social media usage prior and during the employment relationship. This paper has established that the rules of privacy and data protection can adequately be applied to the employment relationship. However, as it was noted in the beginning, there is no specific legal document regulating data protection in this context. Especially with regards to employer social network site monitoring this feels like a legislative gap. In my opinion, both the employer as well as the employee would benefit from such a specific legal document as it will clearly establish a clear standard delineating the expectations of both employees and employers on the issue of electronic monitoring.[229] Whether the european legislator will ever fill this void remains to be seen.

---

[227] A. LUKÁCS, "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, (593) 605.
[228] E. KAJTÁR, "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), (268) 278-279.
[229] M. SIEMENS, "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 20.

LIST OF REFERENCES

LEGISLATION

Charter of Fundamental Rights of the European Union, 2012/C 326/02, available at: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT*.

Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome, 4 November 1950.

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), 2016, *OJ* L199, 1-88.

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. L 281*, 1995, available at *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*.

CASE LAW

ECtHR 5 September 2017, nr. 61496/08, *Bărbulescu v. Romania*.

ECtHR 16 December 1992, nr. 13710/88, *Niemietz v. Germany.*

ECJ 29 Januari 2008, *Productores de Música de España (Promusicae) v. Telefónica de España SAU,* C-275/06.

Volkszählungsurteil (BVferG), 15 December 1983, 1 bVr 209/83.

Arbh. Brussel 3 September 2013, nr. 2012/AB/104, *Juristenkrant* 2013, afl. 278, 6; *JTT* 2013, afl. 1173, 497; *Ors.* 2014, afl. 3, 20; *Or.* 2013, afl. 9, 231; *Rev.trim.dr.fam.* 2014, afl. 3, 711; *RW* 2013-14, afl. 40, 1586.

Higher Labour Court Hamm 10 October 2012, 3 Sa 644/12.

Kantonrechter Arnhem 19 march 2012, *LJN BV* 9483.

JURISPRUDENCE

ARTICLES

ABRIL, P.S., LEVIN, A. and DEL RIEGO, A., "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee", *American Business Law Journal,* Vol. 49, 2012, 63-124.

ALNEMR, R., CAYIRCI, E., DALLA CORTE, L., GARAGA, A., LEENES, R., MHUNGU, R., PEARSON, S., REED, C., SANTANA DE OLIVEIRA, A., STEFANATOU, D., TETRIMIDA, K. and VRANAKI, A., "A Data Protection Impact Assessment Methodology for Cloud", *Lecture Notes in Computer Science,* 2016, Vol. 9484, 60-92.

BERNING, B. and KEPPELER, L., "Datenschutz im Konzern"*, HMD Praxis der Wirtschaftsinformatik*, 2017, 1021-1037.

BIEKER, F., FRIEDEWALD, M., HANSEN, M., OBERSTELLER, H. and ROST, M., "A process for data protection impact assessment under the European General Data Protection Regulation", *Lecture Notes in Computer Science,* 2016, Vol. 9857, 21-37.

BROWN, V. and VAUGHN, E., "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions", *Journal of Business and Psychology,* 2011, Vol. 26 (2), 219-225.

DE HERT, P. and LAMMERANT, H., "Protection of Personal Data in Work-related Relations", *Study for the CCLS and the CEPS,* 2013, 1-73, available at: *http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-LIBE_ET(2013)474440*.

DUVENHAGE, J.C., "Social media in the workplace: Legal challenges for employers and employees", *Masterthesis,* University of Notre Dame Australia, 2017, *https://researchonline.nd.edu.au/theses/164/*, 1-248.

EIVAZI, K., "Computer use monitoring and privacy at work", *Computer Law and Security Review: The International Journal of Technology and Practice,* Vol 27(5), 2011, 516-523.

FARAHBAKHSH, R., XIAO, H., CUEVAS, A. and CRESPI, N., "Analysis of publicly disclosed information in Facebook profiles", *2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,* 2013, 699-705.

FIRE, M. and PUZIS, R., "Organization Mining Using Online Social Networks", *Networks and Spatial Economics,* 2016, Vol. 16(2), 545-578.

FIRE, M., PUZIS, R. and ELOVICI, Y., "Organization Mining Using Online Social Networks", *Networks and Spatial Economics,* 2013, 1-23.

FORD, J., WILLEY, L., WHITE, B.J. and DOMAGALSKI, T., "New concerns in electronic employee monitoring: Have you checked your policies lately?", *Journal of Legal, Ethic al and Regulatory Issues,* 2015, Vol. 18(1), 51-70.

GOMES DE ANDRADE, N.N. and MONTELEONE, S., "Digital natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications" in GUTWIRTH, S., LEENES, R., DE HERT, P. and POULLET, Y. (eds.), *European Data Protection: Coming of Age*, *Springer Dordrecht*, 2013, 119-144.

IRETON, J., "Social Media: What Control Do Employers Have Over Employee Social Media Activity in the Workplace?", *Houston Business and Tax Law Journal,* 2014, 144-178.

KAJTÁR, E., "Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship", *Acta Juridica Hungarica,* 2015, Vol. 56 (4), 268-280.

KEANE, E., "The GDPR and Employee's Privacy: Much Ado but Nothing New", *King's Law Journal*, 2018, Vol. 29(3), 354-363.

KOTSIOS, A., MAGNANI, M., ROSSI, L., SHKLOVSKI, I. and VEGA, D., "An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research", *Cornell University Journal,* 2019, 1-23.

KUSS, D.J. and GRIFFITHS, M.D., "Online Social Networking and Addiction – A Review of the Psychological Literature", *Int.J.Environ.Res.Public Health* 2011, 3528-3552.

LASPROGATA, G., KING, N.J. and PILLAY, S., "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of

Data Privacy Legislation in the European Union, United States and Canada", *Stand.Tech.L.Rev.4,* 2004, 1-46.

LUKÁCS, A., "To Post, Or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection", *Masaryk University Journal of Law and Technology,* 2017, 185-214.

LUKÁCS, A., "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" in L. STAJID (ed.), *Harmonisation of Serbian and Hungarian Law with the European Union Law: Thematic Collection of Papers,* Novi Sad, 2017, 593-606.

MASSIMINO, B., "Accessing Online Data: Web-Crawling and Information Scraping Techniques to Automate the Assembly of Research Data.", *Journal of Business Logistics,* 2016, 34-42.

OGRISEG, C., "GDPR and personal data protection in the employment context", Labour & Law Issues, Milan, 2017, 1-24.

OLSOVSKÁ, A and SVEC, M., "How To Monitor Employees But Protect Employee Privacy?", *Silesian Journal of Legal Studies,* 2016, 81-91.

PERAS, D., MEKOVEC, R. and PICEK, R., "Influence of GDPR on social networks used by omnichannel contact center", *MIPRO* 2018, Opatija, 1132-1137.

POHLE, J. (ed.), "Data Privacy Legislation in the EU Member States – Part Two of the Practical Overview. How EU Member States have adjusted their domestic data privacy law to the GDPR – Update", *Computer Law Review International,* 2018, 133-147.

PURTOVA, N., "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights"*, Netherlands Quarterly of Human Rights,* 28 (2), 2010, 179-198.

SARRAT, J. and BRUN, R., "DPIA: How to carry out one of the key principles of accountability", *Lecture Notes in Computer Science,* 2018, Vol. 11079, 172-182.

SIEMENS, M., "Employee monitoring: crawling publicly available information", *Masterthesis K.U.Leuven,* 2017-18, 1-44.

SILVERMAN, M., BAKHSHALIAN, E. and HILLMAN, L., "Social Media and Employee Voice: The Current Landscape", *CIPD Research Report, https://www.cipd.co.uk/knowledge/work/technology/employee-voice-report,* 2013, 1-27.

SPRAGUE, R., "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship", *University of Louisville Law Review,* 2011, Vol. 50, 1-42.

STERLING, N.L. and FEDELES, E.R., "Introductory note to Barbulescu v. Romania (Eur. Ct. H.R.)", *International Legal Matters*, 2018, 80-124.

VAN DER SYPE, Y., "De gegevensbeschermingseffectbeoordeling voor de verwerking van werknemersgegevens, *Or.* 2018, afl 1, 2-11.

VANDE VORST, C. en VAN GOETHEM, L., "Wanneer is het verplicht om een gegevensbeschermingseffectbeoordeling uit te voeren?", *TPP* 2018, afl. 1, 14-19.

WALLACH, S., "Who's Info is it Anyway? Employees' Right to Privacy and Protection of Personal Data in the Workplace", *Int'l J. Comp. Lab. L. & Indus. Rel. 23,* 2007, 195-226.

ONLINE SOURCES:

Statista, *Number of Social Media Users Worldwide From 2010 to 2020* (2016), *https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/*.

Https://strasbourgobservers.com/2017/10/19/barbulescu-v-romania-and-workplace-privacy-is-the-grand-chambers-judgment-a-reason-to-celebrate/.

Article 29 Working Party, Opinion 2/2017 on Data Processing at Work, adopted on 8 June 2017, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169*.

Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, wp248rev.01, adopted on 4 April 2017, available at: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169*.

Article 29 Working Party, WP 163, Opinion 5/2009 on Online Social Networking, adopted on 12 June 2009, available at: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf*.

Article 29 Working Party, WP 48, Opinion 8/2001 on the processing of personal data in the employment context, adopted 13 September 2001, available at: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf*.

BOOKS

ARANY-TÓTH, M., *Arbeitnehmerdatenschutz in Ungarn im Rahmen des europäischen Datenschutzrechts, Peter Lang,* Frankfurt am Main, 2011, 291 p.

HENDRICKX, F., *Protection of workers' personal data in the European Union, European Commission,* 2002, 122 p.

HONEYBALL, S., *Honeyball & Bowers' Textbook on Employment Law, Oxford University Press*, Oxford, 2008, 468 p.

KRZYSZTOFEK, M., *Post-reform personal data protection in the European Union: General Data Protection Regulation (EU) 2016/679, Wolters Kluwer,* Alphen aan den Rijn, 2017, 255 p.

OTTO, M., *The Right to Privacy in Employment: A Comparative Analysis, Hart Publishing,* Portland, 2016, 221 p.