THESES OF THE DOCTORAL DISSERTATION

PROTECTION OF EMPLOYEES' RIGHT TO PRIVACY AND RIGHT TO DATA PROTECTION ON SOCIAL NETWORK SITES – WITH SPECIAL REGARD TO FRANCE AND HUNGARY

2020

Adrienn LUKÁCS

Supervisors
Dr. habil. Francis KESSLER, associate professor
Dr. habil. József HAJDÚ, professor

Joint PhD between
University Paris 1 Panthéon Sorbonne and
University of Szeged, Faculty of Law and Political Sciences

TABLE OF CONTENT

I. Introduction and background of the dissertation 3

I. 1. Exploring the research problem 3

I. 2. Scope and objectives of the research 5

I. 3. Applied methods and sources of research 7

II. Main elements of the dissertation 8

II. 1. Theses 8

II. 2. Structure of the dissertation 10

II. 3. Conclusions and *de lege ferenda* suggestions 11

II. 3. 1. Findings 11

II. 3. 2. Recommendations and *de lege ferenda* suggestions 13

III. Scientific output related to the research topic 16

III. 1. Publications 16

III. 2. Presentations 18

I. INTRODUCTION AND BACKGROUND OF THE DISSERTATION

New information and communications technologies are fundamentally shaping everyday life in the 21st century – including the world of work as well.[1] Innovations, such as personal computers, Internet, e-mail, blogs or social network sites essentially influence and transform the way individuals live their lives – together with working, creating new challenges for labour market participants. These challenges can relate to a number of matters, such as the arrangement of working time, occupational health and safety, organisation of work or – most important for the dissertation – controlling and monitoring employees.

As part of information and communications technologies, *online social network sites* (hereinafter referred to as: SNSs) have caused profound changes through shaking up the previously existing forms of communication and self-expression. SNSs are gaining growing importance in individuals' everyday lives, and have become an integral part of it. Today the most popular SNSs have millions of users worldwide.[2] There exist hundreds of different international and national (social media) and SNSs[3] and during the use of such services, the personal data of individuals (and of employees, amongst the users) become publicly available in a quantity and quality never experienced before, on a global scale,[4] which results in the appreciation of the examination of their right to privacy and right to data protection.

I. 1. Exploring the research problem

The starting point of the research was the collision of the employees' and employer's rights: when it comes to employee monitoring, the fundamental legal challenge that arises is the collision of the employer's and the employees' rights. On the one side, there are the

[1] Rey, B. (2013) 'La vie privée au travail. Retour sur la place du privé en contexte hiérarchique à l'ère du numérique', *Les Cahiers du numérique*, 9(2), p. 108.

[2] For example, as of October 2018, Facebook had 2.2 billion users, YouTube 1.9 billion, Instagram 1 billion. Source: *Most famous social network sites worldwide as of October 2018, ranked by number of active users (in millions)* (2018) *Statista*. Available at: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed: 4 January 2018).

[3] For an illustrative list of the most popular SNSs, see more in: Mehra, G. (2017) *105 Leading Social Networks Worldwide*, *PracticalEcommerce*. Available at: https://www.practicalecommerce.com/105-leading-social-networks-worldwide (Accessed: 4 January 2019)

[4] International Working Group on Data Protection in Telecommunications (2008) *Report and Guidance on Privacy in Social Network Services – "Rome Memorandum"* -. 675.36.5. Rome. p. 10.

employees' rights (especially the right to privacy and the right to data protection), while on the other side the employer's rights can be found (e. g. right to reputation, protection of business secrets, protection of legitimate economic interests, etc.), manifested in the employer's right to control and to monitor. No right is absolute; they must be carefully weighed against each other in order to find a proper balance between the two sides.[5]

The respect of employees' rights when applying "traditional forms of monitoring" (such as, for example, CCTV surveillance, geo-localisation, monitoring of telephone use and computer/e-mail use) is already regulated both at international and national levels. However, technological development has a huge effect on the already established regulations, as employee misconducts can have more serious consequences, and the employer's intrusion into employees' personal lives can also be deeper.[6] For example, new ways of monitoring – such as obtaining information through SNSs – can even go beyond the physical workplace and enable the employer to try to monitor activity taking place outside the workplace. As regards how to apply the already existing rules to SNSs, several questions were raised, which the dissertation aimed to answer.

However, specific privacy and data protection challenges brought by SNSs are not (yet) addressed in an exhaustive manner (neither in France, nor in Hungary). Although existing case law (especially in France), the practice of the data protection authorities and a number of existing legal articles already examined SNSs in the context of employment, usually they concentrate on one or two aspects of the subject, thus its *exhaustive* analysis is yet to be elaborated. This is *one of* the voids that the dissertation aims to fill, by addressing this question through the examination of the conclusion, management and termination of the employment relationship, by addressing pre-employment, SNS use at the expense of working hours and employees' presence on SNSs. *The other* specific feature of the dissertation is that it adopts a comparative approach and co-examines France and Hungary, providing a currently non-existent angle of examination of the subject.

[5] Hajdú, J. (2005) *A munkavállalók személyiségi jogainak védelme*. Szeged: Pólay Elemér Alapítvány, p. 20.
[6] Michel, S. (2018) 'TIC et protection de la vie privée du salarié', *Bulletin Joly Travail*, (2), p. 149.

I. 2. Scope and objectives of the research

Regarding the *material scope*, the dissertation will focus on the collision between the employees' rights and the employer's rights and will analyse the two sides. *On the one hand*, the employee is entitled to the right to privacy and the right to data protection during controlling and monitoring.[7] *On the other hand*, it is inherent to the employment contract that the employer has the power/right to control and monitor[8] employees' activities in order to enforce different rights.[9] These rights are manifested in different dimensions: e. g. choosing the most adequate candidate during recruitment, monitoring whether the employee truly spends working hours working or controlling and monitoring that the employee does not violate the employer's right to reputation, etc. The rights of the employee and the employer are in close interaction, as what is a right on one side is manifested as an obligation on the other side (e. g. employees' obligation to perform work, obligation of loyalty, obligation to respect business secrets, etc.).[10] Therefore, there is a collision between the employer's and the employees' rights, and the task of the law is to weigh the two sides and to find an appropriate balance between them. As it was already mentioned, this balance is established in the case of "traditional" forms of monitoring but is yet to be determined in the case of SNSs.

Because of their more personal nature in comparison to social media, the thesis will focus on SNSs, although social media will not be completely excluded from the discussion considering the fact that they also constitute platforms used in the course of the private life of the employee. As the main focus is on the examination of the right to respect for private life and right to personal data protection, the dissertation will address the subject of how employees can use these platforms *in the course of their private lives* and whether/to what extent this use might be controlled or monitored. The dissertation aims to exhaustively address the employment context, through the examination of SNSs and employees' right to privacy and

[7] Hendrickx, F. (2002) 'Protection of workers' personal data in the European Union, Two studies'. EC, pp. 23-24.
[8] In French law it is called "pouvoir" meaning power, while in Hungarian doctrine the expression "jog" meaning right is used.
[9] Blanpain, R. (2002) 'Employment and Labour Law Aspects. Setting the Scene. Asking the Right Questions?', in Blanpain, R. (ed.) *On-line Rights for Employees in the Information Society. Use and Monitoring of E-mail and Internet at Work*. The Hague: Kluwer Law International, p. 43-44.
[10] Gyulavári, T. (ed.) (2017) *Munkajog*. ELTE Eötvös Kiadó. Budapest. p. 235.; Breznay, T. (ed.) (2006) *A munkajog nagy kézikönyve.* Budapest: Complex Kiadó, p. 329.

right to data protection during the conclusion, management and termination of the employment relationship.

The dissertation will focus on the *private sector* employment law. The dissertation will focus on *individual labour law*, as the aim is to analyse the employee's right to privacy and right to data protection, which are individually enforceable, while the use of SNSs as a collective mostly raises questions in relation to collective enforcement of interest and not in relation to the boundaries and respect of the right to privacy.[11]

While keeping in mind that the examined phenomenon is universal in societies where SNSs are available,[12] the *examination will focus on the jurisdictions* of France and Hungary. The aim of examining two jurisdictions is to identify separate or common good practices, as well as to introduce the jurisdiction of both countries for research, legislative and teaching reasons.

The dissertation *aims* to answer the overarching question – in the light of employees' right to privacy and right to data protection – whether the employer is entitled to control and/or monitor employees' activities on SNSs during the different phases of the employment relationship, and if yes, to what extent. The dissertation aims to provide answers to questions in relation to how the existing rules[13] of control and monitoring should be applied to the case of SNSs, such as what the conditions of such monitoring are, what data protection requirements the employer must respect and how, what legal risks arise in relation to such monitoring, etc.

[11] On issues related to the era and collective labour law, see especially: Larher, Y.-M. (2017) *Les relations numériques de travail*. Doctoral dissertation. Université Paris 2 Panthéon-Assas; or: Ray, J.-E. (2007) 'Droit du travail et TIC (III). Droit syndical et TIC : sites, blogs, messagerie', *Droit social*, (4), pp. 423–444.; Ray, J.-E. (2009) 'Actualité des TIC. Rapports collectifs de travail', *Droit social*, (1), pp. 22–37.; Ray, J.-E. (2012) 'CGT, CFDT, CNT, CE et TIC. Rapports collectifs de travail et nouvelles technologies de l'information et de la communication', *Droit social*, (4), pp. 362–372.

[12] Which is supported by the fact that, as these platforms are used worldwide, cases related to SNSs and employment emerge in most of the advanced countries. For an extensive presentation of issues relating to the subject, see more in: Lambert, P. (2014) *International Handbook of Social Media Laws.* Haywards Heath: Bloomsbury.

[13] Laid down in the labour codes, or elaborated by case law, by doctrine or by the practice of the data protection authorities.

I. 3. Applied methods and sources of research

Although it does not constitute a research methodology in the traditional sense, the whole research was permeated by the specific construction in the framework of which the dissertation was completed. Namely, the dissertation was prepared in the frame of a joint PhD program between the University of Szeged and University Paris 1 Panthéon Sorbonne.

The research is based on a mixture of descriptive-analytical methods, as the dissertation systematically examines the existing legal framework while it also contains the critical evaluation of the relevant legislation, court decisions, soft law documents or academic literature. The primary *sources of the research* were international, European (EU and Council of Europe), French and Hungarian legislation, jurisdictions and doctrine. Amongst the secondary sources a wide range of publications was used, especially focusing on – but not limited to[14] – the works of French and Hungarian scholars. Also, brief outlooks to other European or international cases and proposed solutions will be made in order to enrich the research. As the examined phenomenon is universal, in order to raise awareness to certain universal aspects of the subject, these sources will be referred to as well – while keeping France and Hungary in the focus of the dissertation.

When examining these norms, throughout the dissertation several criteria will be taken into consideration and followed when determining the order of discussion. Usually the analysis of a sub-topic will start from the international (universal, regional) norms before focusing on national ones. Also, first general matters will be discussed before examining more specific ones. The analysis will also move from the analysis of the legal framework to existing jurisprudence and existing practice of the data protection authorities or other authorities.

I concluded my research on 10th January 2020, thus subsequent changes in legal regulations, publication of new research papers, their evaluation and analysis can only be subjects of further research.

[14] The dissertation also contains sources in English from several authors outside these two countries, especially from Europe and the United States, as the examined phenomenon is universal.

II. MAIN ELEMENTS OF THE DISSERTATION

II. 1. Theses

The dissertation contains 4 hypotheses: one "general" hypothesis, and then a hypothesis for each significant examined area of the research topic.

(1) *Hypothesis 1* holds that in the case of SNSs, the collision between the employees' rights and the employer's rights appears in a more intense form compared to the "traditional" methods of employee monitoring.

To address Hypothesis 1, particularly the following questions had to be analysed and answered in the dissertation:

- What are the rights arising on the employee's and employer's sides?
- How can the employees' private lives be challenged? What are the rights aiming to protect them and how can they be delimited?
- What does (the right to) privacy mean in the context of online SNSs?
- How are these existing rights challenged by SNSs?

(2) *Hypothesis 2* holds that in the phase of recruitment, the protection of job applicants' rights can be better ensured through *regulating* pre-employment SNS screenings instead of prohibiting them. Due to the difficulties in enforcing the ban (especially the invisibility of background checks), the introduction of more flexible rules would be preferable. This would (also) aim to make employers recognize that compliance with data protection requirements results in more reliable decision-making. This would make it possible to protect the rights of jobseekers more effectively.

To address Hypothesis 2, particularly the following questions had to be analysed and answered in the dissertation:

- Is it reasonable to impose a ban on online searches?
- Can an employer google job applicants, or can he/she consult their social media profiles? If yes, with what conditions?

- What data protection principles and requirements are considerably challenged in the course of such searches?

(3) *Hypothesis* 3 intends to prove that *in most regards*, the personal use of SNSs during working hours can be adequately addressed through the already existing rules relating to the monitoring of Internet and e-mail use, as all of them are Internet based. The main reason for this is that social network sites are web-based platforms as well.

To address Hypothesis 3, particularly the following questions had to be analysed and answered in the dissertation:

- Can the employer completely prohibit the personal use of SNSs during working hours?
- To what extent can the employer monitor compliance with the rules relating to the personal use of the equipment provided by him/her?
- What factors should the employer consider when it comes to sanctioning prohibited personal use?
- What are the specific challenges raised by SNSs compared to the personal use of Internet and e-mail?

(4) *Hypothesis 4* aims to prove that as regards employees' activities and presence on SNSs[15] mainly beyond working hours, in the light of the intensification that SNSs brought to the collision of rights, employers have found themselves in an *even more* vulnerable position, rendering it necessary to tilt the balance towards the protection of employer's rights.

To address Hypothesis 4, particularly the following questions had to be analysed and answered in the dissertation:

- With regard to the blurred boundaries: to what extent can professional life flow into the personal life of the employee?
- Are SNSs considered to be public or private platforms?
- Can SNSs constitute a reason for the termination of employment and if yes, with what conditions?
- Can the use of SNSs beyond working hours be prohibited?

[15] For example, through posting, sharing, liking either matters directly relating to the workplace (e.g. opinion on or criticism of the employer) or matters indirectly relating to the workplace (e.g. posting racist content, etc.).

- In what regards can the employee's online behavior be limited?

II. 2. Structure of the dissertation

As regards the *structure*, the dissertation is composed of two Parts: Part I. analyses the collision of the rights, while Part II. focuses on how this collision is manifested particularly in the context of SNSs.

Part I. will examine the collision of rights in detail, through analyzing the colliding rights both on the side of the employee and the employer and will address how this collision is influenced by the innovations of ICT. Part I. provides the conceptual and theoretical background of the research. More precisely, *first*, Part I. will address the conceptual fundaments of the two sides of the collision: the right to respect for private life, right to data protection and employee monitoring and then, *second*, it will examine how this collision has become more intense, and how the boundaries of work and private life have become increasingly blurred due to ICT, notably to SNSs.

After addressing the conceptual and theoretical foundations, *Part II.* will especially focus on this collision in relation to SNSs and will analyse French and Hungarian law regulating the right to privacy and right to data protection during the controlling and monitoring of the use of SNSs in the employment context. Part II. identifies the main areas where specific challenges arise regarding employee control and monitoring and SNSs, aiming to provide an extensive analysis covering the conclusion, management and termination of the employment relationship. Three subjects are examined in detail:

1. recruitment and the protection of prospective employees' rights,

2. SNS use at the expense of working hours and

3. employees' presence and activity on SNSs.

It will be explored, in the light of the collision of rights and interests presented in Part I., where exactly the boundaries are/should be established in France and Hungary; what privacy and/or data protection questions arise and what answers can be provided to them.

II. 3. Conclusions and *de lege ferenda* suggestions

II. 3. 1. Findings

In relation to Hypothesis 1, it was found that despite the fact that this collision of rights already existed, SNSs put it into a new perspective, through intensifying the collision between the employees' right to privacy and right to data protection and the employer's rights. The intensification is brought by the fact that *on the one hand*, through monitoring or regulating employees' use of SNSs, the employer can take a glimpse into the personal life of the employee to an extent never seen before, with ease, due to the vast amount of information shared on SNSs by users. *On the other hand*, the employee is capable of jeopardizing the employer's rights in more serious forms (e. g. Facebook "addiction", which can seriously affect working hours, or harming the employer's reputation in more severe ways as a result of the public nature of these sites, the style usually used on them, the possible identification of the employer, etc.) due to the change of paradigm brought by SNSs. Therefore, both parties are increasingly interested in enforcing their rights, resulting in the intensification of the collision of rights. Furthermore, it was also held that SNSs have contributed to the blurring of the boundaries between personal and professional life – which also challenges the establishment of a balance between the two sides.

The application of the existing rules to SNSs was examined in three areas (recruitment, the use of SNSs at the expense of working hours, employees' activities and behavior on SNSs), as SNSs raise different kinds of questions in these areas.

(1) Pre-employment and Hypothesis 2: during *pre-employment* SNS background checks, it was held that the employer should not base his/her decision on the personal life of the employee, but on his/her professional capacities. However, as the personality of the applicant can also be taken into consideration, the exact limits of personal and professional life are blurred. SNSs raised the issue that the information that could be legally taken into consideration by the employer and the information that cannot are typically present on SNSs in an inseparable way. In addition, on SNSs the employer can access personal data in a quality and quantity never seen before, allowing him/her to access a wide range of information that would not have been available to him/her in the pre-SNS era. Does consulting the applicant's

SNS profile constitute an intrusion into his/her private life? It was established that in cases when the individual posted certain information publicly, the intrusion was unlikely to occur, as it is not reasonable to expect the employers not to consult this publicly available information.[16] The protection of applicants' rights can also be approached from the aspect of data protection, as accessing and then using these data can be better assessed through data protection, since compared to the unclear boundaries between "personal" and "professional" information, data protection has a more exact terminology. In the field of data protection, data quality principles raised some important issues, as the enforcement of this principle is extremely questioned.

As regards pre-employment, one of the main challenges is related to the invisibility of SNS background checks, and thus to the enforcement of the protection of applicants' rights. As typically these searches stay invisible, it is highly questionable that the employer would subject himself/herself to the strict requirements imposed by data protection law. Thus, *Hypothesis 2* held that due to these challenges (e. g. invisibility of background checks), the adoption of a more flexible regulation is needed, through aiming to make employers realize that respecting data protection requirements will lead to more reliable decision-making (otherwise they would be counter-effective in finding the most suitable applicant), thus constituting a more effective way to protect job applicants' rights than completely prohibiting these searches.

(2) SNS use at the expense of working hours and Hypothesis 3: *during working hours* privacy questions were raised in relation to the possible prohibition of SNS use. Employees are entitled to *privacy* even within the workplace, and privacy also means the right to establish relationships with others, and today SNSs constitute a preponderant forum for communicating and staying in touch with contacts, thus the question was raised whether the employer can completely prohibit their use. It was found that the employer can freely determine the use of work equipment: the only limitation to be respected is that it must be ensured that in exceptional cases the employee is able to communicate. As SNSs are not the only means for communication, the employer can decide to completely prohibit their use. After establishing

[16] In relation to *access* it was held that the employer can usually access information that was made publicly available. This means that the user has not applied privacy settings and is freely available to other users of SNSs. However, using stratagems (e. g. creating a fake profile to "friend" the employee, hacking, asking for a password, asking for changing the privacy settings – any method used to bypass the privacy settings or the intended audience chosen by the user) is not compatible with legal regulations.

the bans (or limitations in the case of a more permissive regulation), the employer is also entitled to monitor whether employees complied with the rules. Such a monitoring was approached from the angle of *data protection*.

In the case of SNS use at the expense of working hours, fewer substantially new questions were raised compared to the other fields; as a consequence, *Hypothesis 3* held that the existing rules established for the monitoring of the personal use of the Internet and e-mail are in most regards capable of adequately regulating SNSs as well – despite new challenges raised by SNSs (e. g. accessing SNSs from the personal devices of the employees or considering that as opposed to e-mail, on SNSs it is more difficult to identify their use as personal).

(3) Employees' presence and activities on SNSs and Hypothesis 4: in the case of employees' presence and activities on SNSs, typically conducted *outside the workplace*, *privacy* questions were raised in relation to imposing limitations on the employees' freedom of action, by imposing rules on whether – and if yes, how – they can participate in SNSs. Following from the employees' obligations, naturally he/she can be expected to be subject to certain restrictions, however, these cannot be limitless. During the establishment of the legal limits of such restrictions, it should be taken into consideration that in the light of the intensification that SNSs brought to the collision of rights, employers have found themselves in an *even more* vulnerable position (*Hypothesis 4*). However, apart from certain exceptional cases, *completely* prohibiting the use of SNSs does not seem legally acceptable. Imposing limitations on their use is more feasible; however, the exact extent of such limitations is highly dependent on the workplace and on the position of the employee. *Data protection* questions were raised in relation to monitoring, when the employer decided to monitor or to use data available on SNSs in order to assess compliance or impose certain sanctions.

II. 3. 2. Recommendations and *de lege ferenda* suggestions

In the light of the above, different *recommendations* and proposals were made throughout the dissertation. It was held that in order to successfully address challenges posed by SNSs, a complex approach should be adopted, containing recommendations for the legal sphere (especially to lawmakers, judges and data protection supervisory authorities), for the employer

(mostly aiming at the adoption of internal policies), for technology (encouraging SNS providers to adopt privacy and data protection-friendly technological solutions) and finally for the individual himself/herself.

(1) Recommendations for the legal sphere. For all actors making decisions in the legal sphere (lawmakers, judges, members of data protection supervisory authorities) it is crucial to be aware of the exact functioning of SNSs in order to avoid inaccurate or hardly interpretable reasoning or rules – as it has already happened on various occasions. This can be achieved, for example, through organizing trainings.

From the detailed analysis of French and Hungarian regulations, the following *de lege ferenda* suggestions were proposed.

The *first de lege ferenda suggestion* aims to better adapt to the realities brought by ICT and amongst them SNSs: it recommended the modifications of the French Labour Code and the Hungarian Labour Code, by not only regulating what kind of information can be *requested* from applicants/employees, but the wording of the relevant provisions should also include information that can be *collected*.[17] Such an amendment would remove any uncertainty resulting from the strict grammatical interpretation of the existing provisions of the labour codes.

The *second de lege ferenda suggestion* relates to the Hungarian Labour Code and recommends clarifying in Hungarian law – and in French law alike – that the relevant data protection regulations of the Hungarian Labour Code are applicable to job applicants as well. Such a clarification might include the insertion of a subsection stating that these provisions are to be applied to job applicants as well.[18]

(2) Recommendations for data protection supervisory authorities. For data protection supervisory authorities it is recommended to issue a document or information notice in which

[17] Thus, the following solution (suggestion in italics) is recommended as a *de lege ferenda* suggestion:
Proposed Article L1221-6 of the French Labour Code: "The information requested from *or collected about* a job applicant – in any form whatsoever – shall only have the aim to assess his/her fitness for the proposed employment or his/her professional competence."
Proposed Subsection (1) of Section 10 of the Hungarian Labour Code: "An employee may be requested to make a statement or to disclose certain information, *or information relating to him/her can be collected* only if it does not violate his/her rights relating to personality, and if deemed necessary for the conclusion, fulfilment or termination of the employment relationship."

[18] Such a subsection might be formulated as follows: *"Subsection (6) of Section 10: Subsections (1)-(5) are also adequately applicable to job applicants."*

they extensively lay down the most important rules with regard to SNSs and employment,[19] as such a document can highly contribute to the uniform interpretation of the privacy and data protection requirements relating to SNSs and labour law.[20] These rules would include, for example, specifying the public-private nature of SNSs, clarifying the applicability of the rules to SNSs, challenges and solutions relating to data quality,[21] requirement of transparency and participation of the data subject, principle of proportionality (in relation to prohibiting or monitoring), assessment factors to be considered on a case-by-case basis (e. g. position of the employee, nature of the post, frequency and time spent on SNSs, publicity of posts, consequences of the post, antecedents, etc.). For the Hungarian data protection supervisory authority, it was suggested measuring whether more accessible online presence can be achieved – for example, through social media – possibly based on the example set by the French data protection supervisory authority. Although this would not instantly resolve challenges related to data protection and employment, it would constitute an important step in raising awareness and promoting the right to data protection.

(3) Recommendations for the employer. The employer also plays an important role when it comes to SNSs and employment: as it was seen, it originates from the different rights and obligations imposed on the parties that the employer can control and monitor the employees' use of SNSs. It is the employer's right to determine – in accordance with legal regulations – the exact rules of such control and monitoring, considering the specificities of the given workplace. In addition to the legal obligation of prior information, it was recommended in the dissertation that the employers adopt internal social media policies in order to effectively communicate the rules and expectations relating to/towards employees. Also, organizing internal trainings in order to raise employees' awareness might be recommended.

[19] As they did in the case of traditional means of employee monitoring.

[20] Especially in Hungary, where there is considerably less case law, compared to France. In France, the drafting of such a document can rather serve as a summary of the existing rules elaborated by court decisions.

[21] With regard to data quality, another suggestion proposed by the dissertation is that during the recruitment process – in order to handle the challenges relating to the outdatedness of personal data available on SNSs and to the right to be forgotten – a time limitation period for the processing of personal data originating from SNSs should be introduced. It would mean that in accordance with the general limitation period in labour law, posts, pictures and other contents posted on SNSs before that period should not be processed in the recruitment process. Source: Hajdú, J. *et al.* (forthcoming) 'Közösségi média és munkajog – különös tekintettel a Facebook-ra alapított felmondásokra a hazai szabályozás és a nemzetközi joggyakorlat tükrében', *De iurisprudentia et iure publico (DIEIP)*

(4) Recommendations for service providers. As regards *technology,* SNS providers can also contribute to the protection of personal life by developing technical measures to enhance the protection. This can be achieved, for example, through enabling the users to use pseudonyms, the possibility of choosing customized privacy settings, and also through raising awareness.

(5) Recommendations for the individual. Lastly, the (prospective) employee's role must be mentioned: despite the creation and existence of a protective legal environment, it must not be forgotten that every user is responsible for his/her actions and behavior on SNSs, and that they should actively participate in ensuring the protection of their own personal lives. They should be able and expected to make *informed* decisions as regards whether they should post something to SNSs, to what audience (choice of privacy settings), whether there can be any legal consequences. They should not upload content relating to third persons without their consent and should actively monitor their e-reputation and make the necessary steps if they detect an anomaly.

III. SCIENTIFIC OUTPUT RELATED TO THE RESEARCH TOPIC

III. 1. Publications

1. **Lukács, A.** (forthcoming) 'A GDPR által okozott kihívások a munkajogban', in Strihó, K. and Szegedi, L. (eds.) *Európai szabályozáspolitikai kihívások.* Budapest: Nemzeti Közszolgálati Egyetem
2. **Lukács, A.** (forthcoming) 'Információs és kommunikációs technológiák és munkajog: a munka és magánélet határainak elmosódása, különös tekintettel az online közösségi oldalakra', *Forum: Publicationes Doctorandorum Juridicorum,* IX.
3. **Lukács, A.** (2017) '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. Ljubomir, S. (ed.) *Harmonizaci a srpskog i mađarskog prava sa pravom Evropske uni e = A szerb és a magyar jog harmonizációja az Európai Unió jogával = Harmonisation of Serbian and Hungarian Law with the European Union Law: Tematski*

zbornik = Tematikus tanulmánykötet = Thematic Collection of Papers. Újvidék: Újvidéki Jogtudományi Kar, Kiadói Központ, pp. 593-606.

4. **Lukács, A.** (2017) '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*, 11(2), pp. 185–214.

5. Hajdú, J. and **Lukács, A.** and Lechner, V. Á. and Turi, A. (forthcoming) 'Közösségi média és munkajog – különös tekintettel a Facebook-ra alapított felmondásokra a hazai szabályozás és a nemzetközi joggyakorlat tükrében', *De iurisprudentia et iure publico (DIEIP)*.

6. **Lukács, A.** (2017) 'Adatvédelmi irányelv és rendelet, avagy hogyan változott a közösségi oldalakra vonatkozó szabályozás az Európai Unió adatvédelmi reformjával?', in Homoki-Nagy, M. and Hajdú, J. (eds) *Ünnepi kötet dr. Zakar András c. egyetemi tanár 70. születésnapjára*. Szeged: Szegedi Tudományegyetem Állam- és Jogtudományi Kar, pp. 125–139.

7. **Lukács, A.** (2017) 'The Boundaries of Work and Private Life. Workplace Privacy Protection in French Law', in Tuboly-Vincze, G. (ed.) *XV. Országos Grastyán Konferencia Előadásai*. Pécs: PTE Grastyán Endre Szakkollégiuma, pp. 175–184.

8. **Lukács, A.** (2016) 'Pre-employment and Data Protection in Hungary: the Main Issues Regarding Social Networking Sites and Hiring', in Ljubomir, S. (ed.) *Harmonizaci a srpskog ǰ i mađarskog prava sa pravom Evropske unije = A szerb és a magyar jog harmonizációja az Európai Unió jogával = Harmonisation of Serbian and Hungarian Law with the European Union Law*. Újvidék: Újvidéki Jogtudományi Kar, Kiadói Központ, pp. 543–558.

9. **Lukács, A.** (2016) 'What is Privacy? The History and Definition of Privacy', in *Gábor Keresztes (ed.): Tavaszi Szél 2016 Tanulmánykötet I.* Budapest: Doktoranduszok Országos Szövetsége, pp. 256–265.

10. **Lukács, A.** (2016) 'Recent Challenges of Data Protection Law in the European Union, with Special Regard to the Internet', *Forum: Publicationes Doctorandorum Juridicorum*, 6, pp. 77–91.

III. 2. Presentations

1. Cyberspace 2019 - 17th International Conference: *Job Applicants' Right to Data Protection with Special Regard to the Principle of Data Quality in Social Media* (Brno, Czech Republic, 2019)

2. 12th seminar for Young Researchers on "European Labour and Social Law": *Employees' Right to Privacy and Right to Data Protection and Social Network Sites* (Strasbourg, France, 2019)

3. Marsouin Digital Society Conference: *Privacy and Data Protection in the Digital Age: Social Media and Blurred Boundaries Between Work and Employees' Personal Lives* (Rennes, France, 2019)

4. Queen Mary University of London - Sorbonne Law PhD Conference: *Protection of Employees' Right to Privacy and Right to Data Protection in the 21st Century, with Special Regard to Social Network Sites* (London, United Kingdom, 2018)

5. Cyberspace 17 - 15th International Conference: *Layoff, Facebook, Employment: the Growing Issue of the Right to Data Protection and Social Network Sites with Special Regard to the Termination of Employment* (Brno, Czech Republic, 2017)

6. Harmonization of Serbian and Hungarian (domestic) law with the European Union Law and Cross- Border Cooperation, comparative seminar: *The Regulation of Employees' Facebook use at the Workplace – with Special Regard to the Data Protection Law of the European Union and Hungary* (Novi Sad, Serbia, 2017)

7. A közösségi oldalak használata során felmerülő adatvédelmi jogi problémák a munkajog kontextusában című workshop: *Európai Unió és Franciaország: a közösségi oldalak adatvédelmi jogi szabályozása a munka világában* (Szeged, Hungary, 2017)

8. Cyberspace 16 - 14th International Conference: *To Post, or Not to Post - That Is the question: Why Do Employees Use Facebook and Why Does the Employer Monitor It* (Brno, Czech Republic, 2016)

9. PTE Grastyán és TTK Szentágothai szakkollégiumok közös Ph.D. és TDK konferenciája: *The Boundaries of Work and Private Life - Workplace Privacy Protection in French Law* (Pécs, Hungary, 2016)

10. HR kihívások és gyakorlati megoldások a XXI. század világában, Tudományos Szakmai Konferencia: *HR és adatvédelem: az új technikai eszközök alkalmazásának lehetősége a felvételi eljárás során* (Szeged, Hungary, 2016)

11. Tavaszi Szél doktorandusz konferencia, Óbudai Egyetem: *What is Privacy? The History and Definition of Privacy* (Budapest, Hungary, 2016)

12. Harmonisation of Serbian and Hungarian Law with the European Union Law, Comparative Seminar: *Data Protection in the Workplace: the Main Issues about the Use of Social Networking Sites* (Szeged, Hungary, 2016)