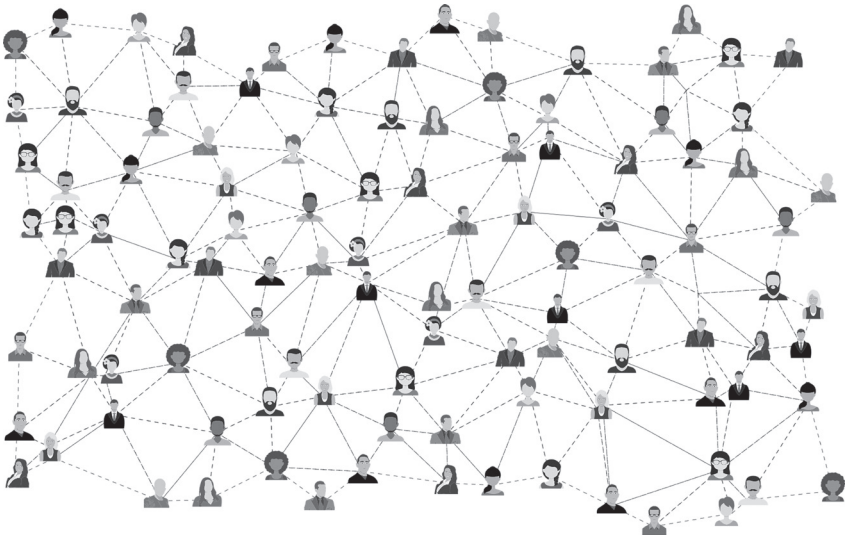
Adrienn Lukács

Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary

A Pólay Elemér Alapítvány Könyvtára
90



Source: https://cdn.pixabay.com/photo/2018/11/29/21/51/social-media-3846597_1280.png

Prepared at the University of Szeged
Faculty of Law and Political Sciences
Institute of Industrial Relations and Social Security.

Institute Head:
József Hajdú
Professor

Adrienn Lukács

Employees' Right to Privacy and Right to Data Protection on Social Network Sites

with Special Regard to France and Hungary

Iurisperitus Publishers
Szeged, 2021

A Pólay Elemér Alapítvány Könyvtára

Series Editor:
Elemér Balogh
Professor

Reviewers:
György Kiss
Nicolas Moizard

This research was supported by the project nr. EFOP-3.6.2-16-2017-00007, titled Aspects on the development of intelligent, sustainable and inclusive society: social, technological, innovation networks in employment and digital economy. The project has been supported by the European Union, co-financed by the European Social Fund and the budget of Hungary.

Manuscript closed: 10th January 2020

Technical Editor:
Ildikó Kovács

Responsible Publisher:
Márta Görög Dean, President of the Pólay Elemér Alapítvány board of trustees
Prepared by Innovariant Ltd
Senior Editor: György Drágán
ISSN 1786-352X
ISBN 978-615-6268-10-5

I would like to thank my former supervisors, József Hajdú and Francis Kessler for their support and guidance during the research, and my mother, Éva Regdon for proofreading my translations during all these years.

TABLE OF CONTENT

LIST OF ABBREVIATIONS

APEC	Asia-Pacific Economic Cooperation
BYOD	bring your own device
CCTV	closed-circuit television
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés (French National Commission on Informatics and Freedoms)
CoE	Council of Europe
DPA	data protection authority
DPD	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
ECHR	European Convention on Human Rights
ECOWAS	Economic Community of West African States
ECSR	European Committee of Social Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ELLN	European Labour Law Network
ENISA	European Union Agency for Network and Information Security
ESC	European Social Charter
EU	European Union
FDPA	French Data Protection Act (Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties)
FLC	French Labour Code (Code du travail)
GDPR	General Data Protection Regulation
HDPA	Hungarian Data Protection Act (Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information)
HLC	Hungarian Labour Code (Act I of 2012 on the Labour Code)
ICCPR	International Covenant on Civil and Political Rights
ICO	Information Commissioner's Office
ICT	information and communication technology
ILO	International Labour Organization
IWGDPT	International Working Group on Data Protection in Telecommunications

NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information)
OECD	Organisation for Economic Co-operation and Development
Privacy Act	Hungarian Act LIII of 2018 on the Protection of Private Life
SNS	social network site
UDHR	Universal Declaration of Human Rights
WP29	Article 29 Data Protection Working Party

FOREWORD

New information and communications technologies (hereinafter referred to as: ICT)[1] are omnipresent and exert a fundamental impact on everyday life in the 21st century – including the world of work as well:[2] digitalisation fundamentally changes not only working conditions, but also the possibilities in workplace monitoring.[3] Innovations of ICT, 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 controlling and monitoring employees.

As part of ICT, *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: according to *Eurostat*, in 2017 one of the most frequent online activities in the European Union (hereinafter referred to as: EU) was the use of SNSs.[4] As *Alissa Del Riego et al*. phrased it, the use of SNSs "*[…] is not a luxury or a lifestyle choice, but part of the reality of the modern world.*"[5] The first SNS – SixDegrees – appeared in 1997,[6] and since then several others have followed. Today the most popular SNSs have millions of users worldwide.[7] There exist hundreds of different international and national (social media) and SNSs.[8] The reasons lying behind such popularity are threefold, according to *James Grimmelmann*. He identifies and describes three main forms of motivations, all three originating from basic human needs that existed before the invention of SNSs, but gained a new form through their appearance.[9] These human needs are self-expression (identity), communication (relationships) and being part of a community; constituting the basic elements of social interaction.[10] During the use of such services, the personal data of individuals become publicly available in a quantity and quality never experienced before,

---

1 According to Eurostat the term ICT "*covers all technical means used to handle information and aid communication.*" https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Information_and_communication_technology_(ICT) (Accessed: 25 October 2019).

2 Rey 2013. p. 108.

3 Fritsch 2015. p. 149.

4 https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage (Accessed: 4 January 2018)

5 Del Riego – Sánchez Abril – Levin 2012. p. 23.

6 Boyd – Ellison 2008. p. 214.

7 In 2018 Facebook had 2.2 billion users, while YouTube, Twitter and Instagram had 1.9 billion, 335 million and 1 billion *active* users, respectively, just to mention a few examples. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed: 4 January 2018).

8 For an illustrative list of the most popular SNSs see more: https://www.practicalecommerce.com/105-leading-social-networks-worldwide (Accessed: 4 January 2019)

9 Grimmelmann 2009. p. 1159.

10 First, users can express their identity through their profiles, by allowing the individual to carefully shape what kind of image of himself/herself he/she wants to express towards other users. Second, they can communicate and maintain different relations with other users in several ways. Third, users can feel that they are a part of a community and they can establish their social position within the community. Grimmelmann 2009. pp. 1151–1159.

on a global scale,[11] which results in the appreciation of the examination of their right to privacy and right to data protection.

Employees are among SNS users as well, which can raise several challenges in multiple fields relating to employment: starting from recruitment, through SNSs' effects on working hours, leaking business secrets or the collective enforcement of employees' rights, till questions relating to employees' freedom of expression on SNSs. These fields notably raise the question of ensuring the employer's rights (manifested in controlling and monitoring employees) during employee use of SNSs, which can enter into collision with the above-mentioned right to privacy and right to data protection.

As opposed to the right to privacy and right to data protection, the employer has different rights, the enforcement of which might justify employee control and monitoring. These rights notably include the right to property (including the economic freedom to decide how to use the employer's property), the right to protect his/her economic interest (e.g. through ensuring productivity, the protection of reputation, the protection of business secrets, the protection of legitimate economic interests) and occupational safety and health (which mostly confers obligations on the employer). In order to ensure the protection of these rights, the employer is entitled to control employees' behaviour and to monitor whether employees respect the relevant rules and requirements.

Controlling and monitoring are inherent to the employment relationship as the employee is subordinated to the employer: he/she is usually integrated into the organisation of the employer, uses the materials provided by him/her and is expected to follow his/her instructions regarding the work.[12] According to general labour law principles, employers have "*a contractually based right to control contract fulfilment and to monitor work performance and the proper use by employees of company equipment facilities*."[13] However, since the early examples of work organisation and employee monitoring,[14] technology has experienced such a leap that it put this existing phenomenon into a different light through facilitating control and monitoring from a technological point of view.[15]

Employee control and monitoring have a close relationship with technological development: various innovations make it possible to monitor one's every step in an extremely detailed way, giving privacy and data protection an increased value.[16] Employers also benefit from these developments and use them to control and monitor their employees in order to ensure the protection of their rights. While earlier monitoring took place in the form of closed-circuit television (hereinafter referred to as: CCTV) surveillance, geo-localisation, monitoring of telephone use and computer/e-mail use, and concentrated mainly on employees' activities within the workplace, today new ways of monitoring – such as obtaining information through SNSs – go beyond the physical workplace and enable the employer to try to monitor activity taking place outside the workplace. Although from a technological point of view everything is possible, everything will not be legally permissible.[17]

---

[11] International Working Group on Data Protection in Telecommunications 2008. p. 10.

[12] European Network of Legal Experts in the field of Labour Law 2009. p. vi.

[13] Hendrickx 2002. p. 114.

[14] Such as for example *Jeremy Bentham*'s Panopticon, *Frederick Taylor*'s scientific management or *Henry Ford*'s surveillance.

[15] Moreira 2016. p. 5.

[16] For example, already two decades ago *Scott McNealy*, former CEO of Sun Microsystems stated: "*[y]ou have zero privacy. Get over it.*" Cited in: Smith-Butler 2009. p. 55.

[17] Ray 2017. p. 118.

From a *legal aspect* both the right to privacy and the right to data protection are regulated by different legal documents. From the international level particularly various human rights agreements[18] must be mentioned, guaranteeing that everyone has the right to privacy, altogether with the relevant documents in the field of data protection, issued by the International Labour Organization (hereinafter referred to as: ILO),[19] the Organisation for Economic Co-operation and Development (hereinafter referred to as: OECD),[20] the Council of Europe (hereinafter referred to as: CoE)[21] and the EU.[22] At the national level in the examined countries, both in France and in Hungary, constitutional protection is guaranteed to these rights,[23] as well as civil law protection.[24] Also, both countries enacted a data protection act.[25] With regard to privacy and data protection challenges specific to the context of employment, both labour codes address the question of respecting employees' rights at a general level.[26] Also, the "traditional" ways of employee monitoring (e. g. CCTV monitoring, monitoring the use of e-mail, Internet, work computer, telephone, GPS monitoring) are already regulated – both in France and in Hungary –: the relevant applicable rules and their interpretation were already elaborated notably through case law and the practice of the data protection authorities, and doctrine as well.

The monograph will focus on the collision between the employees' rights (notably right to privacy and right to data protection) and the employer's rights (notably right to property, right to the protection of business secrets, right to reputation, right to the protection of economic interests) during the use of SNSs, manifested in the employer's right to control and monitor. *On the one hand*, the employee is entitled to the right to privacy and the right to data protection during controlling and monitoring.[27] *On the other hand*, it is inherent to the employment contract that the employer has the power/right to control and

---

18 United Nations: *Universal Declaration of Human Rights*, 1948. Article 12.; United Nations: *International Covenant on Civil and Political Rights*, 1966. Article 17.; Council of Europe: *European Convention of Human Rights*, 1950. Article 8.; European Union: *Charter of Fundamental Rights of the European Union*, 2000. Article 7

19 *Protection of workers' personal data. An ILO code of practice*. International Labour Office, Geneva, 1997

20 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980; *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* – revised, 2013

21 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981; *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, 2018; *Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment*, 2015

22 *Charter of Fundamental Rights of the European Union*, 2000. Article 8.; *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 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)

23 Conseil constitutionnel: décision n° 94-352 DC du 18 janvier 1995; Conseil constitutionnel: décision n° 99-416 DC du 23 juillet 1999; Article VI of the Fundamental Law of Hungary

24 Article 9 of the French Civil Code and Items b) and e) of Section 2:43 of the Hungarian Civil Code

25 In France it is the "Loi informatique" [Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties ("loi relative à l'informatique, aux fichiers et aux libertés")] and in Hungary it is Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information.

26 See especially Article L1121-1 of the French Labour Code and Subsection (2) of Section 9 of the Hungarian Labour Code

27 Hendrickx 2002. pp. 23–24.

monitor[28] employees' activities in order to enforce different rights.[29] 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. 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.).[30] 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 "*labour law is the law protecting the employee to counterbalance the employee's subordination[,]*"[31] the monograph will primarily approach the subject from the employees' perspective and will focus on the question how their right to respect for private life and right to data protection should be ensured.

Relations between privacy and data protection are complex and far from being unequivocal, however, it seems to be undeniable that there is a certain connection between these two rights.[32] Because of their more personal nature in comparison to social media, focus will be 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 the right to personal data protection, the monograph 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.[33] Consequently, the monograph will examine SNSs and employees' right to privacy and right to data protection during the conclusion, management and termination of the employment relationship.

In order to effectively address SNSs, the subject is approached from a double, privacy-data protection approach, which assesses controlling from the aspect of privacy, while monitoring from the aspect of data protection. The question of controlling and monitoring SNSs can be observed from two separate, but interconnected approaches: it can be addressed through a privacy approach and also through a data protection approach. While acknowledging that the right to privacy and the right to data protection are separate rights, when it comes to SNSs, both are necessary to ensure the protection of employees' personal lives. Although both rights are "present" during the whole existence of the employment relationship, depending on various factors either the right to privacy or the right to data protection is more emphatic and raises more substantial challenges.

Which approach being more dominant depends on several factors, such as the activity (controlling or monitoring), the phase of the employment relationship (recruitment, fulfilment or termination) or the examined country (France or Hungary). Controlling employees (regulating what conduct they can or cannot adopt) relates mostly to privacy, while monitoring whether employees comply with the former regulations raises mostly

---

28 In French law it is called "pouvoir" meaning power, while in Hungarian doctrine the expression "jog" meaning right is used.

29 Blanpain 2002. pp. 43–44.

30 Gyulavári 2017. p. 235.; Breznay 2006. p. 329.

31 Kiss 2015. p. 4.

32 http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (Accessed: 28 February 2018)

33 The employer's use of social media and SNSs for public relations purposes (even if it is executed by the employee) constitutes a separate field, distinct from the subject of the present work.

data protection questions. While during the recruitment process the application of the data protection requirements pose more significant challenges, when it comes to employees' expressing themselves on SNSs, the right to privacy gains more importance. Concerning the use of SNSs at the expense of working hours, both approaches are equally significant. Also, in relation to employee monitoring in French labour law, the foundations of privacy seem to be more emphatic,[34] while in Hungary emphasis is put on a data protection approach.[35] As it will be demonstrated, due to the connection between privacy and data protection, the privacy and the data protection approaches complement each other and are both necessary to ensure the protection of employees' rights while engaging in SNSs.

The monograph will focus on the *private sector* employment law. The monograph 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.[36] The use of SNSs and collective enforcement of interests constitute a separate field, distinct from the subject of the present work.

In this context the monograph will analyse– 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 online SNSs during the different phases of the employment relationship, and if yes, to what extent. The monograph will assess how the existing rules[37] 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.

While keeping in mind that the examined phenomenon is universal in societies where SNSs are available,[38] the *examination will focus on the jurisdictions* of France and Hungary, with the aim of identifing separate or common good practices, as well as to introduce the jurisdiction of both countries for research, legislative and teaching reasons. The comparison of the two countries will not be implemented through pure comparative research, but the two systems will be assessed (mostly) in the light of EU legislation.[39] In recent years individuals could witness the adoption and the entering into force of the new EU data protection

---

34 Especially manifested in the central concept of personal life ("vie personnelle") unique to labour law.

35 This can be confirmed by the fact that when it comes to employee monitoring, though privacy is present in Hungarian law as well, when the detailed rules applying to certain types of employee monitoring were elaborated, the Hungarian data protection authority had a preponderant role.

36 On issues related to collective labour law see especially: Larher, Yann-Maël: *Les relations numériques de travail*. Doctoral dissertation. Université Paris 2 Panthéon-Assas, 2017; or: Ray, Jean-Emmanuel: *CGT, CFDT, CNT, CE et TIC*. Rapports collectifs de travail et nouvelles technologies de l'information et de la communication, Droit social, (4), 2012. pp. 362–372.

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

38 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 2014.

39 Besides the EU, both France and Hungary are members in the same international organisations. As such, examining national legislations in a vacuum is not possible: due to both countries being members in the same European (e.g. CoE, EU) and international organizations (e.g. UN, OECD), it is indispensable to examine the international environment into which national legislations are integrated. Thus, the most important international organizations for the subject are also referred to in the research.

framework. Driven by the occurring societal and technological changes, the EU decided to modernize its data protection legislation and adopted new rules, notably the General Data Protection Regulation[40] (hereinafter referred to as: GDPR), which replaced the previously existing Data Protection Directive[41] (hereinafter referred to as: DPD), which regulated matters of data protection for two decades. By opting to regulate data protection in the form of a regulation instead of a directive, the EU unified data protection law throughout Member States,[42] including France and Hungary as well. However, in certain fields the GDPR itself authorizes Member States to adopt more specific rules.[43] One of these fields is data processing in the context of employment, as Article 88 of the GDPR allows Member States to adopt specific rules in relation to data protection and employment. As such, differences might arise between Member States in the field of workplace data protection.

Consequently, it is worth examining what differences might arise in states with different historical, cultural, economic and legal traditions despite the common EU legal background and membership in international organisations. France is a country with considerable history in data protection law.[44] With its data protection act, the "Loi informatique",[45] France was amongst the first countries in the world to enact a data protection act, which considerably influenced subsequent regulations,[46] such as the Council of Europe's Convention 108,[47] the EU's DPD or the United Nations' data protection guidelines.[48, 49] In contrast to such a background, Hungary – a country formerly attached to the Eastern Bloc countries – adopted its first data protection act in 1992,[50] co-regulating matters of data protection and freedom of information. Also the Hungarian data protection regulation was highly penetrated with the concept of informational self-determination.[51]

The monograph 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 monograph will analyse the international, European (EU and Council of Europe), French and Hungarian legislation, jurisdictions, as well as a wide range of publications. Also, as the examined phenomenon is universal, brief outlooks to other European or international cases and proposed solutions will be made in order

---

40 *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). OJ L 119, 4.5.2016, p. 1–88.

41 *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 L 281, 23/11/1995 p. 31 – 50.

42 European Commission 2018. p. 2.

43 E.g. in relation to the processing of deceased persons' personal data [Recital (27) of the GDPR] or in the field of obligations of secrecy (Article 90 of the GDPR).

44 Grynbaum – Le Goffic – Morlet-Haïdara 2014. p. 747.

45 Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties ("loi relative à l'informatique, aux fichiers et aux libertés")

46 Hennette-Vauchez – Roman 2017. p. 553.

47 Council of Europe: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 1981

48 United Nations: *Guidelines for the Regulation of Computerized Personal Data Files*. Adopted by General Assembly resolution 45/95 of 14 December 1990

49 Féral-Schuhl 2010. p. 35.

50 Act LXIII of 1992. However, even before the adoption of the data protection act, the 1977 amendment of the Civil Code already acknowledged the right to data protection.

51 Decision No. 15/1991. (IV. 13.) of the Constitutional Court

to enrich the research – while focusing on France and Hungary. When examining these norms, 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. The research was concluded 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. Also, it is worth noting that the monograph was preceded by my PhD dissertation – which examined the same subject.

As regards the *structure*, the monograph 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 analysing 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, Part I. will address (1) 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 (2) 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, particularly 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 will be examined in detail: (1) recruitment and the protection of prospective employees' rights, (2) SNS use at the expense of working hours and (3) off-duty conduct and SNSs. It will be explored, in the light of the collision of rights and interests presented in Part I., where exactly 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.

PART I.
PROTECTION OF EMPLOYEES' PRIVATE LIFE AND PERSONAL DATA IN THE CONTEXT OF ONLINE SOCIAL NETWORKS

Technological innovations have not only made a fundamental impact on how expectations of privacy have changed,[52] but they have also caused profound changes in the world of work, blurring the boundaries between work and non-work.[53] However, as a preliminary point it must be emphasized that this phenomenon is mainly relevant to employees performing office work, and especially knowledge work.[54] In an age when on social media and SNSs users share such a rich amount of data that a few decades ago would have been called a "dossier",[55] the appearance of such a huge "database" has serious implications for the employment relationship as well.

As a consequence, the use of SNSs can have different impacts on the employment relationship: during such a use, notably employees' right to privacy and right to data protection might raise challenges. The growing number of internal social media policies and "Facebook firings" raise questions in relation to where the boundaries of personal and professional life are, while the monitoring of such a use can also raise data protection challenges.

The respect of employees' rights when applying "traditional forms of monitoring" or regulating their conduct is already regulated both at international and national levels. When it comes to employee monitoring, the fundamental legal challenge that arises is the collision of the employer's and the employee's rights. *On the one side*, there are the 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, right to property, 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.[56]

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.[57] Thus, the collision of rights is more intense in the case of monitoring employees' activities on SNSs – compared to the already regulated, traditional forms of employee monitoring.

In addition, privacy and data protection play an important role in ensuring the exercise of other fundamental rights as well, as SNSs also constitute an important forum of freedom of expression and represent an important source of accessing information. Privacy (and

---

52 Flint 2009. p. 7.

53 Peck 2012. p. 5.

54 Eurofound – International Labour Office 2017. p. 3. The report acknowledges that certain kinds of occupations require the physical presence at the workplace or simply do not involve the use of ICT. Source: *Ibid*. pp. 17–18.

55 Tobok 2013. p. 95.

56 Hajdú 2005. p. 20.

57 Michel 2018. p. 149.

data protection) also plays a crucial role in SNSs considering that their guarantee and respect by the employer is a condition for being able to fully enjoy the possibilities given by SNSs. If users are afraid to use SNSs because of the fear that someone – in the present case the employer – might use the information available on these sites, the freedom and fundamental rights of the individual will be impaired.[58]

Part I. will examine how, 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. Therefore, *first*, Title 1 will discuss the employees' relevant rights at stake, and then present how they collide with the employer's different rights. *Then*, Title 2 will focus on how these already established boundaries between work and private life are changed due to the proliferation of ICT, and especially to SNSs. As a result of Part I., the conceptual background of the collision will be explored, which will serve as a theoretical foundation for Part II., addressing the specific challenges raised by SNSs.

[58] Clark – Roberts 2010. p. 518.

Title 1: Collision of the employees' right to privacy and to data protection and the employer's rights

In the monograph's focal point employees' *personal life* – and the rights aiming to protect personal life – are found.[59] Despite certain common characteristics, the *right* to privacy and the right to data protection are two separate rights, both playing an important role in ensuring the protection of personal life. *On the one hand*, *employees*, just as any individual, are entitled to the enjoyment of the right to privacy and the right to data protection.[60] *On the other hand*, the enjoyment of these rights is naturally influenced by being qualified as an employee: the employee status will automatically limit these rights.[61] Originating from the employment relationship, the *employer* has rights that justify the limitations on privacy and data protection,[62] such as right to property, right to the protection of legitimate economic interests, etc. The rights of the two parties are interconnected: what is a right on one side will be an obligation on the other side,[63] and during their enforcement a balance must be found.[64]

The aim of this title is to provide conceptual foundations, through analyzing in detail the rights with utmost importance for the main research topic. Consequently, the employees' and the employer's relevant rights will be analysed.[65] *Chapter 1* of Title I will analyse the rights that are evoked in the collision of rights: first, the right to privacy; then, the right to data protection.[66] Then, *Chapter 2* of Title I will bring the focus on the employment relationship, by concentrating on employee control and monitoring. First, it will examine the rights and obligations arising from the employment relationship, and the rights granted to the employer that can justify control and monitoring. Then, it will discuss the already established legal framework for employee monitoring.

---

[59] The expression personal life is used to designate a concept very similar to the personal life employed by the Social Chamber of the French Court of Cassation, having a close connection with private life (aiming to protect the parts of employees' life which they wish to conceal from the public) and also with the concept of privacy in public (private life interpreted in a broad way, breaking with the concept of secrecy). The (legal) definitions of these concepts are to be found in Chapter 1.

[60] See, for example, the ILO Code of practice 1997 or documents issued by the EU's former Article 29 Data Protection Working Party in the field of workplace privacy and data protection.

[61] Hendrickx 2002a. p. 49.

[62] See especially the labour codes (Article L1121-1 of the French Labour Code and Sections 9-11/A of the Hungarian Labour Code) laying down the rules on limiting employees' rights.

[63] Prugberger 2011. p. 283.

[64] Hajdú 2005. p. 20.

[65] Title 1 will limit itself to the examination of these rights from an angle focusing on the context of employment in *general*: the specific changes and challenges brought by SNSs will be addressed under Title 2.

[66] As *György Kiss* noted, employees are entitled to the same fundamental rights just as any individual, however, their exact appearance is influenced by the specific characteristics of the employment context. Kiss 2010. p. 226.

Chapter 1: Legal protection of personal life

When it comes to the protection of employees' personal lives, traditionally two rights can gain significant importance: the right to privacy and the right to data protection. They are both acknowledged at the international[67] and at the national level[68] – as it will be discussed in Chapter 1 – confirming their utmost importance. Both the right to privacy and the right to data protection aims to protect the person[69] and are fundamental rights.[70] The respect of these rights is a necessary precondition of the enjoyment of other fundamental rights.[71] The right to data protection is regarded as a guarantee to ensure the inviolability of the individual's privacy, aiming to guarantee non-interference.[72]

Both rights are closely connected to technological developments and largely influenced by them, giving rise to new challenges. Amongst these developments, the proliferation of social media and SNSs has a huge impact on employees' right to privacy and data protection, as during the use of these services individuals often reveal events that are traditionally considered private and share a vast amount of personal data – giving rise to several questions in relation to privacy and data protection.[73]

Section 1: Right to privacy

One of the rights in the collision that must be balanced against the employer's legitimate interests is the (employees') right to privacy. However, when it comes to defining *privacy*, scholars usually face difficulties, as there exists no universal standpoint regarding its meaning.[74] Due to its complexity, creating one single definition leads to a contended result.[75] The aim of Section 1 is to provide a *general conceptual basis* regarding the scope and meaning of (the right to) privacy – which will be an essential precondition to addressing the specific challenges caused by the proliferation of SNSs and their effects on individuals' and society's expectations of privacy.

§1 will address the history and scope of privacy and the way it is apprehended by scholars. Then, *§2* will focus on how the different *legal* regulations regulate the right to

---

67 The most relevant international organizations that adopted international norms in the field of privacy and/or data protection are the UN, OECD, CoE and EU.

68 At the constitutional level, as well as in civil law and penal law regulations.

69 Despite what its appellation might suggest, the right to data protection does not aim to protect personal data, but *the individual* to whom personal data relates. Majtényi 2002. pp. 57–58.

70 Both rights are acknowledged in the CFREU (Article 7 and Article 8), are explicitly present in the Hungarian constitution (Article VI) and gained constitutional recognition by the French Constitutional Council.

71 Rouvroy – Poullet 2009. p. 61.

72 Vissy 2015. pp. 200–201.

73 E.g. is publishing something on an SNS considered to be part of private life? Can the employer monitor how employees use these sites? Can the employer tell the employees how they can use these sites? These and other specific questions will be addressed under Title 2.

74 As *Avner Levin* and *Patricia Sánchez Abril* phrased it: "*[p]rivacy has always been difficult to define. It seems that everyone wants it, but there is no consensus as to its meaning or value.*" Levin – Sánchez Abril 2009. p. 1007. Or see as *Daniel Solove* aptly formulated: "*[p]rivacy seems to be about everything, and therefore it appears to be nothing*." Cited in: Hughes 2015. p. 528.

75 Clarke 2014. p. 174.

privacy, with special regard to the most important international organisations, and to the two countries in the focal point of the monograph: France and Hungary.

§1. The challenges in defining (the right to) privacy: definitions and history

In spite of the numerous attempts that have been made to define privacy, it remains a complex and contested concept,[76] relating to which no universal definition could be formulated.[77] Although the claim for privacy is universal, its concrete form differs according to the prevailing societal characteristics, the economic and cultural environment.[78] It means that privacy must be reinterpreted in the light of the current era and be examined in the current context. Naturally, this ever-changing nature leads to challenges when it comes to defining what should be protected.[79]

It must also be anticipated that what is *considered to be* private and what is *legally protected as* private can differ:[80] focus will be put on the legal aspects of privacy. Although privacy has been in existence for a long time, as certain needs for privacy have their early origins in ancient societies, it only became a generally accepted right in the 19th-20th century.[81]

In the light of the challenges presented above, it is not the aim of the monograph to establish an exhaustive or universal notion of privacy. However, a discussion on privacy is inevitable when addressing the question of workplace privacy protection and social media, in order to understand what privacy means in the context of SNSs and employment. Thus, the most important definitions and approaches to effectively addressing privacy will be presented, with the aim of creating a definition *for the purpose of the monograph*.

(A) History of (the right to) privacy

Before addressing the exact content and scope of privacy, it is needed to define the main context in which (the right to) privacy appeared and continued to develop. Therefore,

---

[76] As *Michael D. Birnhack* stated: "*[p]rivacy is a contested legal concept, with several understandings and more misunderstandings, covering distant areas of human activities. Privacy is under constant attacks from many different angles. Despite the criticism, its inherent vagueness, and instability, privacy is a fundamental human right and a hallmark of democracy*." Birnhack 2008. p. 508.

[77] As *Serge Gutwirth* formulated it: "*[t]he notion of privacy remains out of the grasp of every academic chasing it.*" Gutwirth 2002. p. 31.
Robert C. Post also expressed his doubts regarding whether a universal definition of privacy could be created by stating that "*[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.*" Source: Post 2001. p. 2087.

[78] Majtényi 2006. p. 211.; Simon 2005. pp. 33–34.; Szabó 2005. p. 45.

[79] With regard to these ever-changing circumstances, it is not only impossible but also without interest to establish a definition of privacy. *Fatou Ba Sene* citing *François Rigaux* in: Ba Sene 2015. p. 93.

[80] For example, someone might find all kinds of physical connection – accidental physical contact in a bus during the rush hour or a friendly tap on the shoulder by a distant acquaintance – an intrusion into his/her private sphere, although in the legal sense it is not considered privacy infringement.

[81] Notably see the famous article entitled "The Right to Privacy" written by Samuel D. Warren and Louis D. Brandeis (Warren – Brandeis 1890) or the adoption of the different international human rights documents throughout the 20th century – to be presented later.

the main steps of its history will be addressed in the next paragraphs, followed by the presentation of how privacy gained legal recognition in French and Hungarian legal order, providing the framework of protection.

(a) Universal development

Privacy can be traced back to a long history: in a broad sense, early origins of privacy can be observed even in ancient societies.[82] The idea of privacy traditionally comes from the difference between "private" and "public",[83] which distinction comes from the natural need – as old as mankind – of the individual to make a distinction between himself/herself and the outer world.[84] The limits between private and public differ according to the given era and society,[85] which will cause the on-going change throughout history of what people consider private.[86] Thus, contemporary conceptions of privacy and its protection will considerably differ from its early forms.

It was the 19th century which brought a huge leap in the history of privacy as the new changes in the economy and in the society led to the transformation of the way people lived, and these new changes had consequences for privacy too, as physical and mental privacy were separated and started to evolve in two different ways. Due to urbanization, the population of cities started to grow, and it led to the physical loss of privacy as people in cities had to live in crowded places. On the other hand, citizens could experience a new "type" of privacy, as they ceased to live under the always watching eyes of their village neighbors and the constant moral control set up by them.[87]

It was against this background that the need for the *right to* privacy appeared.[88] Its first appearance dates back to 1890, when *Samuel Warren* and *Louis Brandeis* first stated the need for the legal recognition of the right to privacy in their article titled "The Right to Privacy" (published in the Harvard Law Review).[89] The reason behind was the dangers underlying the appearance and growth of (tabloid) newspapers, combined with the invention of the portable cameras, which were a fertile area for gossip and photojournalism. Their writing became a famous article among legal scholars; an "*unquestioned 'classic'*",[90] the "*most influential law review article of all*".[91] In the above-mentioned article Warren and Brandeis defined the right to privacy as "the right to be let alone".[92] The article also influenced

---

82 From a legal point of view, the Code of Hammurabi contained a paragraph against the intrusion into someone's home, and the Roman law also regulated the same question. (Solove 2011. p. 4.)

83 Szabó 2005. p. 45.

84 Konvitz 1966. p. 274.

85 Szabó 2005. p. 45.

86 *Daniel Solove* made an illustrative example to present the on-going change regarding what people consider private: even the aspects of life that nowadays are commonly considered as private (the family, the body and the home, etc.) had been through considerable changes as initially they were far from being private. For example, marriage was initially considered to be a contract, while nowadays it is one of the most intimate decisions made by the individual. See more: Solove 2002. pp. 1132–1140.

87 Simon 2005. p. 36.

88 Early forms of protection existed as well, relating, for example, to the immunity of the home ("*an Englishman's home is his castle*") or to the protection of correspondence.

89 Warren – Brandeis 1890

90 Shapiro 1985. p. 1545.

91 Kalven 1966. p. 327.

92 Warren – Brandeis 1890. p. 193.

jurisprudence as numerous endeavors to define privacy originated from Warren's and Brandeis' work.[93]

Even before the drafting of the relevant *international document(s)*, certain early forms of privacy protection (e.g. sanctity of the home and secrecy of correspondence) were to be found in the national legal systems, especially in France, England and Germany. However, it was only after the Second World War that the development of the right to privacy took a pace and has not slowed down ever since.[94] The cruelties of the Second World War – during which the use of large databases facilitated the deportation of millions – led to the drafting of the first international human rights agreements,[95] both at the universal and at the regional level. The very first international document that acknowledged the right to privacy as a fundamental human right was the *Universal Declaration of Human Rights* (United Nations, 1948, Article 12, hereinafter referred to as: UDHR).[96, 97] At the regional level, the Council of Europe and the European Union must be mentioned. One of the most important documents regulating the right to privacy is the *European Convention on Human Rights* (Council of Europe, 1950, Article 8, hereinafter referred to as: ECHR), which served as a genesis for several pieces of privacy legislation throughout Europe,[98] and marks the beginning of contemporary privacy protection in Europe.[99] Last but not least, the *Charter of Fundamental Rights of the European Union* (European Union, 2000, hereinafter referred to as: CFREU) must be mentioned.

(b) Legal acknowledgement of the right to privacy: France and Hungary

In addition to the protection afforded by international norms, national systems as well guarantee the protection of the right to privacy. Both in France and in Hungary *constitutional protection* is accorded to the right to privacy. However, *France* is one of those countries which do not expressively state the protection of the right to respect for private life in its constitution.[100] In France constitutional protection is afforded by the *Constitutional Council*, which first recognized the right to respect for private life in its 1995 "vidéosurveillance" decision.[101] Before this date, only the home received protection, but not the right to respect for private life in general.[102] Although it does not refer expressly to the respect of private life as such, the "inspection of vehicles" decision from 1977[103] is considered to be the first step towards recognizing the constitutional value of the right to respect for private life.[104] It was finally granted constitutional value in 1995, in the "vidéosurveillance" decision, when the

---

93 Simon 2005. p. 32.
94 Rigaux 1991. p. 540, p. 545.
95 Buitelaar 2012. p. 174.
96 Mendel et al. 2013. p. 12.
97 Among the documents drafted by the United Nations, the *International Covenant on Civil and Political Rights* (United Nations, 1966, hereinafter referred to as: ICCPR) shall also be mentioned, and its Article 17 guaranteeing the respect of private life.
98 Rustad – Paulsson 2005. pp. 870–871.
99 Otto 2016. p. 69.
100 Burgorgue-Larson 2005. p. 1. (Page number referring to the online version of the article downloaded from: https://hal.archives-ouvertes.fr/hal-01743616/document)
101 Conseil constitutionnel: décision n° 94-352 DC du 18 janvier 1995
102 Burgorgue-Larson 2005. p. 98.
103 Conseil constitutionnel: décision n° 76-75 DC du 12 janvier 1977.
104 Mazeaud 2015. p. 10.

Constitutional Council stated that "*[…] the infringement of the right to respect for private life may pose a threat to the individual liberty.*"[105] By this, it attached the right to respect for private life to *individual liberty*, founded on Article 66 of the Constitution.[106] Following this decision, in its "universal health insurance" decision in 1999,[107] the Constitutional Council found a new legal base, detaching it from individual liberty and acknowledged that it is founded on Article 2 of the Declaration of the Rights of Man and of the Citizen,[108] therefore associated with *personal liberty*.[109, 110]

Hungary's constitution, the Fundamental Law (adopted in 2011) *expressis verbis* states the protection of the right to privacy, through stating in Subsection (1) of Article VI that "*[e]veryone shall have the right to respect for his or her private and family life, home, communications and reputation*." The right to respect of private life as such did not appear explicitly till the adoption of the Fundamental Law,[111] although it does not mean that before this period no legal protection was afforded: the previous constitution already ensured protection to certain aspects of privacy, such as private secrets and the home.[112] In June 2018, Article 4 of the seventh modification of the Fundamental Law introduced certain changes relevant to the right to respect for private life, with regard to the new challenges arising due to technological development, digitalization, and the growing media attention.[113] As a result of the modification, Subsection (1) of Article VI was completed with the phrase "*[t]he exercise of freedom of expression and the right of assembly cannot result in the violation of private and family life or home of others.*" Subsection (2) was inserted into the same Article stating that the State legally protects the tranquility of the home.

Early forms of legal privacy protection appeared even before the right to respect of private life was explicitly declared by the *Civil Codes* – 1970 in France and 1977 in Hungary. In *France* its early history is mostly connected to the freedom of press and to the

---

[105] Conseil constitutionnel: décision n° 94-352 DC du 18 janvier 1995, par 3.

[106] Burgorgue-Larson 2005. p. 17. (Page number referring to the online version of the article downloaded from: https://hal.archives-ouvertes.fr/hal-01743616/document)

[107] Conseil constitutionnel: décision n° 99-416 DC du 23 juillet 1999

[108] Conseil constitutionnel: décision n° 99-416 DC du 23 juillet 1999, par. 45. "*Considering that under Article 2 of the Declaration of the Rights of Man and of the Citizen 'the aim of all political associations is the preservation of the natural and imprescriptible rights of the Man. These rights are liberty, property, security and resistance to oppression.' the freedom proclaimed by this article implies respect for privacy.*"

[109] Crouzatier-Durand 2013. p. 58.; Bioy 2016. pp. 454–456.

[110] The notion of personal liberty ("liberté personnelle") appeared in a 1988 decision of the Constitutional Council (Décision n° 88-244 DC du 20 juillet 1988.) and is considered to have utmost importance ("liberté mère"), serving as a single point of origin ("porte d'entrée unique") for the manifestations of personal autonomy (Bioy 2016. p. 452.). On the notions of individual liberty and personal liberty, and their role in the Constitutional Council's decisions see more in: Vadillo, Floran: Liberté individuelle vs liberté personnelle : l'article 66 de la Constitution dans la jurisprudence du Conseil constitutionnel ou la progressive reconnaissance d'un habeas corpus à la française. *Petites affiches*, (80), 2015. pp. 4–11.

[111] Although it appeared in the practice of the Constitutional Court – which will be addressed in §2.

[112] Act XX of 1949. The original text (Section 57) guaranteed protection to the individuals' individual liberty and its inviolability, the respect of private secrets and the home. The amendment of 1972 ensured the same protection but to the citizens. The final text of the previous constitution was adopted in 1989, with Subsection (1) of Section 59 stating that "*[i]n the Republic of Hungary everyone has the right to reputation, right to inviolability of the domicile, the right to the protection of private secrets and the right to the protection of personal data.*" Source: Jóri 2009. pp. 2171–2172.

[113] *T/332. számú javaslat Magyarország Alaptörvényének hetedik módosítása*, 2018. p. 5.

insults relating to private life.[114] Before 1970, when the right to respect for private life was inserted[115] into the Civil Code,[116] protection could be afforded on the basis of the previous Article 1382 on civil responsibility.[117] The previous *Hungarian* Civil Code (Act IV of 1959) did not ensure *sui generis* protection to privacy, it received protection on the ground of personality rights. It is the primary objective of personality rights to ensure protection to rights which make humans human, which are parts of human personality, without examining the societal circumstances – excluding from their scope political, cultural and social rights.[118] The essence of personality rights is to ensure the free expression of the personality and to prevent anyone from hindering them, within the limits that the community imposes.[119] Naturally, the exercise of these rights is not without limits, it is only in accordance with their social purpose, if it does not infringe other individuals' rights or laws guaranteeing these rights.[120, 121] It appeared in the Civil Code (Act V of 2013), which explicitly declares the protection of right to privacy.[122] Another important step was the adoption of the act on the protection of private life[123] in 2018.

Besides constitutional and civil law protection, *criminal law* also guarantees the protection against infringements of the right to privacy. When introducing civil law protection in 1970, Act No. 70-643 of 17 July 1970 on strengthening the guarantee of individual rights of citizens also inserted provisions into the *French Penal Code* against different invasions of privacy, at present found in Articles 226-1–226-7 of the French Penal Code. The *Hungarian Penal Code* (Act C of 2012) also contains certain provisions aiming to sanction the most serious actions infringing certain components of the right to respect for private life.[124]

Despite the fact that during the last decades the right to privacy gained legal recognition (both at the international and at the national level) and constitutes a dynamically evolving field of law due to its dependence on societal and technological circumstances, it does not mean that a universal definition, valid in all circumstances could be created.

---

[114] See more on the early history of French privacy law in: Whitman, James Q.: The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, 113(6), 2004. pp. 1151–1221.

[115] Inserted by the Act No. 70-643 of 17 July 1970 on strengthening the guarantee of individual rights of citizens ("*Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens*").

[116] Article 9: "*Everyone has the right to respect for his private life.*"
Without prejudice to the right to recover indemnification for injury suffered, judges may prescribe any measures, such as sequestration, seizure and others, suited to the prevention or the ending of an infringement of the intimate character of private life; in case of emergency those measures may be provided for by summary proceedings.

[117] Rigaux 1991. p. 546.
Article 1382 stated that "*[t]he perpetrator of any act that causes damage to another person is obliged to make reparation.*"

[118] Fézer 2014. p. 250.

[119] Petrik 2014. pp. 173–174.

[120] BH. 1992.387.

[121] See more on privacy and personality rights in: Görög 2016. pp. 61–63.

[122] Subsection (1) of Section 2:42 of the Hungarian Civil Code: "*[e]veryone is entitled to freely practice his or her personality rights, in particular the right to privacy and family life, home and communications with others in any way or form, and the right to protection against defamation of character, within the framework of the law and within the rights of others, and to not be impeded by others in exercising such rights.*"

[123] Act LIII of 2018

[124] Such as: Misuse of personal data – Section 219; Illegal Entry into Private Property – Section 221; Harassment – Section 222; Invasion of Privacy – Section 223; Mail Fraud –Section 224.

The next paragraphs will explore the different notions that were created attempting to define privacy.

(B) Understanding privacy

Enumerating exhaustively all existing (philosophical) and legal notions of privacy is an impossible task[125] and would also go beyond the primary scope of the monograph. Therefore, the monograph had to limit itself to presenting only a certain number of approaches relevant for the main topic. The aim of the following paragraphs is to provide insight into the various facets of privacy through reviewing the *(a)* most common types of definitions, then their existing categorizations by several scholars. Then, part *(b)* will demonstrate the factors that can have a considerable influence on understanding privacy – making it an ever-changing concept. The knowledge of this background will be necessary to understand how the legal protection of privacy functions, and what aspects of privacy receive legal protection in the examined jurisdictions.

(a) Definitions and classification of definitions

Besides the ever-changing nature of privacy, numerous attempts to define privacy have been made during the last 120 years.[126] Traditionally, privacy can relate to concealment or secrecy, giving the individual the possibility to separate himself/herself from the outside world. As already presented, *Warren* and *Brandeis* defined privacy as "the right to be let alone".[127] *Sidney M. Jourard* links privacy to concealment and argues that privacy "*is an outcome of a person's wish to withhold from others certain knowledge, past and present experience and action and his intentions for the future.*"[128] Privacy can also be understood as a quasi "aura" around the individual, which constitutes the boundary between him/her and the outside world.[129] *László Sólyom* puts interference into the center of privacy and argues that the common feature of perceptions of privacy is that it means the (physical and mental) area which is controlled by the individual, and which is thus free from external interference.[130]

Accessibility can also play a part in these definitions: according to *Ruth Gavison* "*our interest in privacy […] is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.*"[131] According to *Hyman Gross* "*privacy is the condition of human life in which acquaintance with a person or with affairs*

---

[125] Notably see the ECtHR, which stated in Niemietz v. Germany that "*[t]he Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life.*'" ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.

[126] On the existing definitions see more notably in: Solove 2002. pp. 1087–1156.; Davis, Steven: Is There a Right to Privacy? *Pacific Philosophical Quarterly*, 90(4), 2009. pp. 450–475.

[127] Warren – Brandeis 1890. p. 193.

[128] Jourard 1966. p. 307.

[129] Hajdú 2005. p. 8. referring to Davis, Simon: *Big Brother: Britain's web of surveillance and the new technological order*. Pan, London, 1996

[130] Sólyom 1983. p. 315.

[131] Gavison 1980. p. 423.

of his life which are personal to him is limited."[132] Another definition captures privacy as an "*interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations.*"[133] *Ernest Van Der Haag* provides a similar definition through understanding privacy as "*the exclusive access of a person to a realm of his own. The right to privacy entitles an individual to exclude others from (a) watching, (b) utilizing, (c) invading his private [personal] realm.*"[134]

Privacy can be approached through control over *information* relating to the individual: *Alan F. Westin* defined privacy as "*the claim of an individual to determine what information about himself or herself should be known to others*",[135] while *Charles Fried* stated that "*privacy […] is the control we have over information about ourselves.*"[136, 137] *Richard A. Posner* argued that "*one aspect of privacy is the withholding or concealment of information.*"[138] *Richard B. Parker* goes beyond identifying privacy as control over information and argues that privacy "*is control over when and by whom the various parts of us can be sensed by others.*"[139] According to *Ferdinand D. Schoeman* this control can relate not only to information and sensory access but also to the intimacies of personal identity.[140]

Privacy can also be connected to human *dignity* and *autonomy*: *Edward Bloustein* argued that intrusion into privacy has a close connection with personhood, individuality and human dignity.[141] *Tom Gerety* understands privacy as "*the control over or the autonomy of the intimacies of personal identity*".[142] *Máté Dániel Szabó* argued that "*privacy is the right of the individual to decide about himself/herself*".[143] Privacy attached to dignity is connected to the free development of personality and inner self, enabling the individual to create different public personas through being able to decide which areas of his/her life is the individual going to share with others.[144]

Intimacy also appears in definitions: according to *Julie Inness* all these approaches – information, access or intimate decisions – are linked by the common denominator of intimacy, being in the center of privacy.[145] According to *Charles Fried*, privacy serves as a basis for intimate relationships, such as friendship, love and trust; and constitutes a necessary pre-condition of establishing relationships with others and shaping one's own identity.[146]

Having knowledge of these definitions is crucial for the main topic of the research, as in relation to SNSs, several of these definitions gain importance – as it will be discussed in detail. Privacy interpreted as one's right to decide about himself/herself can be understood as deciding whether to engage in SNSs and if yes, to what extent. Developing one's personality

---

[132] Gross 1967. pp. 35–36.
[133] Clarke 2014. p. 174.
[134] Cited in: McCullagh 2008. p. 4.
[135] Westin 2003. p. 431.
[136] Fried 1968. p. 393.
[137] *Erik Van Hove* adopts the same opinion and complements this definition by adding the right to a private sphere. Cited in: McCullagh 2008. p. 4.
[138] Posner 1978. p. 393.
[139] Parker 1974. p. 281.
[140] Schoeman 2007. p. 2.
[141] Bloustein 1964. p. 973., p. 974.
[142] Gerety 1977. p. 281.
[143] Szabó 2005. p. 46.
[144] Levin – Sánchez Abril 2009. p. 1013.
[145] Cited in: Solove 2002. p. 1121.
[146] Cited in: Levin – Sánchez Abril 2009. p. 1013.

can also take place on SNSs, as SNS profiles play an important role in self-expression and identity. Interpreting secrecy, withholding and the concealment of information in the SNS context is not without difficulties as the whole functioning of these sites is powered by the share of personal information. However, through the use of privacy settings, the individual can decide to withhold from one part of the community and only share information with a chosen audience.

Certain scholars avoided providing a unique definition but defined different categories or clusters of privacy.[147] *Judith Wagner DeCew* differentiated between three clusters of privacy claims: informational privacy, accessibility privacy and expressive privacy.[148] *Jerry Kang* argued that privacy is composed of three overlapping clusters: spatial privacy (physical space), decisional privacy (choice) and information privacy (flow of information).[149] According to *József Hajdú*, privacy protection can take four forms: data protection, protection of the human body, protection of communication and protection of space.[150]

Other scholars regrouped the existing definitions into different groups: according to *Ken Gormley*, the different privacy notions that appeared after Warren's and Brandeis's ground-breaking work can be grouped into four categories: (1) privacy as the expression of one's personality, (2) privacy as autonomy, (3) privacy as the ability to regulate information and (4) privacy composed of different essential components.[151] In addition to these four categories defined by Gormley, *Éva Simon* identified two more to be added to this list: (5) concepts according to which privacy is approached from societal interests, (6) while the sixth category is composed of theories according to which the right to privacy cannot and should not be reduced to one single definition.[152]

Another study from 2013, entitled "*Seven Types of Privacy*", written by *Rachel L. Finn*, *David Wright* and *Michael Friedewald*, made a huge contribution towards how to approach privacy. In this article the authors also opted for categorizing the types of privacy in a structured, logical way instead of creating a universal definition. They based their analysis on the four privacy subsets defined by *Roger Clarke* in 1997 and revised and expanded these categories while taking into account the technological developments that occurred during the past decades. They differentiated between seven types of privacy: (1) privacy of the person, (2) privacy of behaviour and action, (3) privacy of personal communication, (4) privacy of data and image, (5) privacy of thoughts and feelings, (6) privacy of location and space and (7) privacy of association.[153] In order to be able to successfully assess the future challenges posed by new emerging technologies, the authors argued that "*[…] privacy is an inherently heterogeneous, fluid and multidimensional concept, and […] suggest that this multidimensionality may be necessary to provide a platform from which the effects of new technologies can be evaluated.*"[154]

---

147 Instead of providing a unique definition of privacy, it is worth examining what *clusters of privacy or categorization* of the definition of privacy exist, as they can provide important guidance in relation to the far-reaching nature of privacy and can improve instincts on privacy relating to which areas of life should receive legal protection.

148 Solove 2002. p. 1125. See more on their analysis in: McCullagh 2008. pp. 4–6.

149 Kang 1998. pp. 1202–1203.

150 Hajdú 2005. p. 10.

151 Gormley 1992. pp. 1137–1138.

152 Simon 2005. p. 33.

153 Finn et al. 2013. p. 7.

154 Finn et al. 2013. p. 26.

One important example of those who think that privacy should not be reduced to a single definition is *Daniel Solove's* approach. In his article, "*Conceptualizing Privacy*" he argues that instead of creating an overarching concept, privacy should be better understood as "*drawing from a common pool of similar characteristics*".[155] In his article Solove differentiated between six categories of privacy and regrouped the existing definitions into these categories. According to him, privacy can be interpreted as (1) the right to be let alone, (2) limited access to the self, (3) secrecy, (4) control of personal information, (5) personhood and (6) intimacy.[156] He pointed out that there is a problem with all these definitions: their scope is either too narrow or too broad. He emphasized that it does not mean that these concepts lack merit, the problem is that these authors use a traditional method of conceptualizing privacy, and as a result their definitions only highlight either some aspects of privacy, or they are too broad and do not give an exact view on the elements of privacy.[157, 158]

These headings defined by Solove can be understood as the main elements when it comes to the content of privacy, as knowing all these definitions, we can have a clue what areas of life privacy covers, and it can help to broaden and to improve instincts on privacy. Instead of applying these methods of conceptualizing privacy, Solove adopts a pragmatic approach by seeking to provide not one exhaustive definition but rather an approach to better understand privacy.[159] He takes into account that privacy depends on several factors – such as societal norms, technology and context – and argues that a practical approach is needed to address privacy related issues, instead of creating one overarching definition of privacy.[160]

The complexity of the subject was also highlighted by *Koop [et al.]* who have provided in their article, entitled "*A Typology of Privacy*" a typology of privacy "that is more systematic and comprehensive than any existing model."[161] In their typology they positioned the main types of privacy in a two-dimensional model, composed of the degree of privateness[162] and the spectrum of positive to negative freedom.[163] They identified eight types of privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioral privacy) and an extra "one", informational privacy which – as it overlaps but does not coincide with each identified privacy type – constitutes an overarching concept instead of a separate type of privacy.[164]

Again, these classifications are important as they can indicate that privacy in relation to SNSs cannot be reduced to one element, but several aspects of privacy gain significance in relation to SNSs (e.g. communication through using the messenger functions of these platforms, the ability to express one's personality through posting a variety of content,

---

155 Solove 2002. p. 1088.
156 Solove 2002. p. 1094.
157 Solove 2002. p. 1099.
158 Also, for the purpose of the monograph not all "types" of privacy will be relevant – for example, the privacy of the home or physical privacy – instead, focus will be put on control over information and the autonomy or self-determination of the individual.
159 Solove 2002. pp. 1126–1128, p. 1129.
160 On this approach see: Solove 2002. pp. 1129–1154.
161 Koops et al. 2017. p. 483.
162 Koops et al. 2017. p. 564.
163 Koops et al. 2017. p. 565.
164 Koops et al. 2017. pp. 566–568.

deciding who can have access to the shared content through the application of privacy settings, etc.).

(b) Factors influencing privacy

Privacy should not and cannot be interpreted in a vacuum: what is considered to be private is highly dependent on the circumstances: there are huge differences between particular societies and cultures, or scientific development can also lead to a different, urging need for ensuring the protection of privacy.[165] Different factors might influence privacy norms in a given society, such as, for example, the political, the socio-cultural and the personal level,[166] the new generations of technology and new generation of users,[167] or dimensions of time, place, economy and technology.[168] All these factors make it even more difficult to establish one single definition of privacy. Among the possible factors influencing the understating of privacy, attention will be drawn to technology, social norms and the individual and the context.

When discussing the subject of privacy, the impacts of *technological development* pose inevitable questions as privacy has a close connection to technology, making it a very fertile area of research even after more than a century.[169] Technology has always had a close connection with privacy as new innovations of technology change how privacy might be violated, as they gave rise to different kinds of privacy intrusions[170] – which is also in the focus point of the monograph. Technological innovations, such as profiling, location tracking, mobile devices, biometrics, RFID, cloud computing, etc. evoke new kinds of privacy challenges.[171] Existing threats to privacy have become increasingly important due to the growth of Internet and online activities.[172] As part of technological inventions, social media and *SNSs* will have their influence on privacy as well – but these questions will be discussed in detail in Title 2. As it will be demonstrated in relation to the possible existence of "social media law", these technological innovations do not raise the question

---

165 Fried 1968. p. 486., p. 475.

166 Westin 2003. pp. 431–434.

167 Tene 2011. p. 15.

168 UN 2016. par. 21.

169 As Robert Sprague noted, "*[o]ne of the greatest impacts on one's expectation of privacy—and, hence, one's right to privacy—is technology*." Sprague 2008. p. 89.

170 Compared to the big technological threat in the era of Warren and Brandeis, the instant camera, owned only by a few, the change is considerable: today individuals have far overstepped those challenges by carrying around in their pockets complex devices that are capable of tracking, locating and recording every move they make. (Source: Hughes 2015. p. 527.) *Lawrence Lessig* explains in one of his articles how monitoring – a natural societal phenomenon – was completely changed in its paradigm due to the technological development, by making it permanent, pervasive and recordable. (Source: Lessig 2005. pp. 55–74.) Not only scholars, but several international documents have also acknowledged the importance of human rights and among them the right to privacy in this technologically changed environment. See, for example, the UN's document "*The promotion, protection and enjoyment of human rights on the Internet.*" (United Nations, 2012, A/HRC/20/L.13) or the "Resolution adopted by the General Assembly on 18 December 2013 – *The right to privacy in the digital age*" (United Nations, 2013, A/RES/68/167). These documents reaffirm that individuals shall enjoy the same fundamental human rights – and among them the right to privacy – also in the digital and Internet era.

171 On how technology affects and challenges privacy see more in: Weber, Rolf. H.: The digital future – A challenge for privacy? *Computer Law and Security Review*, 31(2), 2015. pp. 236–239.; Tene 2011. pp. 16–21. and Türk 2011.

172 One example is identity theft, which is greatly facilitated in the online environment, compared to its offline counterpart. Source: Knight – Saxby 2014. p. 619.

of the existence of a fundamentally new online privacy law, they rather challenge existing conceptions of privacy.[173]

As technology advances, it naturally influences individuals' behaviour and *social norms* relating to privacy and expectations of privacy: social media and the unprecedented extent of online self-exposure can be mentioned as one example.[174] For example, while a few decades ago it was completely unimaginable to publicly share with an undetermined or a very high number of people what someone ate for breakfast, which itinerary this person used for his/her morning run, or who he/she is dating, today the share of such information is commonplace on SNSs.

The *individual* also plays a central role, as expectations of privacy can vary from individual to individual.[175] *Anders J. Persson* and *Sven Ove Hansson* also took into consideration the individual's expectations and they divided privacy into two parts: a core part, which is protected "by default" – regardless of the individual's acts – and a discretionary part, which is considered to be private depending on the individual's attitudes.[176] Privacy is highly dependent on the given *context* as well: *Helen Nissenbaum* emphasizes the importance of "contextual integrity" when it comes to privacy, pointing out that depending on the concrete situation, on the context in which the same information is shared might be considered private differently.[177, 178]

To conclude, all these factors, such as technology, ever-changing social norms, and perceptions of the individual, hinder the creation of a universal definition of privacy. Consequently, what is considered to be private (e.g. by a society or by an individual) is not *always* going to be subject to legal protection. Despite the lack of the ability to define privacy and despite its ever-changing nature, legal regulations must find an average standard that must receive legal protection. In *§2* these international and national legislations will be discussed.

In spite of the difficulties in creating a uniform definition, a *definition* must be adopted in order to determine what will be understood by privacy *for the purpose of the monograph*. As it became apparent, privacy can comprise different aspects. In the context of SNSs, mostly two aspects of privacy, the informational privacy and decisional privacy will gain utmost importance. Although at the outset it can be concluded that the informational aspect of the question will also be directly regulated by the right to data protection. Therefore, when addressing privacy, particular attention should be paid to autonomy, meaning the individual's right to decide on his/her own. On the basis of the above, *for the purposes of the monograph*, privacy is understood broadly, *as the control over the autonomy of the individual, meaning that the individual should be able to decide how to live his/her life*.

---

[173] The UN special rapporteur on privacy also calls attention to the re-examination of understandings of privacy, such as distinctions between "individual and collective privacy", expectations of privacy in public and in private places, with special regard to the free development of one's personality in the light of technological development. Source: UN 2016. par. 27.

[174] Tene 2011. p. 22.

[175] What one might consider as intrusion into private life – e.g. opening up about his/her relationship to a distant relative – another might consider as completely normal – e.g. sharing the same information documented in detail with photos, videos, etc. on social media with several hundreds of contacts.

[176] Persson – Hansson 2003. pp. 61–62.

[177] Nissenbaum 1998. p. 581.

[178] For example, sharing information relating to one's health might feel appropriate if the recipient is the individual's doctor, but sharing exactly same information might feel inappropriate and as an intrusion into privacy if the employer asks for the same information.

In the context of SNSs – as it will be addressed under Title 2 – it should primarily mean that the (employees') freedom to decide whether to engage in SNSs, and how he/she can use these sites (what content to share, with whom, etc).

§2. The legal regulation of the right to privacy

As it was already referred to, several international human rights agreements guarantee the protection of privacy/respect for private life.[179] In the following, the substance of the relevant *(A)* international (with the European legal order at the focus point) and *(B)* national norms will be addressed, with the aim of understanding what circumstances receive legal protection under the right to privacy.

(A) International human rights instruments

Among the United Nation's international documents ensuring the right to respect for private life, the UDHR and the ICCPR must be mentioned. Both documents guarantee the right for respect of private life by stating that it is a fundamental human right and no one shall be subjected to arbitrary interference with his/her privacy, family, home and correspondence, or to attacks against his/her honour and reputation and they have the right to protect themselves against such unlawful interference (Article 12 of the UDHR and Article 17 of the ICCPR). Certain differences exist between the wording of these provisions: for example, compared to the ICCPR, the UDHR protects only against arbitrary interference and not unlawful interference. Also, regarding honour and reputation, the UDHR gives protection against any kind of attacks, while the ICCPR ensures protection against arbitrary attacks.[180] Under the aegis of the UN, the UN special rapporteur on privacy must also be mentioned, who is an independent expert appointed by the Human Rights Council, whose task is to examine, report and raise awareness on the right to privacy.[181]

In *Europe*, two regional organisations have to be mentioned, both of them having an elaborate system and regulation: the CoE and the European Union. It is the Council of Europe's European Court of Human Rights (hereinafter referred to as: ECtHR) and the European Union's European Court of Justice (hereinafter referred to as: CJEU) which created a detailed case law.

Even though focus will be mainly put on the European legal order, it must be mentioned that it is not only Europe which ensures the right to privacy at a regional level. Article 11 of the *American Convention on Human Rights* (1969) also guarantees the right to privacy. The bodies responsible for ensuring compliance with the convention are the Inter-American

---

[179] So far, the expressions "privacy" and "right to privacy" were employed, but (European) legal regulations mostly refer to the expression "right to respect for private life". It must be emphasized that privacy and private life are not synonyms, private life supposes a narrower scope, traditionally connected to secrecy or concealment, to protection against certain interferences – as it will be presented in the following paragraphs. However, there is a tendency indicating that the right to respect for private life is understood in a broader way (see, for example, the analysis on the ECtHR's practice), incorporating also the autonomy of the individual – which matter is connected to privacy rather than to private life.

[180] Mendel et al. 2013. p. 59.

[181] UN 2015

Commission on Human Rights and the Inter-American Court of Human Rights.[182] Also, the *African Charter on Human and Peoples' Rights* (1981) can be mentioned in relation to regional human rights protection, aiming to ensure fundamental civil and political and economic and social rights in the African region.[183]

(a) ECHR and ECtHR

The centrepiece of the European protection of human rights,[184] one of the most important documents regulating the right to privacy is the *European Convention on Human Rights* (Council of Europe, 1950, Article 8), which served as a genesis for several pieces of privacy legislation throughout Europe.[185] Also, the *European Court of Human Rights* created very important case law regarding Article 8, characterized by rich legal development.[186]

The ECHR guarantees in Article 8 the right to respect for private and family life through stating 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 wellbeing 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."*

Article 8 defines four categories receiving protection: in addition to private life it contains family life, home and correspondence – which can be understood as specific aspects of private life.[187] In relation to the subject of the monograph, mostly private life and auxiliary correspondence[188] will have significant importance, amongst which, due to its ambiguous scope, the next paragraphs will focus on private life.[189]

Although the ECHR guarantees the right to respect for private life through determining when an interference cannot be established, it makes it obvious that the right to privacy is

---

[182] Mendel et al. 2013. p. 61.

[183] Velu – Ergec 2014. pp. 24–25.

[184] Moderne 2012. p. 2.

[185] Rustad – Paulsson 2005. pp. 870–871.

[186] Schabas 2015. p. 366.

[187] Velu – Ergec 2014. p. 659.

[188] The most important relevant decisions in relation to correspondence will be addressed in Part II. when examining SNS use during working hours. However, it must be emphasized that under correspondence protection is afforded not only to traditional letters, but rather to communication in general, regardless of the form it takes. As such it covers, for example, telephone conversations, telegraphs, electronic and radio electronic means of communication. (Source: Velu – Ergec 2014. p. 691.) See more on the ECtHR's jurisprudence on communication in: CoE 2019. pp. 91–111.; Velu – Ergec 2014. pp. 687–691.

[189] Family life covers matters such as marriage, parenthood, relationship between parents and children, imprisonment of parents, etc. Home covers matters such as peaceful enjoyment of one's home (protection against environmental nuisances), or expulsions, while correspondence covers matters such as telephone interception, traditional and electronic messages. See more on these rights in: Schabas 2015. pp. 388–401.

not an absolute right.[190] When the ECtHR examines whether there was a violation of Article 8, it examines two conditions in its decisions: first, whether there was an interference with the right to respect for private life under Paragraph 1 of Article 8 and second, whether the interference was legitimate according to the criteria set in Paragraph 2.[191]

Being a broad notion, private life encompasses numerous aspects, making it difficult, if not impossible, to provide an exhaustive definition.[192] The ECtHR is on the position that it is not "*possible or necessary to attempt an exhaustive definition of the notion of 'private life'*"[193] and argued on several occasions that the concept of private life "*is a broad term not susceptible to exhaustive definition,*"[194] as Article 8 covers very broad areas of life, "*encompassing the sphere of personal autonomy within which everyone can freely pursue the development and fulfilment of his or her personality and to establish and develop relationships with other persons and the outside world.*"[195]

Also, the technological and scientific developments that appeared after the adoption of the ECHR encouraged the ECtHR to create a flexible interpretation of private life under the current circumstances.[196] The preamble of the ECHR itself declares that its aim is to guarantee and further develop human rights,[197] suggesting the constant evolution of the rights guaranteed in the text of the ECHR, ensuring that the ECHR is interpreted in the light of the era.[198] Societal changes,[199] and the development of ICT technologies[200] led to a broad interpretation of private life, responding to the occurring changes,[201] and implying that with the constantly changing societal-economic conditions, what falls under the scope of Article 8 also changes.

As a result, the ECtHR goes beyond the "traditional" interpretation of private life connected mainly to intimacy/secrecy[202] and also guarantees the respect of certain public aspects of the individual's private life.[203] Thus, protection is also afforded to the autonomy of the individual and to the development of personality, which can be manifested in establishing relationships with others, or can even cover professional activities.

---

190 Paragraph 2 of Article 8 of the ECHR; Kéfer – Cornélis 2009. p. 786.

191 See more on the legitimate interference and Article 8 of the ECHR: Grád, András – Weller, Mónika: *A strasbourgi emberi jogi bíráskodás kézikönyve*. HVG–ORAC Lap- és könyvkiadó, Budapest, 2011. pp. 448– 456., pp. 483–526.; Pettiti – Decaux – Imbert 1995. pp. 323–351.

192 Velu – Ergec 2014. p. 659.; Sudre 2015. p. 101.

193 ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.

194 ECtHR: *Pretty v. the United Kingdom*, application no. 2346/02, 2002. par. 61.; ECtHR: *Peck v. the United Kingdom*, application no. 44647/98, 2003. par. 57.; ECtHR: S. and Marper v. the United Kingdom, application nos. 30562/04 and 30566/04, 2008. par. 66.

195 ECtHR: *Jehovah's witnesses of Moscow and Others v. Russia*, application no. 302/02, 2010. par. 117. See also: ECtHR: *Evans v. the United Kingdom*, application no. 6339/05, 2007. par. 71.

196 Grabarczyk 2011

197 Pettiti – Decaux – Imbert 1995. p. 308.

198 Velu – Ergec 2014. p. 33., p. 49.

199 Sudre 2015. p. 101.

200 Moderne 2012. p. 29.

201 CoE 2019. p. 20.

202 Velu – Ergec 2014. p. 659. This concept is closely connected to a so-called inner circle "*in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle*". (Source: ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.)

203 CoE 2019. p. 20.

In relation to the matters belonging to the scope of private life,[204] different authors created different categorisations. However, despite the exact appellations of these categories, a common feature is that the "traditional" protection of private life appears alongside with ensuring the protection of matters having a connection with the outside world. From the relevant case law *Olivier Rijckaert* and *Noël Lambert* identified three sub-divisions of the right to respect for private life from the ECtHR's jurisprudence: the right to intimacy, the right to maintain social relationships and the right to self-determination.[205] According to *Rusen Velu* and *Jacques Ergec*, two elements of private life exist: *first*, the right to respect for private life, which aims to ensure the individual a sphere where third persons do not have access, connected to secrecy; and the *second* element is related to the relationships that the individual can make with others. Both of these aspects aim to ensure the protection of the personality of the individual.[206] *Frédéric Sudre* differentiates between four areas:[207] the *first* is the right to privacy ("le droit à la vie privée personnelle"), which is composed of the right to the intimacies of private life and of the right to the liberty of sexual life. The *second* area is the right to a social private life, covering the establishment of relationships with others, as well as professional activities. The *third* area is the right to personal developments, which involves areas such as knowing one's origins, or choosing how to end one's life. The *fourth* area guarantees the right to live in a healthy environment. A study published by the *CoE* differentiates between three categories: physical, psychological and moral integrity of the individual, private life and identity and autonomy.[208] *Martyn Bond* takes a different approach and differentiates between rights requiring certain protection of the individual ("droit d'être à l'abri") and freedoms ("libertés"). Amongst the rights, he notes that individuals have the right to be free from attacks against physical and psychological integrity, the right to be free from unwanted information gathering practices and the right to be free from serious environmental nuisances. The two freedoms relate to the right to develop relationship with others and the freedom in choosing one's lifestyle.[209]

---

[204] The ECtHR stated in its case law that interference in the following conditions of life fell under the scope of Article 8 (and further examined whether the interference was legitimate or not as it is not an absolute right): access to personal data (ECtHR: *Leander v. Sweden*, application no. 9248/81, 1987, par. 46., par. 48.; ECtHR: *Gaskin v. the United Kingdom*, application no. 10454/83, 1989, par. 36–37.), telephone interception (ECtHR: *Klass and Others v. Germany*, application no. 5029/71, 1978, par. 41.; ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 41., par. 44., par. 46.; ECtHR: *Malone v. the United Kingdom*, application no. 8691/79, 1984, par. 64.; ECtHR: *Huvig v. France*, application no. 11105/84, 1990, par. 25.; ECtHR: *Kruslin v. France*, application no. 11801/85, 1990, par. 26.), physical and moral integrity (ECtHR: *X and Y v. The Netherlands*, application no. 8978/80, 1985, par. 22.), protection of image (ECtHR: *Reklos and Davourlis v. Greece*, application no. 1234/05, 2009, par. 40.), choice or change of name (ECtHR: *Guillot v. France*, application no. 22500/93, 1993, par. 21–22.; ECtHR: *Burghartz v. Switzerland*, application no. 16213/90, 1994, par. 24.), sexual life (ECtHR: *Dudgeon v. the United Kingdom*, application no. 7525/76, 1981, par. 40–41.), profession or domicile (ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 28–33.), honour and reputation (ECtHR: *Chauvy and Others v. France*, application no. 64915/01, 2004, par. 70.), protection against environmental nuisances (ECtHR: *López Ostra v. Spain*, application no.16798/90, 1994, par. 51.), the right to establish and develop relationships with others (ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.).

[205] Rijckaert – Lambert 2012. pp. 6–7.

[206] Velu – Ergec 2014. p. 660.

[207] Sudre 2015. pp. 101–104.

[208] CoE 2019. p. 20.

[209] Bond 2018. p. 39.

Although the ECHR and Article 8 do not contain a *right to self-determination* as such, the ECtHR found that it remains an important principle when it comes to interpreting Article 8 – altogether with the concept of quality of life.[210] Physical and moral integrity is guaranteed through ensuring the development of the personality of the individual without outside interference.[211] Personal autonomy comprises the right to establish details of the individual's identity as a human being.[212]

Albeit the formulation of Article 8 suggests a negative right, the right to be left alone,[213] the interpretation of the ECtHR acknowledges that private life can comprise a zone of interaction between individuals, even in the public context.[214] Establishing and developing relationships is closely related to the development and fulfilment of one's personality.[215] Article 8 also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.[216] Dress and other "public" features – the desired appearance of the individual – might also concern private life, as it can constitute a way of expressing one's personality.[217] Article 8 is not limited to the protection of a mere inner circle rigidly delimiting the individual and the public, outside world; it rather ensures the right to establish and develop relationships with others.[218] Such observations have high topicality and importance in the age when social media might be considered an important area of self-expression and establishing relationship with others.[219]

The ECtHR explicitly addressed the right to privacy in the employment context with regard to employee monitoring in several cases, such as Niemietz v. Germany (1992),[220] Halford v. United Kingdom (1997),[221] Copland v. the United Kingdom (2007),[222] Bărbulescu v. Romania (2017),[223] Libert v. France (2018).[224] These cases, and the analysis of where the boundary of employee privacy lies will be addressed in detail in Chapter 2 focusing on workplace privacy.

---

[210] ECtHR: *Pretty v. the United Kingdom*, application no. 2346/02, 2002. par. 61. and par. 65.
[211] Schabas 2015. p. 370.
[212] ECtHR: *Christine Goodwin v. the United Kingdom*, application no. 28957/95, 2002., par. 90.
[213] Schabas 2015. p. 366.
[214] ECtHR: *Von Hannover v. Germany*, applications nos. 40660/08 and 60641/08, 2012. par. 95. Also see more on how Article 8 includes intimacy, social aspects and environmental well-being in: Bugorgue-Larsen, Laurence: *La Convention européenne des droits de l'homme*. 2nd edn. LGDJ, Issy-les-Moulineaux, 2015. pp.133–142.
[215] Commission of the ECtHR: *X v Iceland*, application no. 6825/74, 1976
[216] ECtHR: *Peck v. the United Kingdom*, application no. 44647/98, 2003. par. 57.
[217] ECtHR: *S.A.S. v. France*, application no. 43835/11, 2014. par. 107.
[218] ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992
[219] To be further addressed in Title 2 how privacy and private life should be understood in the social media age.
[220] ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992
[221] ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997
[222] ECtHR: *Copland v. the United Kingdom*, application no. 62617/00, 2007
[223] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017
[224] ECtHR: *Libert v. France*, application no. 588/13, 2018

(b) EU and the CFREU

The EU's main human's rights document, the *CFREU* also guarantees in Article 7 the protection of private life.[225] Article 7 reads as follows:

> *"Everyone has the right to respect for his or her private and family life, home and communications."*

Similarly to other international legal documents, the CFREU identifies the "traditional" interests that must be protected: private life, family life, home and communications.[226, 227] In the EU as well, the right to respect for private life is not absolute, as Article 52 of the CFREU contains a provision in relation to the possible limitation of the rights recognized by the CFREU, making it possible to limit these rights if certain conditions are met.[228]

The CFREU has a close connection with the ECHR, as according to Article 52(3) the rights which also appear in the ECHR have the same meaning and scope in the Charter, too.[229] However, this implies a minimum requirement: the EU can grant a higher level of protection compared to the ECHR.[230] Also, the CJEU refers many times intentionally to the practice of the ECtHR,[231] as the content of privacy can be derived from the case law of the ECtHR.[232]Also, it is not uncommon for scholars to refer to the case law of the ECtHR when it comes to analysing the case law of the CJEU.[233]

As such, Article 7 of the CFREU corresponds to Article 8 ECHR, as the wording of the CFREU reflects Article 8 of the ECHR, with one difference. The CFREU is deliberately broader in a way that it does not employ the expression "correspondence" but refers to "communications", as it has taken into account the technological changes that occurred.[234] However, from a substantial point of view it does not make a difference, as the ECtHR interpreted the expression "correspondence" broadly to all communications.[235]

For the above reasons, as regards the meaning of "private life" it is identical to the interpretation of the ECtHR, meaning that none of the court interprets "private life"

---

[225] However, even prior to the CFREU, the right to privacy was a recognized general principle of the EU law. See, for example: CJEU: Case C-62/90, 1992. par. 23.; CJEU: Case 136/79, 1980. (Source: Cariat 2017. p. 162.)

[226] Nyman-Metcalf 2014. p. 28.

[227] Incidentally, other articles can also aim at the protection of private life, such as Article 3 on the right to the integrity of the person, Article 8 on the right to data protection, Article 24 on the rights of the child and Article 37 on environmental protection. Source: Lock 2019. p. 2115.

[228] Article 52 of the CFREU: Scope of guaranteed rights "*1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*"

[229] Naturally, the CFREU is not a simple repetition of the ECHR but introduces certain new rights – such as the right to data protection for example. Source: Gaïa 2004. p. 234.

[230] Cariat 2017. p. 163.

[231] See, for example: CJEU: *Case C-400/10*, 2010. par. 53.; CJEU: *Case C-275/06*, 2008. par. 64.

[232] Gellert – Gutwirth 2013. p. 524.

[233] See, for example: Lock 2019. pp. 2115–2120.; Eriksson 2006. pp. 78–89.; Nyman-Metcalf 2014. pp. 21–36.

[234] *Explanation on Article 7. Explanations relating to the Charter of Fundamental Rights* (2007). 2007/C 303/02.

[235] Lock 2019. pp. 2119–2120.

restrictively.[236] The preamble of the CFREU explicitly states that the strengthening of fundamental rights must take place in the light of the changes in society, social progress and scientific and technological developments, ensuring a dynamic interpretation of the right to respect for private life.[237] As such the ECtHR can serve as example,[238] private life covers certain aspects of professional and commercial activities, can relate to the health status of the individual, relationships with others, marital status, physical integrity, reputation, image of the individual, family name, sexual orientation.[239]

(B) National legislations

After addressing how privacy is understood in the most important international organisations, it is necessary to have a look at national legislations. First *(a)* common characteristics – such as affording constitutional and civil law protection will be addressed, then *(b)* the specific, unique features of each country will be examined in detail.

(a) Protection of private life in France and in Hungary

Private life can be assessed as opposing to collective life: traditionally private life was conceived as "*[...] the individual's right to dispose a private space, distinct from the collective life of the community.*"[240] In *France*, the Constitutional Council opted for a particular interpretation, adopting a restrictive approach: it links private life to the concept of secrecy – unlike national lower courts and the jurisprudence of the ECtHR.[241] In this regard, the right to respect for private life is understood as protection against public or private intrusions into the intimate sphere of the individual,[242, 243] but it does not include the freedom of private life.[244] *Vincent Mazeaud* points it out that the Constitutional Council's practice was initially centred around the concept of secrecy and mainly focuses on aspects such as domicile, correspondence or intimacies of private life, aspects where the concept of secrecy dominates.[245] In its jurisprudence, the Constitutional Council examined matters in relation to intrusion and divulgation, such as intrusion into the home, search of vehicles, camera surveillance, GPS localisation, data protection or intercepting communication.[246]

However, despite the prevailing concept of secrecy in the jurisprudence of the Constitutional Council, when examining the doctrine, several authors differentiate between

---

[236] Kokott – Sobotta 2013. p. 223.
By contrast, *Christophe Vigneau* notes that it is not precluded that certain public spheres of private life are excluded from the protection of private life. Vigneau 2006. p. 120.

[237] Lock 2019. p. 2115.

[238] Eriksson 2006. p. 78.

[239] Cariat 2017. pp. 165–168.

[240] Détraigne – Escoffier 2009. p. 11. However, as it will be discussed in Title 2, SNSs considerably challenge the boundaries of private and public life, posing new challenges in defining the limits of private life.

[241] Source: Mazeaud 2015. pp. 16–17.

[242] Commentaire: Conseil constitutionnel: décision n° 2012-248 QPC du 16 mai 2012

[243] According to Hubert Alcatraz, the right's original aim is to ensure a "*bubble of secrecy around the individual*". Cited in: Favoreu et al. 2015. p. 273.

[244] Favoreu et al. 2015. pp. 273–275.

[245] Mazeaud 2015. p. 8.

[246] Mazeaud 2015. p. 9.; Favoreu et al. 2015. p. 277.

two layers or "spheres" when it comes to private life: a hard core,[247] closely connected to the concept of secrecy and another layer, moving beyond the narrow concept of secrecy. *Vanessa Barbé* distinguished between *personal private life* and *social private life*.[248] *Xavier Bioy* interpreted the hard core as "*to be let alone*", which refers to matters such as correspondence, inviolability of the home – and also data protection. To this hard core, the *right to autonomy of private life* is added, comprising fields such as the freedom to choose an occupation, identity or relations.[249] *Florence Crouzatier-Durand* enumerated elements pertaining to the *protection* of private life and to the *expression* of private life.[250] For *Laurence Burgorgue-Larsen*, the hard core is associated with *intimacy and secret*, encompassing protection against intrusions and divulgations. It is completed by recognizing *personality* – not the right to personality – by attaching the right to respect for private life to the legal fundaments of personal liberty.[251]

In Hungary the Constitutional Court clarified the content of the right to privacy in several decisions, among which the most important ones will be addressed.[252] In *decision No. 8/1990 (IV. 23.)*, the Constitutional Court linked the right to privacy to the right to human dignity[253] and considered the latter to be the formulation of the general right to personality and then identified the right to privacy as one aspect of it.[254] In *decision No. 56/1994 (XI. 10.)*, the Constitutional Court identified the "right to the freedom of privacy" ("magánélet szabadságához való jog") as a fundamental right aiming to ensure the protection of the autonomy of the individual, originating from the inherent human dignity.[255] In a decision relating to secret collection of information,[256] the Constitutional Court extended the scope of protection ensured by the right to privacy to the intimate/private sphere, to communication, to the home and to the right to reputation.[257, 258]

In relation to camera surveillance,[259] *László Kiss* and *István Kukorelli* expressed in a dissenting opinion their view regarding surveillance as the exercise of informational power, drawing attention to the negative consequences of such a monitoring and its adverse effects on individuals' behaviour. Although the decision relates to CCTV monitoring and dates back to 2002, one paragraph already referred to how this monitoring affects and changes

---

247 When assessing what constitutes the *hard core of respect for private life*, the Code on Internal Security and the Penal Code could serve as useful reference. Articles 226-1–226-7 of the Penal Code provide protection against different invasions of privacy, such as against the home, against image or words uttered, against identity theft, while Subsection 1 of Article L801-1 of the Code on Internal Security stipulates that "*[t]he respect of private life and all of its components, notably the secrecy of correspondence, the protection of personal data and the inviolability of the home are guaranteed by law.*" Source: Bioy 2016. pp. 496–497.

248 Barbé 2018. pp. 112–121.

249 Bioy 2016. pp. 496–497

250 Crouzatier-Durand 2013. pp. 58–72.

251 Burgorgue-Larson 2005. p. 72.

252 See more on the relevant decisions of the Constitutional Court in: Majtényi 2002. pp.72–78.; Szüts – Karsai – Mándi 2006. pp. 222–229.

253 Sári – Somody 2008. p. 127.

254 Lábady 1995. p. 85.; Majtényi 2008. p. 277.

255 Decision No. 56/1994 (XI. 10.) of the Constitutional Court, Part II.; Fézer 2014. p. 263.

256 Decision No. 32/2013. (XI. 22.) of the Constitutional Court

257 Decision No. 32/2013. (XI. 22.) of the Constitutional Court, par. 84.

258 However, *Béla Pokol* expressed his parallel reasoning regarding this reasoning and found that the Constitutional Court overstepped its competence and created a general right to privacy from the separate rights declared in the Fundamental Law. Par. 143. of Decision No. 32/2013. (XI. 22.) of the Constitutional Court

259 Decision No. 35/2002. (VII. 19.) of the Constitutional Court

the boundaries of private life[260] – gaining particular importance in the social media era. In another decision relating to camera surveillance, the Constitutional Court stated that "*the core element of privacy is that no intrusion or insight into the private sphere of the individual shall be conducted against his or her will*". In the case of an unwanted intrusion not only the right to privacy is infringed but also other aspects of the right to dignity (e.g. self-determination or physical and personal integrity of the person).[261]

Traditionally, civil law aims to provide protection to this already mentioned "hard core", governed by the concept of secrecy.[262] Article 9 of the *French Civil Code* regulates the right to respect for private life.[263] Although in paragraph 1 the expression right to respect for private life is used, paragraph 2 uses a confusing expression and refers to "*the infringement of the intimate character of private life*." Historically, France has a narrow conception of privacy, based on the concept of secret (the right to the secrecy of private life) – and treated questions such as family, sex, identity and self-determination separately from privacy.[264] *Jean Carbonnier* understood it as a secret sphere of life from which the individual can exclude third persons, where he/she could be left alone.[265]

The elements of private life cannot be exhaustively defined, "*every arbitrary interference in one's private life is unlawful*".[266] The right to respect for private life[267] is not an absolute right: it has to be balanced against other rights.[268] Also, although "*every person, regardless of their rank, wealth, current or future functions, has the right to respect for his/her private life*",[269] the limits of that protection can vary according to the status of the given person. Private life can cover elements such as domicile, correspondence, the body, image, health, personal convictions, family life, marital life, sexual life, identity (name, sex, origins).[270] Although recently a broader definition was provided by *Jean-Christophe Saint-Pau* (according to whom the right to respect for private life can be defined as the individual's right to demand the State and other individuals to respect his/her freedom to act and as

---

260 "*By the end of the 20th century, this form of control has become widespread in both the public sector and the business sector. The almost constant surveillance redefines the boundaries of private life. It becomes traceable how and with whom we spend our free time; with whom, when and about what we are talking; what kind of newspapers we read or what other habits we have. The risk relating to the misuse of technical achievements does not appear as a threat only on the part of the state, the private sector also uses camera surveillance as a means of increasing efficiency.*"

261 Decision No. 36/2005. (X. 5.) of the Constitutional Court

262 Burgorgue-Larson 2005. p. 72.

263 Article 9: "*Everyone has the right to respect for his or her private life.*
Without prejudice to the right to recover indemnification for injury suffered, judges may prescribe any measures, such as sequestration, seizure and others, suited to the prevention or the ending of an infringement of the intimate character of private life; in case of emergency those measures may be provided for by summary proceedings."

264 Bioy 2016. p. 493.

265 Carbonnier 1971. p. 254.

266 Cour de cassation, chambre civile 1, 6 mars 1996, N° 94-11273

267 Here again, various terminologies are used: secrecy of private life, freedom of private life, respect for private life (incorporating the former two notions). Kayser 1995. p. 17.

268 Alleaume 2016. p. 454.

269 Cour de cassation, chambre civile 1, 23 octobre 1990, N° 89-13163

270 See more on the content and regulation of (the right to respect for) private life: Alleaume 2016. pp. 453–464.; Saint-Pau, Jean-Christophe: *Le droit au respect de la vie privée*. In: Saint-Pau, Jean-Christophe (ed.): Droits de la personnalité. LexisNexis SA (Traités), Paris, 2013. pp. 673–943. On the notion of private life defined by courts in: Lepage, Agathe: *Droits de la personnalité*. Répertoire de droit civil. Dalloz 2009. par. 67–95.

the secrecy of personal information),[271] traditionally the Civil Code's right to respect for private life was centred around the concept of secrecy – and originally, the Social Chamber of the Court of Cassation took over the secrecy concept of private life.[272]

The *Hungarian Civil Code* affords protection to the right to respect for private life (and to the right to data protection) on the ground of personality rights. It is the primary objective of personality rights to ensure protection to rights which make humans human, which are parts of human personality, without examining the societal circumstances – excluding from their scope political, cultural and social rights.[273] The essence of personality rights is to ensure the free expression of the personality and to prevent anyone from hindering, within the limits that the community imposes.[274] Naturally, the exercise of these rights is not without limits, it is in accordance with their social purpose only if it does not infringe other individuals' rights or laws guaranteeing these rights.[275]

The Civil Code states in general the protection of personality rights by declaring that "*[e]veryone is entitled to freely practice his or her personality rights, in particular the right to privacy and family life, home and communications with others in any way or form, and the right to protection against defamation of character, within the framework of the law and within the rights of others, and to not be impeded by others in exercising such rights.*"[276] The Civil Code identifies a list of infringements of personality rights, although the legal protection is extended also to the personality rights not identified in the Civil Code. Among the specified infringements of personality rights, the infringement of private life and of the right to data protection is mentioned.[277]

The right to respect for private life is one of the most private components and one of the manifestations of the single and indivisible personality.[278] According to Hungarian jurisprudence, interference in the private life of the individual infringes personality rights if it is arbitrary, unjustified and unnecessary. An interference is considered to be arbitrary if it expressly contradicts the will and intention of the person concerned or he/she is not aware of it and if it is not justified based on the carefully assessed circumstances.[279] In another decision, the High Court of Budapest ("Fővárosi Ítélőtábla") interpreted the right to privacy as the individual's right to decide about his/her faith, actions, body and information relating to him/her.[280] The individual shall be able to decide whether to show himself/herself to the world or whether to hide from it.[281] By this, the High Court basically identified this right with the right to informational self-determination.[282]

---

271 Saint-Pau 2016. par. 26.
272 Savatier 1992. p. 330.
273 Fézer 2014. p. 250.
274 Petrik 2014. pp. 173–174.
275 BH. 1992.387.
276 Subsection (1) of Section 2:42 of the Hungarian Civil Code
277 Items b) and e) of Section 2:43 of the Hungarian Civil Code
278 Görög 2016. p. 61.
279 LB Pfv. IV. 21 028/2000. – BH2001/61.
280 Fővárosi Ítélőtábla 2.Pf.20.429/2010/3
281 Fézer 2014. p. 264.
282 Sulyok 2017. p. 224.

(b) Specificities of national legislations

In addition to this general apprehension of the right to privacy, both France and Hungary have unique assets to address the question of privacy protection. This uniqueness is especially present in French law, where in the employment context the notion of personal life has substituted the notion of private life since 1997[283] – while in Hungarian labour law there is no distinction between the concepts of private life or personal life. In Hungary, the adoption of the Act on the protection of private life[284] can be mentioned as a "national specificity". Since the adoption of this act, the protection of private life is not only ensured by the Fundamental Law and the Civil Code but also constitutes the subject of a separate act, hitherto inexistent.[285]

(a) The concept of personal life in French labour law

Even though the right to respect for private life has been guaranteed in the French legal system since 1970, during the decades courts had to establish the boundaries of exercising employees' rights in opposition to the employer's legitimate interests and powers, as employees' rights can only be exercised consistently with these powers and with the legitimate interests of the undertaking. Balance should be found between these two sides, closely connected to the concepts of professional life and the personal life of the employee.[286]

The complete separation of professional and private spheres is not possible: private life flows into professional life and vice versa. By concluding an employment contract, the employee partially resigns his/her liberties – but keeps an inalienable part of them, an inherent condition of being a human.[287] Also, following from the rights and obligations of the parties of the employment relationship, as the employer must respect employees' rights within the workplace, the employee must also accept certain limitations while acting outside of the workplace.[288]

Attempts to separate these two spheres have come a long way.[289] Traditionally, the first distinction was made between professional life and *extra-professional life* ("vie extraprofessionnelle"),[290] making a distinction between the acts of the employee in the workplace and outside of it. Then the concept of extra-professional life was replaced by the respect for *private life* ("vie privée"), to finally settle with the concept *personal life* ("vie personnelle").

---

283 Waquet 2002. p. 6.

284 Act LIII of 2018

285 Although in French law private life is not regulated by a specific act, the adoption of the Act for a Digital Republic in 2016 should be mentioned, which contains a chapter entitled "protection of private life online". However, as the act mainly focuses on data protection and information society, its relevant provisions will be further addressed in Section 2.

286 Pizzio-Delaporte 2001. p. 404.

287 Rivero 1982. p. 422.

288 Adam 2013. p. 436.

289 The first case regarding the opposition between personal life and professional life can be traced back to 1955, when a worker was dismissed due to statements he made in his private space. The Court of Cassation declared that the dismissal violated the worker's freedom of opinion, as with his acts he did not exceeded the limits of his individual powers. Source: Bello 2012. p. 13.

290 This expression was first used by *Michel Despax* in 1963 in his article entitled "La vie extra-professionnelle du salarié et son incidence sur le contrat de travail" [*Juris-Classeur Périodique. La Semaine Juridique. éd. G.*, (1776)].

Although the concepts of both extra-professional life and private life have their own merits, in themselves they were not suitable to ensure the protection required.[291] The notion of *extra-professional life* covered the acts of employees conducted *outside the workplace*, opposing to professional life, conducted within the workplace; in principle firmly separating the extra-professional and the professional life of the employee.[292] As it was contested, this notion did not take into consideration that within the workplace, too, employees have their rights to a certain degree.[293]

Then, the notion of extra-professional life was replaced by the notion of *private life*. On the 20th November 1991, the Court of Cassation confirmed the first time the principle that "*an employee cannot be dismissed for a reason originating from his/her private life*".[294] In 1992 this principle was reinforced, and was completed with a direct reference to Article 9 of the Civil Code.[295] Although *private life* can cover acts taken within the workplace, it did not protect the extra-professional life as such, instead was primarily centred on the concept of secret, covering only the intimacies of the person. Therefore, it did not cover acts relating to the public life of the employee, such as participating in a political reunion, practicing religion, etc.[296]

For these reasons, adopting the *notion of personal* life was a logical and welcomed step.[297] The notion of personal life therefore became the terminology used – specific to labour law[298] – to describe the spheres of the employee's life that are not subject to the subordination.[299] This notion of personal life was elaborated by *Philippe Waquet*[300] and was later adopted by the Court of Cassation. In 1997 the Court of Cassation noted that "*the acts of the employee pertaining to his/her personal life cannot constitute a reason for dismissal*",[301] referring to personal life for the first time. Soon, it reinforced this principle in another decision stating that an element pertaining to the personal life of the employee cannot constitute a fault ("faute").[302, 303]

Personal life encompasses not only the private life, but also the public life of the employee, and not only outside the workplace, but also within the workplace, during working hours. Personal life is composed of private life (e.g. home, secrets, correspondence), the exercise of civil rights (e.g. marriage, divorce, properties) and the exercise of civil liberties (e.g. political life, participating in associations).[304]

---

[291] Waquet – Struillou – Pécaut-Rivolier 2014. p. 183.
[292] Despax 1963. par. 2.
[293] Waquet – Struillou – Pécaut-Rivolier 2014. p. 183.
[294] Cass. soc., 20 novembre 1991, N° 89-4460
[295] Cass. soc., 22 janvier 1992, N° 90-42517
[296] Waquet 2003. pp. 116–117.
[297] Pizzio-Delaporte 2001. p. 406.
[298] Indeed, private life is a civil law concept – alien in labour law, while personal life and professional life are concepts unknown to civil law. Molfessis 2004. p. 31.
[299] Waquet 2001. p. 513.
[300] Waquet 1994. p. 289.
[301] Cass. soc., 14 mai 1997, N° 94-45473
[302] Cass. soc., 16 décembre 1997, N° 95-41326
[303] However, as *Agathe Lepage* pointed out, the Court of Cassation was not always consistent with the use of the expressions of personal life and private life: that the latter was still used after the general acceptation of the expression personal life. Lepage 2006. pp. 373–374.
[304] Waquet 1994. p. 290.

Private life is located at the core of personal life: it encompasses the "secret" part of the employee's life – in accordance with the traditional conception of private life – such as sentimental relations, correspondence or domicile.[305] But the concept of personal life does not stop here: it aims to provide protection to the "*irreducible core of autonomy*"[306] of the employee. Acknowledging the impossibility to define the exact scope of the elements pertaining to personal life, *Waquet* notes that physical appearance, free time activities, consumer activity, militant and sport activity, religious activities all make part of personal life.[307] These activities are not secret at all: they all take place in the light of the public, constituting the *public life* of the employee.

The primary principle of the concept of personal life (private life and public life) is to ensure that in his/her extra-professional life (beyond working hours), the employee is free to act as he/she wishes. However, personal life is also present in the professional life of the employee: at the workplace, during working hours. The Court of Cassation explicitly stated in its famous Nikon decision that "*[…] the employee is entitled, even at the time and place of work, to respect for his/her private life […]*"[308] In principle, activities not having a secret character are also protected under the scope of personal life even within the workplace: e.g. talking with colleagues, choices relating to physical appearance, etc.

The significance of the elaboration of the notion of personal life is that through its application the Social Chamber has broken with the civil law – secrecy based – concept of privacy. Instead, personal life incorporates not only private life, but also the public private lives of employees. In this regard this notion is similar to the ECtHR's interpretation of privacy. As a result, when it comes to the protection of employees' rights, a forward-thinking notion is applied.

Despite the recognition of protecting employees' personal life, it does not guarantee its inviolability without barriers: even in his/her personal life, the employee is bound by certain obligations (e.g. obligation of loyalty): both in his/her professional life and extra-professional life. As it was already stated, in such cases a balance must be found between the employer's legitimate economic interests and the employees' rights. Establishing the balance with regard to SNSs will constitute the main subject of Part II.

(β) Hungarian Act on the Protection of Private Life

In order to ensure the effective protection of private life in the light of the seventh amendment of the Fundamental Law, the Hungarian Parliament adopted Act LIII of 2018 on the Protection of Private Life (hereinafter referred to as: Privacy Act).[309] The Privacy Act lays down aims pervading the entire legal system in order to ensure a more comprehensive protection of private life and refers to the essential elements of this right, laid down in

---

[305] Waquet 2003. p. 122.

[306] Waquet 2004. p. 25.

[307] Waquet 2003. pp. 123–124.

[308] Alhough this judgement employs the expression private life and not personal life. The *Nikon case* aimed to protect employees' correspondence within the workplace, by stating that the right to respect for private life "*[…] implies the secrecy of correspondence*." On the same day, in the *Abram case* (Cass. soc., 2 octobre 2001, N° 99-42727), the Court of Cassation also addressed the question of another inherent part of private life by limiting the expansion of professional life into the employee's home ("*the employee is not obliged either to accept to work from home, or to install there folders and work equipment*").

[309] 2018. évi LIII. törvény indokolása a magánélet védelméről

different acts,[310] such as the Civil Code, Penal Code and Data Protection Act.[311] In addition, the Privacy Act guarantees that the fundamental rules regulating the protection of private life shall only be stated in acts, and the laws governing the right to privacy shall be interpreted in accordance with the Fundamental Law and with the Privacy Act itself.[312]

According to the Privacy Act, the *right to private life* is part of the right to the free development of personality and means that the individual has the freedom to responsibly and independently shape his/her life and to create and preserve human relationships.[313] It is the essence of the right to private life that – with the exceptions specified in a separate Act – against the will of the individual others cannot breach it.[314]

The aim of the right to respect for private life is to protect especially the right to bear a name, personal data, private secrets, image and voice recordings, honour and good reputation.[315] Its infringement can occur especially through the abuse of personal data, secret, image and voice recording intended to be protected by the individual in relation to his/her private life and through the infringement of honour and good reputation.[316]

Relating to the research subject, the act contains one considerable *novelty*. The preamble of the Privacy Act acknowledges that the tools of ICT changed the way of communication, and that the protection of private life is extended to physical and to online harassment as well. Although it relates to harassment, after the preamble it states that the individual's dignity and right to respect for private life shall be ensured in social media as well. For this reason, the legislator's intention guarantees the security of the private sphere regarding content shared and published for private purposes. Subsection (3) of Article 8 of the Privacy Act stipulates that personal data provided on the Internet for exclusively private purposes can be processed based on the unambiguous consent of the data subject, except for the cases of mandatory processing.

The general reasoning of the Privacy Act gives no guidance regarding the exact meaning of these provisions: it only declares that in addition to the traditional forms of harassment, protection against every form of online harassment should be guaranteed.[317] In the reasoning relating to Article 8, it is stated that the general principle according to which it is the essence of the right to respect for private life – unless otherwise prescribed by law – that it shall not not be infringed by others applies here, too.

It is too early to assess the implications of the Privacy Act, due to the lack of doctrine and jurisprudence because of its recent adoption. Although at first sight it might be welcomed that an act assembles the existing regulations in relation to privacy present in different acts;[318] substantially, except for a few provisions,[319] the Privacy Act does not bring essential novelty. It is forward-thinking to declare that the online world merits protection just as

---

310 2018. évi LIII. törvény indokolása a magánélet védelméről

311 Section 6 of the Privacy Act

312 2018. évi LIII. törvény indokolása a magánélet védelméről

313 Subsection (1) of Section 2 of the Privacy Act

314 Subsection (3) of Section 2 of the Privacy Act

315 Subsection (1) of Section 8 of the Privacy Act

316 Subsection (2) of Section 8 of the Privacy Act

317 2018. évi LIII. törvény indokolása a magánélet védelméről

318 As it was, for example, expressed by *Mariann Arany-Tóth*. Source: Arany-Tóth 2019. p. 34.

319 See the provisions relating to social media. Besides, the rules relating to public figures was considerably changed, as now the protection of their private life is strengthened through the stricter separation of their public life and private life. [Preamble and Subsection (2) of Section 7]

the offline world, however, even without the declaration of that principle this was a rule deduced from the general rule of law.

Also, the Privacy Act employs different terminology, sometimes in a confusing manner. For example, in the very first paragraph of its preamble, the act refers to two notions [right to respect for private life ("magánélet tiszteletben tartásához fűződő jog") and right to privacy ("magánélethez való jog")]. In the third paragraph the expression "private sphere" ("privátszféra") is employed, without giving further explanation regarding the meaning or scope of this notion, raising the question whether it has an autonomous meaning or simply used as a synonym to privacy/private life.[320] Also, the Privacy Act mainly uses the expression right to private life: it only refers to the right to respect for private life in Article 8. Neither the Fundamental Law, nor the Civil Code employs the expression "right to private life".

In addition, these provisions relating to social media and the Internet raise several questions, especially the expressions "content shared and published for private purposes" and "personal data provided on the Internet for exclusively private purposes" ("magáncéllal megosztott és közzétett tartalmak" and "magáncélból közölt személyes adat"). What does the security of private sphere in relation to this shared or published content enshrined in the preamble mean? Is protection afforded to a personal Facebook post available to ten Facebook friends? Or to several hundreds of Facebook friends? Is it only applicable to chat messages within these sites?

The use of the expression "publish" suggests the sharing of a content with a larger audience, going beyond the scope of personal communication. Is the right to private life guaranteed when the user publicly shares a personal content relating to his/her private life, without using any privacy settings? In relation to Subsection (3) of Article 8, similar questions can be asked regarding personal data provided on the Internet for exclusively private purposes. Moreover, the phrasing of Subsection (3) of Article 8 is confusing, as it seems to implicate terminology referring to the outdated dual concept of legal grounds of the former Hungarian data protection act based on the dichotomy between consent and authorisation of the law.[321] These questions are yet to be answered.

In conclusion of Section 1, despite the numerous attempts to define privacy, no universal definition could be created due to privacy's embeddedness in the societal, technological and individual circumstances. In addition, what is considered to be private and what is legally protected as private might differ: the scope of privacy and the scope of the right to respect for private life are not always in overlap. The right to privacy covers a broader range of matters, while the right to respect for private life – terminology usually applied in the European legal order – is traditionally centred on the narrower concept of secrecy. However, even in these legal orders the concept of public privacy, or privacy as autonomy or self-determination appeared (first of all, see the ECtHR jurisprudence in relation to Article 8 of the ECHR), providing broader protection.

In the French legal order especially the concept of personal life, specific to the employment context should be mentioned: personal life encompasses private life, as a hard core of protection; but it also includes some elements of (public) extra-professional life. In the Hungarian legal order, this broader apprehension of right to respect for private life also appeared in the Constitutional Court's practice, and in civil courts.

---

[320] In addition, Subsection (2) of Section 2 employs the expression "private sphere" ("magánszféra").

[321] Although the Privacy Act introduced changes in this regard. Balogh et al. 2012. p. 97.

Section 2: Right to data protection

The right to privacy and the right to data protection are often mentioned together,[322] and typically there is clearly a connection between these two rights.[323] However, formally they are regulated in separate documents, and when it comes to their substantial scope, there exist different theories describing the relations between these two rights, and the additional role fulfilled by the right to data protection.[324] What is clear is that besides privacy, data protection can also play an important role in protecting employees' private lives, in consequence, its analysis must be included.

The right to data protection is much more than just the protection of personal data. Despite what its appellation might suggest, the right to data protection does not aim to protect personal data, but *the individual* to whom personal data relates.[325] *Pál Könyves Tóth* emphasizes the connection between the right to data protection and human dignity, stating that it is an essential condition to human dignity that individuals be able to take decisions regarding the disclosure of personal data relating to them.[326] *Máté Dániel Szabó* points out that personal data is more and more valued, as the individual's personality can be increasingly expressed through personal data.[327] To the outside world, the individual is more and more often perceived through (mainly) his/her personal data – instead of as a physical person.[328] Because of such an enhanced role, if the processing (e.g. collection and use of such information) does not take place according to the established guarantees and rules, the individual might suffer serious consequences.[329]

The Section will first *(§1)* address what additional role data protection can fulfill in comparison to privacy, aiming to clarify the relations between these two rights. Then *(§2)*, it will present how exactly the individuals' rights must be respected, through examining the most important points of the relevant legislation.

§1. Introduction to the right to data protection

The first data protection regulation appeared a few decades after the right to respect for private life,[330] followed by several other instruments both at the international and the national level. Although they will be addressed in detail in part §2, even at this point it must be noted that today data protection is subject to detailed regulations. For its importance, focus will be put on EU regulations: though ever since 1995 the question of data protection has been

---

[322] See, for example, Article 1 of the DPD, and Convention 108.

[323] http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (Accessed: 28 February 2018)

[324] *Orla Lynskey* identified three models of understanding the relation between privacy and data protection: they can be understood as separate but complementary rights; data protection can be understood as a subset of privacy; or data protection can be perceived as a separate, independent right in service of different functions, but not limited to privacy. Source: Lynskey 2015. p. 90. and pp. 91–106.

[325] Majtényi 2002. pp. 57–58.

[326] Könyves Tóth 1990. p. 621.

[327] Szabó 2005. p. 47.

[328] Szabó 2005. p. 47.

[329] For example, as it will be addressed later, if the employer does not process personal data according to the pertinent regulations, it not only infringes the employees' or prospective employees' rights but can also have serious consequences for his/her employment – e.g. termination of employment or unfavorable hiring decision.

[330] It was adopted in 1970 in Germany. Source: Simitis 2010. p. 1995.

regulated in the DPD, in 2016 the adoption of the GDPR brought considerable changes and became a central piece of legislation.

In the following part, first, *(A)* it will be explored what the reasons for the emergence of data protection rules were. Then, *(B)* it will be examined why there was a need when the right to respect for privacy had already existed. To put it differently, it will be explored in what regards there are substantial differences (if there are) between the two rights, which would justify the existence of two rights.

(A) The birth of the right to data protection

The right to data protection is a relatively recent right: it appeared in the 1970s. Similarly to the right to privacy, the right to data protection also emerged as a reaction to technological development: owing to the appearance of computers, the collection, storage, transfer, etc. had never been easier, and the plan for establishing different state registers was evoked by the states. Under the shadow of how state registers had contributed to the horrible events of the Second World War,[331] combined with the growing fear of a surveillance state, the public feared the consequences of unregulated automated processing of personal data. Still, prior to the 1960s and 1970s, technology did not make it possible to conduct automatic data processing; also, mass surveillance came at high costs, and thus the protection of the individual was naturally ensured.[332] However, due to the technological development, the situation had changed, and as a response to the arising threats, data protection appeared,[333] as these innovations offered unprecedented opportunities for the state to keep records in order to fulfil its functions (e.g. in relation to taxation, etc.).[334] At the same time, plans appeared throughout Europe aiming to unify or to connect national databases.[335] It was against this background that the first documents regulating data protection appeared. The world's first data protection act was adopted in 1970, in the German federal state of Hesse,[336] and was soon followed by other countries (Sweden in 1973, Germany in 1977, France in 1978).[337] After adopting these national data protection acts, it became also necessary to regulate the transborder flow of personal data, which led to the adoption of international data protection norms.[338]

France adopted its data protection act, the "Loi informatique" in 1978 [Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties ("loi relative à l'informatique, aux fichiers et aux libertés") hereinafter referred to as: FDPA – standing for French Data Protection Act], as a result of the SAFARI scandal concerning a project to interconnect certain files of the French administration – revealed to the public in an article in the newspaper *Le Monde*.[339] In 1978 the FDPA also established the French national data protection authority, named French National Commission on Informatics and Freedoms ("Commission nationale de l'informatique et des libertés") (hereinafter referred to as:

---

331 Galántai 2003.
332 Jóri 2005. p. 22.
333 Szőke 2015. p. 27.
334 Sári – Somody 2008. p. 133.
335 Szőke 2015. p. 31.
336 Simitis 2010. p. 1995.
337 On the history of data protection see more in: Szőke 2015. pp. 27–34.; Jóri 2005. pp. 21–66.
338 Jóri 2005. p. 28.
339 Boucher 1974. p. 9.

CNIL). The FDPA was significantly amended in 2004[340] in order to transpose the EU's data protection directive, and in 2016 by the Act for a Digital Republic aiming to address the new challenges of the information society.[341] Although the *GDPR* is directly applicable, it did not repeal national data protection acts: in the case of conflicting provisions, the former will be applied.[342] The amendment of the FDPA was realized in June 2018 by Act No. 2018-493 of 20 June 2018 on the Protection of Personal Data ("Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles").

While France was amongst the first countries in the world to adopt a data protection act in 1978, in *Hungary* this process was slower: Hungary adopted its first data protection act, Act LXIII of 1992 on the protection of personal data and access to data of public interest in 1992. The act also established the institution of the Hungarian data protection commissioner,[343] who was first appointed in 1995. This act was amended in 2003[344] due to Hungary's accession to the EU and replaced in 2011 by Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information (hereinafter referred to as: HDPA – standing for the Hungarian Data Protection Act). The HDPA also introduced significant changes to the national data protection authority: it replaced the institution of the data protection commissioner by establishing the Hungarian National Authority for Data Protection and Freedom of Information ("Nemzeti Adatvédelmi és Információszabadság Hatóság ", hereinafter referred to as: NAIH). After the entering into application of the GDPR, the Hungarian legislators adopted Act XXXIV of 2019 on legislative amendments required for the implementation of the European Union's data protection reform (hereinafter referred to as: Enforcing Act) in April 2019, aiming to adapt the Hungarian legal system to the GDPR, by amending more than 80 acts.

Despite the recent birth of the right to data protection, scholars already distinguish between different *generations of data protection regulations*. However, these generations are not universal, different authors established different stages in the history of data protection regulations. According to *Michael D. Birnhack*, the *first* stage was the very appearance of these regulations, the *second* was the appearance of international regimes instead of solely national regulation and the *third* was the emphasis being put on the transfer of personal data instead of the collection.[345] In 2005, law professor *Yves Poullet* differentiated between three generations of data protection regulations, starting with Article 8 of the ECHR, continuing with the EU's Data Protection Directive and the CoE's Convention 108, and ending with the EU's E-privacy Directive.[346] Back in 1997, *Viktor Mayer-Schönberger* already distinguished four generations of data protection regulations. The first one dates back to the very appearance of data protection laws, when these acts aimed to regulate

---

[340] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[341] See more on the Act for a Digital Republic in: Masnier-Boché, Lorraine: Loi « pour une République numérique » : état des lieux en matière de protection des données personnelles. *Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique*, 131, 2016. pp. 50–55.; Richard 2016.

[342] Bourgeois 2017. p. 13.

[343] Section 23 of Act LXIII of 1992

[344] By the Act XLVIII of 2003 on the amendment of Act LXIII of 1992 on the protection of personal data and access to data of public interest. Source: Könyves Tóth 2010. p. 55.

[345] Birnhack 2008. pp. 511–512.

[346] Poullet 2005. pp. 4–8.

the technology, when processing was conducted only by a few controllers. Then, when processing became differentiated and available not only for states but for businesses too, data protection regulations shifted from regulating technology to guaranteeing individual liberty. The third generation is characterized by the right to informational self-determination, while the fourth (e.g. the EU Data Protection Directive) manifests an intention to strengthen the rights of the individual and to create a mandatory protection of certain data, and a shift and an opening towards sectoral regulation.[347]

Gergely László Szőke differentiates between three generations: *the first generation* is characterized by the aim of regulating the automated processing of certain data controllers (mainly the state) who processed a huge amount of personal data. With the appearance and spread of the personal computer in the 1980s, this landscape changed, as the processing of personal data became available to a wider audience (to businesses or to private individuals): a *second* type of regulation was needed. These regulations are characterized by the aim of providing the individual the right to informational self-determination in general, instead of regulating the processing of only a few data controllers. The European Data Protection Directive, the OECD Guidelines, the CoE's Convention 108 are typical examples of the second generation of data protection regulations. However, since then, technology has not stopped evolving: the mass adoption of the Internet, social network sites, profiling, the use of mobile devices, etc. have evoked the necessity for a *third generation* of regulation. According to Szőke, the EU's General Data Protection Regulation (then proposal) represents new tendencies in personal data protection, by taking into account the obligations of data controllers (instead of the individual's right to self-determination), differentiating between certain types of controllers, aiming to regulate technology and strengthening the role of the internal regulations of controllers.[348] Either categorization we agree with, it is undisputed that the changes posed by the mass adoption of the Internet, social media, mobile devices and the shift in users' behaviour represent a challenge both for the right to privacy and for the right to data protection.

From the generations identified above, it can be observed that data protection went through different phases: since its appearance in the second half of the 20th century, the technological, societal and legal environment has been completely transformed. The conclusion that can be drawn from these generations is that data protection as well should be adequately adjusted to the given circumstances. While data protection at the beginning was regulated at the national level, it was soon recognized that the absence of an international legal framework would inhibit the international transfer of personal data[349] –, resulting in the adoption and existence of a complex regulation. While at the beginning data protection regulations had to cope with a limited number of huge databases, nowadays data processings have multiplied due to the rapid advancement of technological development. These changes had an effect on the regulations as well, as at the beginning these regulations constituted

---

[347] Mayer-Schönberger 1997. pp. 221–233.

[348] Szőke 2013. pp. 108–111. In his article Szőke also refers to the different existing theories amongst Hungarian scholars. According to *László Majtényi*, the first generation consists of norms regulating data processing by computers, while the second generation is technology-neutral, and the third focuses on challenges arising in different sectors. (Majtényi 2008. pp. 582–583.) According to *András Jóri*, the first generation of norms focuses on big data controllers and processing by computers, the second generation is centred around the right to informational self-determination, while the third one is concentrated on the new arising challenges. (Jóri 2005. pp. 23–66.)

[349] Jóri 2005. p. 28.

mainly technical regulations, but later shifted towards guaranteeing the freedom of the individual.[350] Existing rules are constantly challenged – for example by social media and SNSs, as it will be examined under Title 2.

(B) Defining data protection: substantial delimitation from the right to privacy

As a starting point, data protection can be comprehended as "*the regulation and organisation of the conditions under which personal data can be lawfully processed*."[351] However, it must also be established what is data protection and what is its relation to privacy? There is an uncontested connection between these two rights,[352] however, just like regarding the exact meaning of privacy, there is no uniform standpoint in this question, as there is still no universal consensus with respect to the relationship between these two rights.[353]

Different interpretations suggest that *data protection is a subset of privacy* and not a separate right.[354] On the one hand, different grammatical formulations support this view: data protection can be associated with privacy, as *Patrik Hiselius*' formulation suggests: "*[i]n the European Union, instead of using the term 'Privacy', in general the notion 'right to data protection' is used.*"[355] In the literature, the expressions informational privacy[356] or data privacy[357] are also used to describe data protection.

On the other hand, *Juliane Kokott* and *Christoph Sobotta* also point out that both the ECtHR and the CJEU consider data protection as an expression of the right to privacy.[358] Even in the EU, where the CFREU contains two separate articles for these two rights (Article 7 and Article 8), it is not excluded that data protection still forms a part of privacy.[359] In the jurisprudence of the CJEU, though in certain decisions it acknowledged that the right to privacy and the right to data protection are two separate rights,[360] the two rights are consistently conflated in most of its practice.[361] In contrast to the CFREU, the ECHR does not

---

[350] *Marta Otto* referring to *Mark Freedland* in: Otto 2016. pp. 106–107.

[351] Gellert – Gutwirth 2013. p. 525.

[352] According to *László Sólyom*, it is undisputed that the right to data protection originates from the right to privacy, although it has to be seen that both rights have grown beyond the concept of mere secrecy or intimacy. Source: Sólyom 1988. p. 55.

[353] Purtova 2010. p. 181.

[354] For example, *Endre Ferenczy* argues that data protection is one component of privacy. Ferenczy 2010. p. 48.

[355] Hiselius 2010. p. 203.

[356] See, for example: Mayer-Schönberger 1997. p. 226.

[357] *Lee A. Bygrave* argues that instead of the use of the expression "data protection", the expression of "data privacy" is better suited as it can constitute a bridge between the US and the European concept of privacy and data protection, and it better reflects the values to be protected. Bygrave 2004. pp. 321–322.

[358] Kokott – Sobotta 2013. p. 222.

[359] Purtova 2010. p. 185.

[360] In the Bavarian Lager case, the CJEU referred to the existence of a specific system of protection in relation to personal data protection [CJEU: Case C-28/08 P, 2010. par. 60.]. In its opinion in the Volker case, it was stated that "*[t]wo separate rights are evoked here: a classic right (protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No 108)*" acknowledging the existence of a separate right to data protection. (par. 71.) However, in the Volker judgement the CJEU employed the confusing expression of "*the right to respect for private life with regard to the processing of personal data*" (par. 52.) Source: CJEU: *Joined cases C-92/09 and C-93/09*, 2010

[361] For example, in the Rundfunk case he CJEU interpreted the DPD in the light of Article 8 of the ECHR. (CJEU: *Joined Cases C-465/00, C-138/01 and C-139/01*, 2003. par. 21.) In the case of Promusicae the CJEU

contain a separate provision corresponding to the right to data protection, still, the ECtHR deducted certain data protection rules from Article 8,[362] treating data protection as a privacy interest.[363] *Lee A. Bygrave* refers to the existence of an "almost universal consensus" that data protection mostly aims to protect privacy.[364] Indeed, privacy occupies a central role in data protection, as supported by numerous legal documents and by scholars as well. According to these views, data protection aims to ensure privacy.[365]

In contrast to interpreting data protection as a subset of privacy, different authors understand data protection as having a wider *scope* than privacy.[366] For example, *Orla Lynskey* argues that the right to data protection – though overlapping with the right to privacy – offers an additional protection for individuals.[367] Several other authors draw attention to the fact that despite the connection between privacy and data protection, data protection cannot be limited to the protection of privacy, but aims to ensure the protection of other rights, being broader than privacy.[368] *Bygrave* also expresses that while data protection aims to benefit society as a whole, privacy has a narrower aim, and concentrates on the

employed the term "*the right that guarantees protection of personal data and hence of private life*" to refer to one fundamental right, treating privacy and data protection as one right. (CJEU: *Case C-275/06*, 2008. par. 63.) See more on the conflating position of the CJEU in: Lynskey 2014. pp. 569–597.

362 Though Kokott and Sobotta argue that the ECtHR gave rise to a right to data protection, *Paul De Hert* and *Serge Gutwirth* are more cautious when it comes to this subject. They argue that though the ECtHR indeed went further than the narrow concept of privacy as intimacy and acknowledged several data protection aspects under Article 8 case law, basic data protection assumptions are not incorporated in its protection. Kokott –Sobotta 2013. p. 223. and De Hert – Gutwirth 2009. p. 24. and p. 27.

363 Purtova 2010. p. 198.

364 http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (Accessed: 28 February 2018), par. 2.

365 For example, according to *András Jóri*, data protection is "*a unique legal way to protect the private sphere of the individual*" and "*can be interpreted within the protection of private sphere, as the legal instrument protecting privacy in the current societal and technological environment*." Jóri – Soós 2016. p. 15 and p. 20. *Nadezhda Purtova* also interpreted existing doctrine as suggesting that the right to data protection and the right to privacy – though not completely synonymous – can be reduced to the same core, which is the protection of the private sphere of the individual. Purtova 2010. pp. 182–183.
According to Article 1 of the DPD, its objective was to "*[…] protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*." The CoE's Convention 108 also contained a similar paragraph. However, the WP29 expresses the contrary by stating that this formulation suggests that the purpose of the right to data protection is wider than the mere protection of privacy. WP29: *Opinion 4/2007*. p. 7.
A "separation" of data protection from privacy might also be observed in the GDPR, as, with the data protection reform, the world privacy is gone from the GDPR: Article 1 aims to protect "*[…] fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*." Also, a change in the terminology can be observed, adopting the concepts data protection by design and data protection impact assessment, replacing the "traditional" expressions privacy by design and privacy impact assessment. Costa – Poullet 2012. p. 255.
According to Section 1 of the HDPA, the purpose of the act is to "*[…] define rules in relation to data processing in order to make data controllers respect the private lives of individuals[.]*"

366 However, as it was also pointed out, data protection has a narrower scope compared to privacy, regarding the protection of moral persons: while data protection is solely offered to natural persons, the ECtHR expanded protection to moral persons. Source: ECtHR: *Société Colas Est and others v. France*, application no. 37971/97, 2002. par. 40. and Kokott – Sobotta 2013. p. 225.

367 Lynskey 2014. p. 582.

368 http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (Accessed: 28 February 2018), par. 18.
Similarly, according to *Isabelle Falque-Pierrotin*, in the age of the Internet the right to privacy no longer covers all aspects of the right to data protection – which is conceived to be a right at the intersection of property rights, the right to freedom of expression and the right to privacy. Falque-Pierrotin 2012. p. 36.

individual.[369, 370] *András Jóri [et al*.] also noted that data protection can be wider as it covers personal data not necessarily falling under privacy.[371] Usually such statement is supported by the fact that data protection rules apply regardless of the private or public nature of personal data, while traditionally privacy enjoys limited protection outside the private sphere.[372] This question gains significant importance in the context of SNSs, as on SNSs users typically (publicly) share a vast amount of personal data, raising several questions in relation to whether they fall under the scope of privacy and/or data protection.

Instead of solely stating that the right to data protection is wider than the right to privacy, *Raphaël Gellert* and *Serge Gutwirth* found that it is wider and narrower at the same time. They argued that as regards the content of these two rights, there are overlaps, still data protection is wider and narrower than privacy and vice versa.[373] Data protection is wider, as the data protection regulation applies to all kinds of personal data processing, even when the right to privacy is not infringed by the processing.[374] It is also more specific because it only deals with personal data, while the right to privacy covers more aspects. Privacy is also wider and more specific, as it could apply to cases concerning the processing of *not* personal data,[375] but which nevertheless can have an effect on one's privacy; but it will not apply to a processing which does not infringe privacy.[376]

While privacy remains a relatively vague concept, with a highly context-dependent nature, data protection is characterized by a more exact terminology. It is enough to look at basically any international or national piece of legislation: these documents usually contain the most important definitions, such as data protection, data processing, etc. having a more exact nature, leaving less place for interpretational questions. Naturally, it does not mean that data protection would not have to adapt to technological and societal changes[377] (see, for example, the EU data protection reform), or that no interpretational questions would arise (see, for example, the pre-GDPR discourse on IP addresses).

Raphaël Gellert and *Serge Gutwirth* also argued that privacy protects not only privacy but other fundamental rights as well. Gellert – Gutwirth 2013. p. 530. Data protection regulation can cover other significant values besides privacy, such as requirement of fair processing, consent, legitimacy and non-discrimination. Source: De Hert – Gutwirth 2009. p. 9.

369 http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (Accessed: 28 February 2018), par. 20.

370 In contrast to such an opinion *Anoinette Rouvroy* and *Yves Poullet* refer to other scholars who suggested that privacy aims to protect the society as a whole. Rouvroy – Poullet 2009. p. 60.

371 Jóri – Hegedűs – Kerekes 2010. p. 34. In contrast, *Attila Péterfalvi* argued in an interview that the right to data protection is narrower than the right to privacy. Source: Szabó 2004. p. 40.

372 Lynskey 2014. p. 583.; Gellert – Gutwirth 2013. p. 526.; Kokott – Sobotta 2013. p. 225.

373 Gellert – Gutwirth 2013. p. 526.
De Hert and Gutwirth also argued that data protection is both wider and more specific than the protection of privacy. De Hert – Gutwirth 2009. p. 6.

374 "*[…] storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 […]*" (ECtHR: *Amann v. Switzerland*, application no. 27798/95, 2000. par. 65.) However, when the processing does not concern the private life of the individual – for example, in the case of public camera surveillance, more precisely in the case of the use of "photographic equipment which does not record the visual data" – the Commission held that there was no interference with the applicant's private life. Commission of the ECtHR: *Pierre Herbecq and the Association Ligue des droit de l'homme v. Belgium*, Applications N° 32200/96 and 32201/96 (joined), 1998

375 It is enough to think of physical privacy, or of the protection of home or family life. See, for example, Kuner 2009. p. 309.

376 Gellert – Gutwirth 2013. p. 526.

377 De Hert – Gutwirth 2009. p. 4.

Another important difference is that while privacy aims to protect against intrusions (thus prohibiting intrusion), data protection regulations usually do not prohibit data processing but rather regulate how this processing can take place.[378, 379] While the right to privacy is a "redress" right, which ensures the protection from interference by public powers, the right to data protection is a "control" right, which aims to give the right to control the processing of personal data relating to the individual.[380] Another approach is to interpret the right to privacy as an opacity tool, ensuring the individual's "invisibility" towards the state; while the right to data protection as a transparency tool, regulating the processing of personal data in order to achieve transparency.[381, 382] Instead of providing protection against data processing, the right to data protection protects individuals from *unlawful* processing and regulates under which conditions personal data can be processed.[383]

In the light of the above, for the purposes of the monograph, data protection will be considered as the set of rules governing the processing of personal data relating to the employee. Indeed, privacy is at the core values of data protection, as there are often overlaps between the two rights. However, the two rights have different sets of tools to ensure the protection of employees' rights, therefore they cannot be treated as synonyms. While data protection channels the processing of personal data, privacy aims to ensure the employee to be able to decide about himself/herself. This can be interpreted as privacy enabling the employee to decide whether and how to use SNSs,[384] as data protection aiming to regulate whether employers can process personal data obtained from SNSs and if they can, they perform it according to the guarantees laid down in pertinent regulations.

§2. Legal regulation of the right to data protection

Besides the substantial differences, the right to data protection also became a formally separate right, laid down in several international and national documents. Due to their utmost importance, amongst the international instruments the EU's data protection framework will be focused on here, while other global and regional regulations will be addressed incidentally. Special attention will be paid to the GDPR, as it introduced considerable changes to EU data protection law. Its significance is mainly due to the form of the instrument chosen by the EU legislator: by regulating data protection in a regulation, EU law was unified in this field.

Although – as it will be demonstrated – data protection is already subjected to detailed regulation, it does not mean that this right lacks paths to evolve. The development of ICTs constantly challenges existing conceptions of data protection, giving rise to new questions or aspects to consider – for example, through the appearance of the right to informational

---

[378] De Hert – Gutwirth 2009. p. 3.

[379] In contrast to this view, *Gloria González Fuster* and *Serge Gutwirth* point out that data protection can be interpreted as being of prohibitive nature. Source: González Fuster – Gutwirth 2013

[380] Knight – Saxby 2014. p. 626.

[381] González Fuster – Gutwirth 2013. p. 536. and De Hert – Gutwirth 2009. p. x.

[382] In contrast to this view, *Marta Otto* emphasizes the deficiency of this opacity-transparency approach, as according to her it does not take into consideration the established case law of the ECtHR interpreting privacy beyond a negative right. Source: Otto 2016. p. 112.

[383] De Hert – Gutwirth 2009. pp. 3–4.

[384] Or reconnecting to the "traditional" concept of secrecy, it can be formulated as aiming to guarantee protection against the intrusions into the *autonomy* of private life.

self-determination. In some countries this right has been present for decades,[385] in others it constitutes a new issue[386] – but its existence and scope must be (re)examined in the light of technological and societal developments.

(A) Formal distinction from the right to privacy: norms regulating the right to data protection

Although no binding regime of data protection exists at the global level, the *United Nations' Guidelines for the Regulation of Computerized Personal Data Files* (hereinafter referred to as: UN Guidelines) should be mentioned.[387] The UN Guidelines contain recommendations to nations and also to governmental international organizations on what requirements and principles they should respect during the processing of personal data. The other document that must be mentioned is the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (hereinafter referred to as: OECD Guidelines). These guidelines were revised in 2013. Despite the lack of binding effect, the OECD Guidelines have particular importance as the principles[388] laid down in them are reflected worldwide in different privacy and data protection regulations.[389]

At the regional level the *CoE's* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[390] (hereinafter referred to as: Convention 108) was the first binding international document regulating the processing of personal data,[391] serving as the foundation for several European countries' data protection regulation.[392] Throughout the years, the adoption of Convention 108 was followed by a series of sectoral recommendations and resolutions in various fields, [393] such as in the field of employment, and the Convention itself was modernized in 2018.[394]

Even though the ECHR does not contain any article expressively stating the right to the protection of personal data, the ECtHR has found a way to ensure the protection of personal data, more precisely certain data protection principles (e.g. access to personal files, deletion and correction of personal data, purpose limitation principle) under its case law relating to Article 8.[395]

---

[385] See, for example, the German population census judgement from 1983.

[386] For example in France, where the Act for a Digital Republic introduced this right in 2016.

[387] United Nations: *Guidelines for the Regulation of Computerized Personal Data Files*. Adopted by General Assembly resolution 45/95 of 14 December 1990

[388] These principles are the following (OECD Guidelines, 1980, par. 7–14.): collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle, accountability principle. See more on these principles at: Majtényi 2008. p. 586.

[389] Hendrickx 2000. p. 254.

[390] Council of Europe: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981

[391] Which document was highly inspired by the French national data protection act. Source: Bioy 2016. p. 524.

[392] CoE 2018. par. 1.

[393] See these documents at: https://www.coe.int/en/web/data-protection/legal-instruments(Accessed: 7 March 2018)

[394] CoE: *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. CM/Inf(2018)15-final, Elsinore, Denmark, 2018

[395] Gellert – Gutwirth 2013. p. 526.

Besides the European regulation, other regional regimes exist too, such as the Asia-Pacific Economic Cooperation's (hereinafter referred to as: APEC) *Privacy Framework* of 2005 (revised in 2015) the Economic Community of West African States' (hereinafter referred to as: ECOWAS) *Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS* or the Organisation of American States' *General Assembly Resolution 2661 on Access to Public Information and Protection of Personal Data*.[396]

Although the GDPR leaves a certain margin of maneuver to the *Member States*, for example in the field of employment,[397] it unified data protection in the EU. As neither the HDPA nor the FDPA contains employment specific provisions, their detailed general analysis will not be discussed.[398] In accordance with Article 88 of the GDPR – which legitimizes Member States to adopt specific provisions in the field of employment – both France and Hungary enacted employment specific data protection provisions, laid down not in the data protection acts but in the labour codes. Therefore, national specificities of the data protection acts will not be addressed, instead, emphasis will be put on the general provisions of the GDPR in part (b), while the employment specific privacy and data protection provisions in France and in Hungary will be addressed in Chapter 2.

(a) EU framework of data protection

The *European Union* also has its own data protection regime. The right to data protection is recognized at the EU constitutional level. Even though the right to data protection had existed before the adoption of the CFREU, the CFREU went further and – contrary to the ECHR – regulated the right to data protection as a fundamental right, separate from the right to respect for private life.[399, 400] The *Treaty of Lisbon* (2007/2009) has a great significance as it provided the CFREU legally binding force and also incorporated the right to data protection into Article 16 of the Treaty on the Functioning of the European Union.[401]

In 1995 the EU adopted *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, which was described as "*the most comprehensive and successful international instrument of data protection laws*"[402]

---

396 Mendel et al. 2013. p. 73.

397 Article 88 of the GDPR

398 For more information on the French data protection legislation see more in: Desgens-Pasanau, Guillaume: *La protection des données à caractère personnel: la loi 'Informatique et libertés'*. LexisNexis, Paris, 2012; Féral-Schuhl 2010. pp. 31–109.; Grynbaum – Le Goffic – Morlet-Haïdara 2014. pp. 747–784., pp. 803–851.; Bourgeois 2017. pp. 5–274.
On *Hungarian* data protection see more in: Jóri – Soós 2016; Péterfalvi 2012. On the 1992 data protection act see more in: Jóri – Hegedűs – Kerekes 2010; Jóri 2005; Majtényi 2006

399 De Hert – Gutwirth 2009. pp. 7–8.

400 CFREU: Article 8, Protection of personal data:
"*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."

401 González Fuster – Gutwirth 2013. p. 531.

402 *Michael D. Birnhack* referring to Bennett, Colin J. – Raab, Charles D.: *The governance of privacy: policy instruments in global perspective*. MIT Press, Cambridge, 2006 and Swire, Peter P. – Litan, Robert E.: *None of your business: world data flows, electronic commerce and the European privacy directive*. Brookings Institution Press, Washington DC, 1998. Cited in: Birnhack 2008. p. 512.

and which was highly inspired by Convention 108.[403] The DPD adopted a technology-neutral approach. The CJEU also dealt with data protection in several of its cases.[404]

For more than 20 years the DPD was the central document of data protection in the EU. In 2016 – although the process started back in 2009[405] – an important event happened in the history of data protection: in the frame of the EU's data protection reform, the DPD was replaced by the GDPR. Almost two decades after the adoption of the DPD, the revision of the EU data protection framework became necessary, as the developments in technology and globalization made the processing of personal data become more elaborated and less detectable.[406] Also, the DPD did not result in the desired harmonisation effect.[407] A reform was needed in order that the EU could ensure the effective protection of personal data in the 21st century, too.[408] This reform was composed of two documents: the GDPR was one of them.[409] It is important to state that the core principles and values laid down in the DPD remain valid, and the GDPR kept the technology-neutral approach of the regulation.[410] The relevant provisions of the GDPR will be further detailed in part b.

Besides the general requirement set by the GDPR, sectoral rules must also be mentioned, as they react to the specific data protection questions raised in certain fields. The EU has also adopted *sectoral data protection norms* in the fields of the electronic communications sector,[411] data processing by the Community Institutions and Bodies,[412] data processing and criminal matters,[413] data retention[414] and on the transfer of personal data.[415]

---

403 Wong 2012. p. 229.

404 See more on the CJEU's jurisprudence in the field of data protection in: Wong 2012. pp. 229–244.; European Union Agency for Fundamental Rights – Council of Europe 2018

405 De Hert – Papakonstantinou 2012. p. 131.

406 European Commission 2010. p. 2.

407 De Hert – Papakonstantinou 2012. p. 131.

408 de Terwangne – Rosier – Losdyck 2016. p. 6.

409 The other document was *Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. OJ L 119, 4.5.2016, p. 89–131

410 European Commission 2010. p. 3.

411 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*. OJ L 201, 31.7.2002, p. 37–47

412 *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*

413 *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. OJ L 350, 30.12.2008, p. 60–71. replaced by *Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. OJ L 119, 4.5.2016, p. 89–131.

414 *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*. OJ L 105, 13.4.2006, p. 54–63

415 *2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and*

Also, the *Article 29 Data Protection Working Party* (hereinafter referred to as: WP29) should be mentioned. The WP29 was an independent advisory board set up by Article 29 of the DPD, which addressed various sectoral questions of data protection – e.g. employee monitoring – in several of its documents. However, as a result of the data protection reform, the WP29 was replaced by the European Data Protection Board (hereinafter referred to as: EDPB), an independent body of the EU.[416] In these documents the WP29 basically translated the general provisions set in the DPD to the special context of employment. Even though they did not have legally binding force, – partly due to the WP29's composition – they provide useful guidance for the Member States, and national data protection authorities take into consideration these opinions when it comes to the enforcement of national data protection rules.[417]

(b) General Data Protection Regulation – rules of data processing

The following paragraphs will address the most important rules set by the GDPR regarding data processing, focusing on the provisions which have higher relevancy in the context of employee monitoring and the protection of employees' right to privacy and right to data protection[418] and on the challenges raised by SNSs in relation to employment. Adequate knowledge of these provisions is necessary in order to be able to address the specific challenges raised by SNSs in the employment context.[419]

The GDPR kept the technology-neutral nature and the core values[420] of the DPD and applies to all kinds of processing, regardless of the technology used.[421] One of the most striking differences between the instruments is that the EU legislators choose to regulate data protection by a regulation instead of the previous directive, unifying data protection law throughout Europe.

Although having a regulation instead of a directive indeed leads to more uniformity, it does not mean that no differences will exist between Member State regulations, as in certain

---

related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) OJ L 215, 25.8.2000, p. 7–47 replaced by *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176*. OJ L 207, 1.8.2016, p. 1–112

416 Recital (139) of the GDPR

417 Otto 2016. p. 97. and Retzer – Lopatowska 2011. p. 2.

418 On the detailed and exhaustive analysis of the GDPR see: Jay, Rosemary et al.: *Guide to the General Data Protection Regulation: a companion to data protection law and practice.* 4th edition. Sweet & Maxwell, London, 2017; Rücker – Kugler 2018; Bensoussan, Alain. (ed.): *Règlement européen sur la protection des données: textes, commentaires et orientations pratiques*. Bruylant, Bruxelles, 2018; Beaugrand, Thomas et al.: *Protection des données personnelles : se mettre en conformité d'ici le 25 mai 2018*. Editions législatives, Montrouge, 2017; Prévost, Stéphane – Royer, Erwan (eds): *Le RGPD*. Dalloz, Paris, 2018. Jóri et al. 2018; Péterfalvi – Révész – Buzás 2018; Bölcskei 2019.; De Terwangne – Rosier – Losdyck 2016.

419 Throughout this part references will be made to the text of the GDPR and also to the different documents issued by the WP29 to clarify how these general provisions should be interpreted in the employment context. Though the WP29 existed under the auspices of the DPD, and not the GDPR, the inclusion of its documents is justified by the following: as it was already noted, despite the reform, the core values and principles of data protection remain valid, therefore the statements of the WP29 can keep providing guidance adequately and with caution.

420 European Commission 2010. p. 3.

421 Recital (15) of the GDPR

questions the GDPR empowers Member States to adopt specific rules. Particularly, Article 88 of the GDPR contains *special provisions* regarding processing in the employment context, stating that Member States can provide for more specific rules in order to ensure employees' right to data protection.[422] Such rules should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to, amongst others, monitoring systems at the workplace.[423] This means – as there is no unified "EU labour law" – that some differences between Member State regulations might still exist in the future in the field of employment monitoring, giving rise to certain national specificities.

On SNSs users (employees) share a myriad of personal data. According to Paragraph 1 of Article 4 of the GDPR, *personal data* "*means any information relating to an identified or identifiable natural person ('data subject') […]*". The EU purposefully adopted such a wide definition,[424] and the GDPR provides more guidance by adding a list of examples: "*[…] in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]*" An employee's name, phone number, e-mail address, image, the metadata regarding their communication, IP address, online identifiers,[425] etc. all qualify as personal data.[426] The GDPR requires to fulfil stricter conditions[427] when it comes to the processing of "s*pecial categories of personal data*", such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, *per se* prohibiting their processing with certain exceptions (Article 9) and defines genetic data, biometric data and data concerning health. On SNSs, a user often shares information that is qualified as sensitive data. For example, through sharing relationship status and identifying with whom the employee is in relationship can reveal his/her sexual orientation. The liking of the pages of certain political parties or politicians, posts, or comments made under posts, confirming the attendance at certain political events can reveal one's political opinions. The same goes for religious and philosophical beliefs.

Data processing is defined as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available,*

---

422 Schultis 2017. p. 266. Article 88 of the GDPR: Processing in the context of employment: "*1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*"

423 WP29: *Opinion* 2/2017. p. 9.

424 WP29: *Opinion* 4/2007. p. 4.

425 Recital (30) of the GDPR

426 As concerns what is qualified as personal data see more in: WP29: *Opinion 4/2007*

427 As a main rule, Article 9 of the GDPR prohibits the processing of such data and then provides exception from this prohibition.

alignment or combination, restriction, erasure or destruction[.]" (Paragraph 2 of Article 4) It is also a wide definition, basically any operation made on personal data falls under the notion of processing (e.g. consulting a Facebook profile, making a screenshot of it, etc.). Even though nowadays most processings are conducted by automatic means (e.g. with the help of a computer or a mobile device),[428] the GDPR does not exclude manual processing, as these kinds of activities are also capable of posing a threat to the rights and interests of data subjects, protected by the GDPR.[429]

As concerns the parties participating in the processing: the *data controller*[430] is the actor (natural or legal person, public authority, agency or other body) who, alone or jointly with others, determines the purpose and means of the processing of personal data; or the *data processor*,[431] who processes personal data on behalf of the controller.[432] The GDPR introduces the notion of *joint controllers*: if two or more controllers jointly determine the purposes and means of processing, they will qualify as joint controllers. They should adopt an arrangement detailing their respective responsibilities in order to comply with their obligations regarding the data processing.[433] Depending on the circumstances of the processing, the employer can qualify either as controller/joint controller or processor. The employee/former employee/job candidate will qualify as the *data subject*:[434] the identified or identifiable natural person to whom the personal data relates.

Regarding the *material scope* of the GDPR: it applies to data processing conducted wholly or partly by automated means, and also to processing which is not conducted by automatic means but which forms or is intended to form part of a filing system.[435] The WP29 clearly stated that monitoring employees' e-mail or Internet use, video surveillance or the processing of sound data clearly falls under the scope of the regulation and also stated that usually most manual records are also likely to fall under the scope of the regulation.[436], [437] The WP29 also declared that the data protection requirements are to be applied to the case of processing *prospective employees'* personal data obtained from SNSs during the recruitment process.[438] By analogy, it should also apply to the processing of *employees'* personal data obtained from SNSs.

According to its *territorial scope*, the GDPR applies to processing when the controller or the processor has an establishment in the EU (Paragraph 1 of Article 3) or when the

---

428 European Union Agency for Fundamental Rights – Council of Europe 2018. p. 99.

429 Rücker – Kugler 2018. p. 11.

430 Paragraph 7 of Article 4 of the GDPR

431 Paragraph 9 of Article 4 of the GDPR

432 On the notion of controller and processor see more in: WP29: *Opinion 1/2010 on the concepts of 'controller' and 'processor'*. 00264/10/EN WP 169, 2010

433 Article 26 of the GDPR

434 Paragraph 1 of Article 4 of the GDPR

435 Paragraph 1 of Article 2 of the GDPR

436 WP29 *Opinion 8/2001*. p. 13.

437 Article 2 of the GDPR defines some exceptions from its scope, such as processing:
- relating to activities falling outside the scope of EU law,
- relating to the common foreign and security policy of the EU,
- by a natural person for purely personal or household activity,
- relating to criminal matters and public security,
- conducted by EU bodies and institutions.

However, these provisions do not affect the applicability of the GDPR to processing in the employment context.

438 WP29 *Opinion 2/2017*. p. 11.

controller or the processor does not have an establishment within the territory of the EU but the processing relates either to the offering of goods or services to data subjects in the EU, or to the monitoring of data subjects' behaviour within the EU. (Paragraph 2 of Article 3). Therefore, the GDPR applies if the employer is situated within the EU or the monitoring aims at employees' behaviour on SNS within the EU.

Principles of data processing are orienting principles.[439] They apply to every data processing activity and play a huge part in interpreting the provisions of the GDPR, thus helping the data controller to establish a lawful processing[440] and also courts to interpret the GDPR.[441] These principles govern the processing of personal data and aim to ensure the protection of the individual. They are not new, the core of them is the same as those defined by previous data protection instruments.[442] These principles are wide and general provisions, which have to be considered as a guideline and framework for the processing. Throughout the GDPR specific provisions complement these general principles.[443] Every data processing has to comply with the following principles (Article 5): lawfulness, purpose limitation, fairness, data minimization, accuracy, transparency, storage limitation,[444] integrity and confidentiality,[445] accountability.[446] Especially the principles of purpose limitation, accuracy, data minimization and transparency are considerably challenged by SNSs. These

---

[439] Péterfalvi – Révész – Buzás 2018. p. 95.

[440] Bölcskei 2019. p. 74.

[441] Voigt – von dem Bussche 2017. p. 84.

[442] de Terwangne – Rosier – Losdyck 2016. p. 18.

[443] Rücker – Kugler 2018. pp. 49–50.

[444] According to this principle, personal data shall be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*" (Item e) of Paragraph 1 of Article 5 of the GDPR) with certain exceptions. Recital (39) of the GDPR expressively states that the period of storing personal data is limited to a strict minimum. This principle can be understood as the temporal aspect of the necessity principle. Source: Rücker – Kugler 2018. p. 70.

[445] *Integrity and confidentiality*: personal data shall be processed "*in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*" [Item f) of Paragraph 1 of Article 5 of the GDPR] This provision aims to ensure the security of the personal data themselves, by obliging the employer to implement appropriate technical or organizational measures in order to ensure that the personal data processed are secure and safe from outside intrusion. (WP29: W*orking document on the surveillance of electronic communications in the workplace*, 2002. p. 18.) Further provisions on data security can be found in Articles 32–34 of the GDPR detailing the obligations of controllers and processors.

[446] *Accountability*: the employer, as data controller is responsible for compliance with these principles and also shall be able to demonstrate compliance. Article 24 further develops the responsibility of the controller by stating that depending on the circumstances of the processing, the controller shall adopt appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. The controller shall also review those measures. (Paragraph 1 of Article 24) Compliance might be demonstrated through the adherence to approved code of conducts or approved certification mechanisms. (Paragraph 3 of Article 24) The controller can demonstrate compliance – amongst others – through the adoption of internal policies, implementing the principles of data protection by design and by default, appointing a data protection officer implementing data minimisation and transparency or using pseudonymisation. [Recital (78) of the GDPR] The stakes are high: data subjects have the right to an effective judicial remedy against a controller or processor and can lodge a complaint with a supervisory authority if they consider that controllers or processors infringe or are in non-compliance with the regulation. (Article 79 of the GDPR) In the most severe cases, administrative fines up to 20 million euros, (or up to 4 % of the total worldwide annual turnover of the preceding financial year in the case of an undertaking) can be imposed. (Paragraph 5 of Article 83 of the GDPR)

specific challenges will be dealt with in Part II., here, the following paragraphs will focus on their general presentation.

Lawfulness means that the data processing must have one of the six legal grounds defined in Article 6 of the GDPR, which are the following: consent; performance of a contract or when processing is necessary in order to take steps at the request of the data subject prior to entering into a contract; compliance with a legal obligation to which the controller is subject; vital interests of the data subject or of another natural person; performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; legitimate interests. In the employment context some of them (namely consent, performance of a contract, legitimate interests)[447] are more commonly applied than the others, therefore only these are going to be addressed in detail.

One of the possible legal grounds is *consent*. However, the WP29 expressed on several occasions that the applicability of consent as a legal ground of processing in the employment context is highly questionable. According to the GDPR, consent is a "*[…] freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her[.]*" (Paragraph 11 of Article 4) In Recital (43) the GDPR further states that consent shall not constitute a valid legal ground when its freely given nature is not ensured, such as in cases when there is a clear imbalance between the controller and the data subject. This provision is in harmony with the WP29's previously manifested opinion, according to which the reliance on consent should be limited, as there is a hierarchal relationship between the parties, questioning the genuinely free nature of consent.[448] If the employer asked the employees to consent to the installation of a monitoring or surveillance system (e.g. monitoring their use of SNSs or processing personal data obtained from SNSs), employees might not consent freely, as they fear the possible consequences of a refusal. Therefore, consent should not constitute the valid legal ground of employee monitoring.[449, 450]

SNSs raise questions, as the employer might take advantage of his/her position to obtain access to certain content posted by the employees. For example, in the US case *Pietrylo v. Hillstone Restaurant* the employer accessed a private chat room where employees had a discussion, by obtaining the login credentials of one of the employee, who gave them to the employer in the fear of getting in trouble in the case of not complying with the request.[451] The applicability of consent can be challenged as there are no clear social conventions about social media use,[452] which can have an effect on consent – for example, what should the employee do if the employer adds him/her as a "friend"? Can the employee ignore the friend request without consequences or is he/she "obliged" to accept it? However, *Emmanuel Plasschaert* points out that the formulation of Recital (155)[453] implicitly implies

---

[447] Kajtár – Mestre 2016. p. 33 Note: the authors' statement relates to pre-employment background checks.

[448] WP29: *Opinion 8/2001*. p. 23.; WP29: *Opinion 2/2017*. p. 23.

[449] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 21.

[450] This does not mean that consent as a valid legal ground is completely missing from the employment relationship. The WP29 provides an example of employees consenting to the upload of their photos into their intranet profiles. Source: WP29: *Opinion 15/2011*. p. 14.

[451] District of New Jersey: *Pietrylo v. Hillstone Restaurant Group*, No. 06-05754, 2009

[452] Van Eecke – Truyens 2010. p. 536.

[453] "*Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions*

that the EU legislator did not want to prohibit completely the use of consent as a legitimate ground in the employment context.[454] In my opinion, because of the hierarchal relationship between the parties, employee's consent should not constitute a legitimate legal ground for the processing of his/her personal data present on SNSs.

Another possible legal ground – especially during recruitment – is *performance of a contract* or when processing is necessary in order to take steps at the request of the data subject prior to entering into a contract: when without the processing of personal data the contract between the parties could not be executed, the processing of these data will be considered lawful. For example, one of the main obligations of the employer – to pay the employee – necessarily comes with the processing of his/her bank account number.[455] Or, in order to enter into contract with a prospective employee, the processing of certain personal data – such as name, date of birth, data relating to education and professional experience, etc. – is inevitable during the recruitment process. However, employee monitoring is likely to be considered as processing going beyond the performance of a contract,[456] necessitating the application of another legal ground. Also, prior to entering into contract, a detailed background check following a candidate's application should not be understood as necessary for entering into contract.[457]

Data processing is lawful when it is necessary for the purposes of the *legitimate interests* pursued by the employer, except when these interests are overridden by the data subjects' fundamental rights and freedoms.[458] This provision requires a balancing, an assessment of whether the controller's legitimate interests can override the data subject's reasonable expectations of privacy and data protection.[459] The WP29 pointed out that the legitimate interests of the employer can constitute a valid legal ground of employee monitoring.[460] The WP29 emphasizes that this legal ground should not be treated as a last resort, which applies automatically when no other legal ground can be evoked, but has to fulfil severe conditions and involve a careful balancing of the two opposite sides in order to be considered lawful.[461] The field of employee monitoring is considered to be a field where the balancing of legitimate interests can take place.[462] Besides the employer's legitimate interests, the employees' rights also have to be taken into consideration: what impact would the processing have on these rights (e.g. what kind of data will be processed and how, what is the relation between the controller and the data subject)?[463] Also, the implementation of additional safeguards is crucial when striking the balance.[464] This means that although the legitimate interest can constitute a valid legal ground for employee monitoring, it does not apply automatically:

---

under which personal data in the employment context may be processed on the basis of the consent of the employee […]."

454 Plasschaert 2017. pp. 113–114.

455 WP29: *Opinion 8/2001*. p. 15.

456 WP29: *Opinion 06/2014.* p. 17.

457 WP29: *Opinion 06/2014.* p. 18.

458 Item f) of Paragraph 1 of Article 6 of the GDPR

459 Recital (47) of the GDPR

460 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. pp. 16–17., WP29: *Opinion 2/2017*. pp. 7–8.

461 WP29: *Opinion 06/2014*. p. 9. The WP29 provides further guidance in this Opinion regarding how the balancing test should be implemented.

462 WP29: *06/2014*. pp. 24–25.; Péterfalvi – Révész – Buzás 2018. p. 133.

463 WP29: *Opinion 06/2014*. pp. 36–41.

464 WP29: *Opinion 06/2014*. pp. 42–48.

the balancing test must be implemented,[465] carefully assessing the two sides. In my opinion, this is the legal ground that in most cases can be applied to the cases of SNS monitoring.[466]

Purpose limitation is a principle bearing utmost importance[467] and requires that every data processing shall have a specified, explicit and legitimate purpose and shall not be further processed in a manner incompatible with the original purpose.[468] This means that – even when there is a valid legal ground justifying the processing – every processing shall have a specific purpose, the employer cannot process data "just in case" it is useful one day. This principle has huge importance, as determining the purpose is considered to be a precondition for the whole processing and application of the other principles. It also sets the boundaries of the processing.[469] In the employment context different purposes might have relevancy originating from the employer's legitimate interests and rights (such as assessing whether a job candidate is adequate for the position, monitoring employees' performance, monitoring the adequate use of the employer's equipment, safety or monitoring the compliance with a non-compete clause).[470] The purpose determines the whole processing activity: for example, if an employer started a processing for the purpose of ensuring safety, then this original purpose determines the rest of the processing: this data cannot be used to monitor, for example, employees' behaviour.[471]

In the case of SNS, the legitimate purpose might be, for example, to monitor whether employees truly spend working hours working (and not surfing on Facebook instead), whether they respect the possible restrictions imposed by the employer on the personal use of work computers, whether employees respect the employer's reputation (and do not post defamatory content on SNSs or bring shame to the employer in other ways), whether the job candidate is the best who could be employed, etc.

According to the WP29, in order for processing to be *fair*, personal data "*must be processed in a way that does not bring about unfairness to the data subject*."[472] This imposes an additional test on controllers. However, the definition of fairness is not given, leaving room for the interpretation of this principle.[473] It is closely connected to the principle of transparency – the Recitals of the GDPR[474] mention fairness together with the principle of transparency ("fair and transparent processing")[475] –, but they are not synonymous concepts. The principle of fairness goes beyond transparency and can be interpreted as the requirement to process personal data in an ethical way.[476, 477]

---

[465] Bölcskei 2019. pp. 62–63.

[466] However, as remarked by *Edit Kajtár* and *Bruno Mestre*, when it comes to pre-employment background checks, the application of the 'balancing test' is also dubious, as the employer's legitimate interest to find the best candidate possible can be achieved through less intrusive methods. Kajtár – Mestre 2016. p. 33.

[467] Péterfalvi – Révész – Buzás 2018. p. 96.

[468] WP29: *Opinion 8/2001*. p. 20.; Jóri et al. 2018. p. 195.

[469] Péterfalvi – Révész – Buzás 2018. p. 96.; WP29 (2013) *Opinion 03/2013 on purpose limitation*. 00569/13/EN WP 203. p. 4.

[470] WP29: *Opinion 8/2001*. pp. 6–7.

[471] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 14.

[472] WP29: *Opinion 8/2001*. p. 18.

[473] See more examples in: Bölcskei 2019. p. 80.

[474] Recitals (39), (60) and (71) of the GDPR

[475] Rücker – Kugler 2018. pp. 51–52.

[476] European Union Agency for Fundamental Rights – Council of Europe 2018. p. 119.

[477] An example is ensuring the presence of the employee when searching through his/her professional e-mail account. Source: NAIH/2019/51/11., p. 19.

According to *data minimisation*, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. It places further limitations regarding what personal data the employer can process: the processing of personal data has to be *necessary* in order to achieve the purpose:[478] the employer must consider whether the monitoring is truly needed, or the same result could be achieved through traditional forms of monitoring.[479] Any monitoring shall be proportionate and the least intrusive possible[480] compared to the purpose of the processing. For example, if the employer prohibits the use of social media at the workplace during working hours, then he/she should only monitor whether employees visit these sites, he/she must not monitor the content of these websites.[481] The WP29 emphasizes that when it comes to electronic monitoring, prevention should be more important than detection.[482] Instead of monitoring the access to these "prohibited" sites, blocking of access or the use of pop-up warning windows should be considered.[483] Monitoring should be tailored to the circumstances of the processing: continuous and automatic monitoring should be avoided.[484] It is advisable that in accord with the purpose, the risks, etc., limitation in scope, time or place are applied.

The principle of *accuracy* means that personal data shall be accurate and, where necessary, kept up-to-date. When personal data are inaccurate, every reasonable step, with regard to the purpose of the processing, shall be taken that these data are erased or rectified without delay.[485] The GDPR does not provide a definition of 'accurate': data are considered to be inaccurate if they do not correspond with reality and also if they are not complete or are embedded into the wrong context.[486]

Transparency requires that employees shall be aware of the characteristics of the processing (e.g. identity of the controller, what kind of personal data are processed, for what purpose, risks associated with the processing, what rights they have as data subjects and how they can exercise them), these pieces of information shall be easily accessible and easy to understand by using clear and pain language.[487] This means that employers need to be open and clear about data processing, as a main rule covert monitoring is not permitted.[488] Naturally, if employees are not aware of the processing/monitoring, they will not be able to exercise their rights,[489] therefore transparency of processing is a precondition for being able to exercise data subjects' rights. It relates also back to the population census judgement and to the core of the right to informational self-determination, as the German Federal Constitutional Court considered it crucial for the exercise of fundamental rights that the individual is aware of who processes, what data and why, etc.[490] It is not enough to state that the use of the Internet or social network sites will be monitored, further

---

478 Péterfalvi – Révész – Buzás 2018. p. 101.

479 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 13.

480 Jóri et al. 2018. p. 208.; WP29: *Opinion 8/2001*. p. 4, p. 21, p. 25.; WP29: *Opinion 2/2017*. p. 7.

481 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 24.

482 WP29: *Opinion 2/2017*. p. 23.

483 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 15, p. 18.

484 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 17.

485 Jóri et al. 2018. 215.

486 Rücker – Kugler 2018. p. 68.

487 Recital (39) of the GDPR

488 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 14.

489 WP29: *Opinion 2/2017*. p. 10.

490 Simitis 1995. pp. 447–448.

details regarding the processing shall be provided. The principle of transparency is further strengthened by Articles 12–14 regulating the controller's obligation to inform data subjects regarding the processing (the data subject's right to information)[491] and also by the data subject's right to access (Article 15).

The already existing *rights of the data subject* were reinforced and new ones were introduced in order to ensure effective protection of the individuals.[492] The employee has the *right to information* – which was already discussed in relation to the employer's obligation to inform employees regarding the processing. However, employees have the right to obtain information not only at the time of the collection of personal data, but also during the processing. Therefore, in the frame of the *right to access*, the employee has the right to know whether the employer processes his/her personal data, and if there is processing taking place, the employee can obtain further information regarding it (e.g. what the purpose is, what personal data are processed, etc.) and also has the right to obtain a copy of the processed personal data.[493] The *right to rectification* guarantees that at the demand of the employee, inaccurate personal data shall be rectified, incomplete personal data completed.[494]

The *right to be forgotten* is one of the novelties introduced by the GDPR, though not completely new as it already existed in the DPD.[495] It means "*the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes*."[496] This right has two aspects.[497] The first one is the "traditional" right to erasure, which means that "*[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay […]*" if other conditions are met. (Paragraph 1 of Article 17) It is completed by a second provision in order to strengthen the data subjects' rights in the online world: with the obligation of the data controller to take all the reasonable steps to inform other controllers processing those data that the data subject wants these controllers to erase the data, any links to it, any copies or replication if the controller has made the data – subject to the right to erasure – public. [Recital (66), Paragraph 2 of Article 17] Of course, the right to be forgotten is not an absolute right; there exist some interests that justify that the right to be forgotten does not prevail in some cases: e.g. freedom of expression, or historical, scientific research. (Paragraph 3 of Article 17)

The reason for the acceptance of the right to be forgotten is that, while the human mind has its limits in remembering, the Internet does not have any limits.[498] However, the concrete way of the implementation of this right is still a question, as right now the Internet is not

---

[491] Depending on the given country's regulation – that is the case, for example, in Hungary and in France, further requirements, such as the information of works council might be necessary in order to make the processing lawful.

[492] Bounedjoum 2016. p. 44.

[493] Article 15 of the GDPR

[494] Article 16 of the GDPR

[495] See more on this subject: Bunn, Anna: The curious case of the right to be forgotten. *Computer Law and Security Review*, 31(3), 2015. pp. 336–350.

[496] European Commission 2010. p. 8.

[497] European Digital Rights. p. 6.

[498] Kindt 2015.

capable of forgetting, as it is not possible to permanently remove content.[499] Still, this right is a great step in protecting personal data, however, it might be more accurate to interpret it as the right to not to be found, as complete erasure from the Internet is technically not possible.[500] Several users have possessed an SNS profile for years now: if these platforms are used actively, a considerable amount of personal data is accumulated – with a huge part of them being irrelevant to the purposes of the employment.[501]

The GDPR introduces *new ways* beyond the traditional legal protection, by regulating the technology itself, by making it more privacy-friendly. Three principles make this possible: data protection by design, data protection by default and data protection impact assessment.[502] *Data protection by design*[503] basically means – after the analogy of privacy by design – the use of built-in data protection-friendly solutions into the whole designing of the processing.[504] *Data protection by default*[505] means that controllers should ensure that personal data is processed with the highest privacy protection. *Data protection impact assessment* means the evaluation of the possible risks related to the protection of personal data, prior to the processing. In cases when data processing comes with higher risks for the rights of the individual, the controller should evaluate these risks in a data protection impact assessment, by taking into consideration the characteristics of the processing. [Recital (83), Article 35] Employee monitoring will likely fall under the notion of "high risk" processing, placing an obligation on employers to conduct a data protection impact assessment.[506, 507]

---

499 Bolton 2014. p. 133.

500 International Working Group on Data Protection in Telecommunications 2013. pp. 1–2.

501 The *right to data portability*, introduced by the GDPR, is another Internet specific right, it enables interoperability between different service providers. [Recital (68) of the GDPR] It consists of two parts: the first part is the right to obtain a copy of the personal data processed by the controller in a structured way, and the second one is the right to transmit this personal data to another service provider. Source: Costa – Poullet 2012. p. 257. According to the *right to restriction of processing*, the data subject has the right to obtain the restriction of processing from the controller when certain conditions are met. (Article 18 of the GDPR) Employees have *the right to object* when the processing is based on the legitimate interest ground (or on the performance of a task carried out in the public interest), on grounds related to their particular situations. In such a case the burden of proof is on the employer to demonstrate that his/her legitimate interest overrides the interests or the fundamental rights and freedoms of the employees (or the processing is for the establishment, exercise or defence of legal claims). [Article 21 and Recital (69) of the GDPR] Finally, the employees also have the *right not to be subject to a decision based solely on automated processing, including profiling*, which would produce a legal effect concerning him/her or would similarly significantly affect the employee. (Paragraph 1 of Article 22 of the GDPR) This means that employees have the right not to be subject to decisions made without human intervention. [Recital (71) of the GDPR]

502 Costa – Poullet 2012. p. 259.

503 "*[…] the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*" (Par. 1 of Article 25 of the GDPR)

504 De Hert – Papakonstantinou 2012. p. 260.

505 "*[t]he controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.*" (Paragraph 2 of Article 25)

506 https://www.taylorwessing.com/globaldatahub/article-employee-monitoring-update.html (Accessed: 1 May 2018)

507 The aim of the assessment is to ensure the security and confidentiality of the processing. When there is a high risk which might cause difficulties to the controller in ensuring the appropriate measures, a consultation of

In conclusion, the GDPR is one of the most recent milestones in the history of data protection. Regulating the question of data protection in the form of a regulation strengthened and unified data protection law throughout the EU – even with the possibility of adopting more specific regulations in certain fields, for example, in the field of employment; leaving room for certain divergences between Member States. In spite of these divergences, the provisions presented above are cornerstones of the data protection framework. Their knowledge will be essential in assessing the processing of employees' personal data obtained from SNSs, as these are the principles and rights that are going to be tested.

(B) The right to informational self-determination in France and in Hungary

Nowadays, the right to privacy and the right to data protection continue to be challenged by new innovations. *Isabelle Falque-Pierrotin*, president of the French data protection authority drew attention to the changes regarding the relations between the right to privacy and the right to data protection caused by the appearance of a certain grey zone. This grey zone emerges when individuals want to share certain aspects of their personal life and to use their personal data to create a "public life": who, instead of seeking protection, wish to be able to have control over their personal data.[508] Therefore, besides the right to privacy and the right to data protection, another concept, the right to informational self-determination appeared as well in legal literature and order. Before addressing how the right to informational self-determination is regulated in France and in Hungary, it is necessary to clarify the conceptual foundations of the right and what the right to informational self-determination means in the international context.

(a) Conceptual foundations

The right to informational self-determination first appeared in 1983 in the famous *population census judgement* of the German Federal Constitutional Court. In the background of this decision there is an act regulating a planned population census. This act resulted in a public outcry, as citizens feared the consequences of processing such a wide range of personal data, with a considerable amount of time for retention and used for several purposes. The Act was challenged before the German Federal Constitutional Court, which upheld the general aim of the population census, but required several obligations to safeguard the processing of personal data.[509]

In its reasoning the Court argued that the provisions to be applied are the provisions of the Basic Law guaranteeing the general right to the free development of one's personality [Article 2 (1)] and the right to dignity [Article 1 (1)]. These two provisions aim to protect the value and the dignity of the individual, who functions as a member of a free society in free self-determination. The Court emphasized that in the light of the rapid technological developments allowing more elaborate data processing, the individual's decisional authority

---

the supervisory authority shall take place. [Recital (84) of the GDPR] It is considered to be easier to ensure the protection of privacy and personal data if the risks endangering them are taken into account in the early stages of the planning of the processing. Source: European Commission 2010a: par. 131.

[508] Assemblé Nationale 2014

[509] Hornung – Schnabel 2009. p. 85.

needs special protection.[510] Protection shall be granted not only to the processing of personal data having a "special private or intimate character", but also to "trivial data" as with modern data processing – through the combination of data – conclusions about the individual could be drawn even from these data.[511] Even under these circumstances of modern data processing, the individual shall be granted the freedom to make decisions freely and without influence.[512] The right to informational self-determination means that individuals are free to decide whether, who, for what purposes, etc. can process personal data relating to them.[513]

The Court emphasized the interconnectedness of the ensuring of the right to informational self-determination and other fundamental rights, noting that if the individual is uncertain about whether, who, for what purposes etc. processes his/her personal data, – instead of acting according to his/her will –, he/she will conform and adopt a behaviour that he/she thinks is considered to be in conformity with the data processors' expectations.[514] This could lead to the impairment of other fundamental rights (e.g. right to freedom of expression), damaging also the functioning of a free democratic society. Therefore, the protection against the unlimited processing of personal data must be guaranteed – based on the right to freely develop his/her personality and the right to dignity. The Court also notes that this right is not unlimited, and the individual shall accept certain limitations on the grounds of a compelling public interest.[515] Instead of providing exclusive control to the individual, the State should process the personal data in a manner respecting the rights of the individuals, a legitimate aim, and compliance with certain principles – such as proportionality, data minimisation, obligations of the data controller, rights of the data subject – is required.[516] Incidentally, although these data protection principles appeared in the population census judgement, up to now they constitute the key data protection principles.[517]

Since the appearance of the right to informational self-determination, scholars have also addressed this right. The right to informational self-determination can be connected both to privacy and to data protection: *De Hert* and *Gutwirth* point out that the right to informational self-determination can be interpreted as one of the values underlying the right to privacy and to data protection.[518]

Different scholars emphasize the connectedness of informational self-determination's to privacy: *Eva Fialová* associates it with informational privacy, and also remarks that informational self-determinations aims to ensure the control over personal data – similarly to informational privacy suggested by Westin.[519] *Jacky Richard* goes even beyond privacy and data protection and interprets the right to data protection as a defensive concept, while self-determination implies a positive content. It goes beyond the protection of the right to privacy by ensuring – instead of guaranteeing protection from interference – that the

---

[510] Kommers – Miller 2012. p. 409.
[511] Lauth 2009. p. 8.
[512] Kommers – Miller 2012. p. 410.
[513] Simitis 2010. p. 1997.
[514] Simitis 1995. pp. 447–448.
[515] Kommers – Miller 2012. p. 410.
[516] Schwartz 1989. p. 690.; Kommers – Miller 2012. p. 410.; Hornung – Schnabel 2009. p. 87.
[517] Hornung – Schnabel 2009. p. 87.
[518] De Hert – Gutwirth 2009. p. 5.
[519] Fialová 2014. p. 47.

individual is able to freely decide how to exercise his/her rights.[520] He also states that in this regard, the right to informational self-determination does not constitute a separate right, but rather a fundamental principle which gives meaning to the interpretation and guaranteeing of other fundamental rights.[521]

In contrast, *Antoinette Rouvroy* and *Yves Poullet* limit the scope of informational self-determination and argue that it should not be interpreted as self-determination, but rather as a precondition to exercising self-determination.[522] Others emphasize its connection to data protection: the right to informational self-determination can be understood as a step in the evolution of data protection – for example, *Viktor Mayer-Schönberger* examined a shift towards self-determination as part of the third generation of data protection rules.[523] Similarly, *Gloria González Fuster* and *Serge Gutwirth* understood the appearance of the right to informational self-determination in German law as the redefinition of the main rules relating to data protection.[524] *De Hert* calls for the need of revising existing data protection regulation in order to decrease the traditionally protective aspect and the passive role of the individual by providing him/her a more active role.[525]

(b) Right to informational self-determination in France and in Hungary

In France, data protection is traditionally considered as a defensive concept, but the developments of ICT challenged this concept.[526] Recognizing the changes brought by these developments, the legislator decided to step towards a more proactive protection. By adopting the *Act for a Digital Republic* in 2016,[527] significant changes were introduced to the FDPA.[528] Among these changes, the appearance of the concept of informational self-determination should be mentioned in the first place.

Inspired by the German Federal Constitutional Court's population census judgement, now the FDPA refers to the right to informational self-determination through stating that "*[t]he individuals' right to decide and to control the uses of personal data relating to him/her*" must be ensured as provided by the GDPR and by the FDPA.[529] Although the already existing data subject rights provided the possibility for the individual to participate in the processing, they did not ensure the true control over that data.[530] According to the reasoning

---

[520] However, it should not be forgotten that the individual is not completely free to decide regarding every processing: in many instances he/she cannot withdraw from the data processing. Therefore, the use of the expression informational co-determination might be more appropriate. Source: http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html(Accessed: 28 February 2018), par. [8]

[521] Richard 2016. p. 91.

[522] Rouvroy – Poullet 2009. p. 51.

[523] Mayer-Schönberger 1997. p. 229.

[524] González Fuster – Gutwirth 2013. p. 534.

[525] De Hert 2008. p. 74.

[526] Falque-Pierrotin 2012. pp. 36–37.

[527] Act No. 2016-1321 of 7 October 2016 for a Digital Republic ("Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique)

[528] Such as the right to be forgotten for minors or provisions relating to post-mortem data protection. On the reforms introduced by the act see more in: Masnier-Boché, Lorraine: Loi « pour une République numérique » : état des lieux en matière de protection des données personnelles. *Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique*, 131, 2016. pp. 50–55.; Richard 2016

[529] Article 1 of the FDPA

[530] *Rapport d'activité 2016.* La documentation française, Paris, 2017. p. 40.

of the Act, this amendment was an answer to the loss of control over personal data and contributes to the interpretation of the already existing data protection rights.[531]

Instead of considering it a separate right, *Falque-Pierrotin* understands the right to informational self-determination as "*[...] a kind of 'umbrella right' which covers the specific rights on the protection of personal data.*"[532] The right to informational self-determination should not be considered as a new right of the data subject,[533] but a principle providing sense to all these rights, a guiding principle of the French data protection act, aiming to provide the data subject the control over his/her personal data.[534]

The right to informational self-determination has been present in the *Hungarian system* since the Constitutional Court's Decision No. 15/1991. (IV. 13.), in which the Constitutional Court defined the right to informational self-determination[535] as "*the right to decide about the disclosure and use of [the individual's] personal data.*"[536] Since 1991 the *Constitutional Court* has interpreted the right to data protection as a right to informational self-determination. One of the greatest and most disputed decisions in the field of data protection[537] was *decision No. 15/1991. (IV. 13.)*, in which the Constitutional Court stated as a general legal principle that the right to data protection shall be interpreted as a right to informational self-determination, interpreting it as an active right, rather than a defensive one.[538] The Constitutional Court provided a detailed analysis regarding the content of this right – requirement of purpose limitation, rights of the data subject, legal ground of processing, etc. – laying down the fundaments of Hungarian data protection regulation and the fundaments of the data protection act to be adopted.[539, 540]

In Hungarian doctrine, instead of interpreting them as separate rights, the notions of data protection and informational self-determination are closely connected: *András Jóri* interpreted the right to data protection as a right conferring the right on the individuals to *determine* the processing of their personal data.[541] *Gergely László Szőke* interprets the right to informational self-determination as a phenomenon affecting the development of the second generation of data protection rules.[542] Similarly to data protection, the right to informational self-determination aims to ensure the protection of the private sphere.[543] As it is interpreted as an active right, this primarily relates to privacy interpreted as the right to choose how to live one's life,[544] and not to privacy interpreted as secrecy.

---

[531] Exposé des motifs: Act No. 2016-1321 of 7 October 2016 for a Digital Republic

[532] « *[...] une sorte de droit chapeau qui abriterait les droits spécifiques sur la protection des données personnelles*. » Source: Assemblé Nationale 2014. p. 9.

[533] Conseil d'Etat 2014. p. 26.

[534] Bruguière et al. 2017. p. 32., Richard 2016. p. 91., Geffray 2014. p. 515.

[535] Szüts – Karsai – Mándi 2006. p. 222.

[536] Decision No. 15/1991. (IV. 13.) of the Constitutional Court, Part II.

[537] Majtényi 2002. p. 74.

[538] Even preceding this decision, the right to data protection was already conceived as a right to informational self-determination in László Sólyom's dissenting opinion to *decision No. 2/1990 (II. 18.)*.

[539] Majtényi 2002. p. 74.; Sólyom 2001. p. 466.

[540] Similar to the French precedents, this cornerstone decision concerned the adoption of a general and unified personal identification number – which the Constitutional Court found unconstitutional.

[541] Jóri – Soós 2016. p. 15.

[542] Szőke 2013. p. 110.

[543] Péterfalvi 2014. p. 487.

[544] For example, *Máté Dániel Szabó* interprets this right in an extensive way, as according to him the right to informational self-determination implies that the individuals are entitled to decide to "*show themselves to the world*". Source: Szabó 2008. p. 335.

Despite the interpretation of the right to data protection as a right to informational self-determination, inconsistencies can be found in Hungarian legislation. Regarding the wording of the previous constitution ("protection of personal data"), former Hungarian data protection commissioner, *László Majtényi*, expressed his opinion according to which the wording as such is erroneous because it suggests that the right to data protection is a defensive right, while in reality it shall be conceived as the right to informational self-determination.[545] It is interesting to note that the legislator did not correct this mistake when adopting the new constitution, despite the fact that the Constitutional Court interpreted the right to data protection as a right to informational self-determination and that the new data protection act is also entitled as the act on the right to informational self-determination.[546] The HDPA is entitled as the "*Act on the Right to Informational Self-Determination and on Freedom of Information*", however, the expression "informational self-determination" is not present in the text of the HDPA. Naturally, through the regulation of the purpose limitation principle or the rights of the data subjects, the right to information self-determination prevails without being specified.

In conclusion, though the appellation suggests that it constitutes a separate right, I understand the above-presented views as suggesting that instead of a separate right, the right to informational self-determination constitutes a guiding principle of privacy and/or data protection law, emphasizing the active aspect of these rights. This is also supported by the fact that the expression "right to informational self-determination" is not mentioned either in the DPD or in the GDPR.[547] Neither in France, nor in Hungary does the right to informational self-determination constitute a right separate from data protection. The right to information self-determination appeared relatively late in *French* data protection law, but not as a separate right. Incorporated into the FDPA, it is conceived as a guiding principle of French data protection law, emphasizing the importance of ensuring that the individual exercises true control over his/her personal data. In *Hungary*, the right to data protection is interpreted as a right to informational self-determination, being an active right. According to the preamble of the HDPA, the Act was adopted in order to ensure the right to informational self-determination. Like in French law, instead of constituting a separate right, it rather remains a guiding principle.

Chapter 2: Employee control and monitoring

The employer is in control of the employment relationship: he/she can unilaterally determine the conditions of the employment relationship, resulting in the subordinate position[548] of the employee.[549] It means that the employer is entitled to choose amongst applicants, to

---

[545] Majtényi 1995. p. 96.

[546] *Béla Pokol* expressed in his paralell reasoning that the Constitutional Court shall respect the decision of the legislator not to insert into the Fundamental Law the terminology suggested by the Constitutional Court. Source: par. 144 of Decision no. 32/2013 (XI. 22.)

[547] Even though Recital (7) of the GDPR declares that "*[n]atural persons should have control of their own personal data.*"

[548] Under subordination the employee provides his/her workforce (and not his/her whole life or personality), according to his/her best knowledge, while following the employer's instructions.

[549] Kiss 2003. p. 80.

organize the work, and instruct employees, monitor compliance with instructions or even to sanction them. It is important to emphasize that controlling and monitoring employees is not an arbitrary decision of the employer: the employer is not only entitled to monitor employees, it is also his/her obligation at the same time.[550]

Although these rights/powers are inherent to the employment relationship itself, they are not absolute, as employees' rights – such as the right to privacy and the right to data protection – impose limitations on the employer's right to monitor.[551] During enforcing these powers/rights, the employer limits employees' rights, such as their right to privacy or right to data protection. Controlling and monitoring employees interfere with privacy and data protection, as posing limitations on the use of SNSs might concern the employees' personal life, while consulting whether the employee complies with such a regulation implies data processing and as such concerns data protection. However, such a limitation must not be without limits or abusive: the employer's rights must be balanced against the employees' rights – such as the right to privacy and right to data protection. As the WP29 neatly formulated:"*[w]orkers do not abandon their right to privacy and data protection every morning at the doors of the workplace.*"[552] However, these rights are not absolute either, as they are also limited by the employer's right to monitor.[553] Therefore a balance must be found between the two sides.[554]

Chapter will analyse the existence of the employer's right to control and monitor, and then the present state of legal rules regulating employee monitoring – serving as a conceptual basis for the detailed analysis of monitoring and SNSs in Part II. The knowledge of these rules is crucial as they constitute the general framework of different emergences of employee monitoring – and amongst them social media.

Chapter 2 is composed of two Sections: *Section 1* will present what is at stake on the other side against the right to privacy and right to data protection. It will deal with how the right to monitor is acknowledged in labour law. Then, *Section 2* will deal with how exactly this collision appears in the context of employment, what the already established rules at the international and national level in the field of employee monitoring are.

Section 1: The employer's right to monitor

Anders J. Persson and *Sven Ove Hansson* emphasized the significance and specificity of the employment relationship: according to them it is the rights and obligations ensuing from the employment contract which makes workplace privacy/monitoring issues such a specific subject, compared to other kinds of relations.[555, 556] They argue that an intrusion into the privacy of employees must be justified by what the parties can require from each

---

[550] Gyulavári 2013. pp. 248–249.

[551] Hendrickx 2002. pp. 23–24.

[552] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 4.

[553] Plasschaert 2017. p. 106.

[554] Hajdú 2005. p. 20.

[555] Persson – Hansson 2003. p. 63.

[556] The ILO highlighted the significance of processing in the employment context from a different aspect stating that "[i]n hardly any other case are so many personal data processed over such a long period of time as in connection with the employment relationship." Source: *Protection of workers' personal data. An ILO code of practice*. International Labour Office, Geneva, 1997. p. 8. (Commentary)

other based on the rights and obligations set forth in the employment contract.[557] This supposes that the privacy issues are specific regarding the employment relationship (other kinds of legal relations such as self-employment, entrepreneurship or mandates give rise to different kinds of privacy challenges) and that the employer's right to monitor can be derived from the obligations and rights imposed on the parties.

Given the importance of the employment relationship, it must be examined what employment is and what its main characteristics are, making it special in the field of workplace privacy and data protection. It follows from the subordination between the employer and employee that the employer has power to exercise authority over employees.[558] *Frank Hendrickx* identified monitoring as an element of authority and subordination, which is essential in the employment relationship.[559] The Section will first explore the main characteristics of the employment relationship, and the rights and obligations ensuing from it, which also give rise to the employer's right to monitor.

These characteristics and the main observations drawn from them are common to industrialized societies, therefore the right to monitor will first be approached from *(§1)* a more general angle, based on international standards and rules. The exact appearance of these general principles and rights can differ from state to state, therefore then *(§2)* it will be addressed how the right to monitor materializes in the French and in the Hungarian legal order.

§1. Rights and obligations arising from the employment relationship

The *ILO* addressed the question of the employment relationship – which is a concept common in every legal system[560] – on several occasions. In a document entitled "T*he employment relationship. Report V(1)*", the ILO demonstrated through several examples that when it comes to the employment relationship, the most commonly used factors to describe this relationship (in order to delimitate it from other concepts) are dependency, subordination, authority, direction, supervision, control.[561]

A report and questionnaire were sent out to the Member States' governments containing different questions regarding the possible content of an ILO document. Question eleven [Qu. 11 (1)–(3)] was related to the factors and indicators determining the existence of an employment relationship, and to the question what indicators should be used in order to achieve this [Qu. 11 (3)]. Dependency, subordination, supervision, control of work, direction, authority were often listed by governments.[562] Finally, the adopted Recommendation included amongst the possible indicators that the work "*[...] is carried out according to the instructions and under the control of another party [...]*"[563] The annotated guide to the Recommendation, while referring to Paragraph 12 of the Recommendation, identifies control and dependence (or subordination) amongst the most important criteria.[564]

---

[557] Persson – Hansson 2003. p. 64.
[558] Hendrickx 2002a. p. 49.
[559] Hendrickx 2001. p. 248.
[560] ILO 2006. p. 6.
[561] ILO 2006. p. 21.
[562] ILO 2006a. pp. 155–160.
[563] *Recommendation concerning the employment relationship*. (No. 198.) 95th ILC session, Geneva, 2006. par. 13 a
[564] ILO 2007. p. 33.

Control is considered to be an important indicator of subordination.[565] In every industrial country, the employment relationship is centred on subordination and is conceived as a relation where the employer can command and the employee shall obey.[566] The fundamental concepts laid down in these documents are relevant for European countries as well. A report prepared by members of the European Labour Law Network (hereinafter referred to as: ELLN) addressing the question of the characteristics of the employment relationship in the EU argued that "*[i]n all countries, the main criterion for establishing an employment relationship or an employment contract is that one person is subordinated to or dependent on another person.*"[567] It basically refers to the organisational subordination,[568] meaning that "*the employee is subjected to supervisory power exercised by the employer.*"[569] The CJEU also confirmed that "*[t]he essential characteristic of the employment relationship is that for a certain period of time a person performs services for and under the direction of another person in return for which he receives remuneration*".[570]

This could be described by four characteristics. *First*, organisational subordination, which encompasses the employer's power to give instructions regarding the work: both personal and functional instructions. *Second*, the control of work and the supervision of employees are also considered to be crucial in most Member States. *Third*, the integration of the employee into the organisation is often a relevant indicator. *Finally*, amongst the 'other' indicators, the provision of tools and materials by the employer and the fact that work is carried out within specific hours or at an agreed time can also be an indicator of organizational dependence.[571] Another, more recent study in 2013 affirmed the importance of dependency and/or subordination when determining the existence of an employment relationship, which often involves control and the power to give instructions to employees, and provided several examples from EU Member States' legal systems.[572]

A study[573] conducted back in 2001 under the supervision of *Frank Hendrickx* analysed the labour law regulations of EU Member States with regard to employee data protection and monitoring. This study also stated that the authority of the employer and the (legal) subordination of the employee are common factors in all Member States when it comes to the employment relationship.[574] It refers to the general labour law principles and acknowledges that "*these principles imply that employers have a contractually based right to control contract fulfilment and to monitor work performance and the proper use by employees of company equipment facilities.*"[575] Ensuing from authority and from the right to manage the workplace, the employer – who is also the owner of the company equipment – is entitled

---

565 ILO 2007. pp. 35–36.

566 Supiot 2002. p. 109.

567 European Network of Legal Experts in the field of Labour Law 2009. p. 16.

568 Economic dependency also exists, but its mere existence is not enough to establish the existence of an employment relationship. When it comes to economic dependency, the indicators of remuneration, bearing of financial risks and work performed solely or mainly for the benefit of the employer shall be examined. See more in: European Network of Legal Experts in the field of Labour Law 2009. pp. 19–21.

569 European Network of Legal Experts in the field of Labour Law 2009. p. 16.

570 CJEU: *Case C-27/91*, 1991. par. 7.

571 European Network of Legal Experts in the field of Labour Law 2009. pp. 16–19.

572 International Labour Office, Governance and Tripartism Department and European Labour Law Network 2013. pp. 36–40.

573 Hendrickx 2002.

574 Hendrickx 2002. pp. 12–13.

575 Hendrickx 2002. p. 114.

to impose certain limitations on its use.[576] For example, health and safety requirements, the protection and the correct use of the employer's equipment, monitoring production processes and work performance and conducting quality control can justify employee monitoring.[577, 578] Moreover, the employee has not only rights, but also certain obligations such as carrying out work in person, respect and cooperate with his/her colleagues, loyalty towards the employer – where controlling the compliance with these obligations can justify monitoring.

Monitoring employees' use of SNSs might contribute to the enforcement of several of these rights. *In the hiring phase*, it is notably the employer's right to choose the most adequate applicant that might be enforced though conducting social media background checks. Monitoring SNS use *during working hours* at the expense of working hours might constitute a method for the employer to enforce his/her interests and rights in the field of productivity, work performance and the protection of the work equipment. Monitoring SNS use beyond working hours can serve the purposes of protecting against employee conducts detrimental to the employer's reputation or the leaking of business interests. On the details and the possibility of monitoring employees' use of SNSs in order to achieve these interests will be dealt with in detail in Part II.

§2. Appearance of the right to monitor in national legal orders

It is worth noting that in the different languages used for the research different terminologies are used to describe similar phenomena. In English literature the expression right to monitor is used, while in French literature the expression *employer's power* ("pouvoir") is employed, comprising the prerogative to control work. The Hungarian literature mentions *legitimate economic interests of the employer* ("jogos gazdasági érdek"), as the main value is materialized in the form of the right of the employer to direct, to give orders and to control ("irányítási, utasítási és ellenőrzési jogkör").

(A) France: the employer's powers

In both countries subordination has great importance when it comes to determining the existence of an employment relationship. In *French law*, subordination is a key element of the employment relationship. The Court of Cassation defined the employment contract in its jurisprudence as "*a convention according to which a person engages in performing work for another person under its subordination for remuneration*."[579] The employment

---

[576] Hendrickx 2002. p. 101.

[577] Hendrickx 2002. p. 119. More specifically, the monitoring of *the use* of the employer's equipment (e.g. telephone, computer, Internet) may be justified by the following lawful purposes: monitoring work performance and quality control, monitoring compliance with different standards and procedures, investigating and detecting the security of the system, preventing crimes, collecting evidence of business transactions.

[578] *Roger Blanpain* also identified property rights, the right to manage and employer's liability amongst the employer's legitimate interest to monitor (the employees' use of computer). Blanpain 2002. pp. 43–44.

[579] "*Le contrat de travail est une convention par laquelle une personne s'engage à travailler pour le compte d'une autre et sous sa subordination moyennant une remuneration.*" Cour de cassation du 22 juillet 1954 (Bull. civ. IV, no 576) referred to in: Le Lamy social 2019

contract – originally based on the idea that the worker leases his workforce – supposes the leasing of the employees' workforce. As the employer could not take possession of the employees' workforce, this lack was compensated by the employees' subordination to the employer.[580]

In order to be qualified as an employment contract, three attributes must be present: the employee has to (1) perform *work* (2) under the *legal subordination* of the employer (3) in exchange for *remuneration*.[581] These main elements also appear in the definition of labour law provided by *Gérard Lyon-Caen*, who argued that labour law is "*all the legal rules applicable to individual and collective relations between private employers and employees who work under their authority for a remuneration called salary.*"[582] Subordination means that the employee is under the authority of the employer and is manifested in the employer's power to give orders, and the employees' correlative obligation to obey those orders.[583] According to a landmark decision of the Court of Cassation, subordination is characterised by the "*execution of work under the authority of an employer who has the power to give orders and directives, to control their execution, and to sanction the breaches of the subordinates*."[584] Different indicators can help to determine the existence of subordination, such as the exercise of authority, the right to control whether employees comply, the right to impose sanctions (essential criteria),[585] the employer bearing the risk of his/her activity, integration into the organisation,[586] the equipment and raw material provided by the employer, work hours defined by the employer,[587] the localisation of work.[588] The subordinate relation originates from the submission to the employer's regulatory, directive and disciplinary power in order to perform work on behalf of the employer.[589, 590]

From the definition of the employment contract itself, the main obligations and rights of the parties (connected to the three central attributes: work, remuneration and subordination) can be identified. On the one hand, the employer shall provide work for the employee;[591] while on the other hand, the employee is obliged not only to work but also to be at the

---

[580] Supiot 2000. p. 132.

[581] Peskine – Wolmark 2016. p. 27. and pp. 27–34.; Bailleul – Jourdan 2011. p. 20. and pp. 20–22.; Hess-Fallon – Maillard – Simon 2015. p. 88., and pp.88–90.; Petit 2011. p. 74.

[582] "*L'ensemble des règles juridiques applicables aux relations individuelles et collectives qui naissent entre les employeur privés et les salariés qui travaillent sous leur autorité, moyennant une rémunération appelée salaire*." Source: Ray 2018a. p. 14.

[583] Kéfer – Cornélis 2009. p. 782.

[584] "*[...] que le lien de subordination est caractérisé par l'exécution d'un travail sous l'autorité d'un employeur qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements de son subordonné*." Cass. soc., 13 novembre 1996, N° 94-13187

[585] Bailleul – Jourdan 2011. p. 22.

[586] Peskine – Wolmark 2016. pp. 31–33.

[587] Hess-Fallon – Maillard – Simon 2015. p. 90.

[588] Petit 2011. p. 75.

[589] Mazeaud 2016. p. 339.

[590] *Emmanuel Dockès* draws attention to the fact that labour law was originally conceived based on the work performed by industrial workers. Therefore, attention should be paid when assessing the new forms of performing work. *Jean-Emmanuel Ray* has pointed out in one of his articles that technological changes may question the assessment of these indicators, and especially their effects on working hours and place of work might be "challenged". Sources: Dockès 2004. p. 1. (Page number referring to the online version of the article downloaded from: https://www-dalloz-fr); Ray 1992. pp. 1–4. (Page number referring to the online version of the article downloaded from: https://www-dalloz-fr)

[591] Cass. soc., 17 février 2010, N° 08-45298

disposal of the employer.[592] One of the employer's main obligations is to pay remuneration for the work, while the employee has the right to be remunerated.

Following from the criteria of subordination, the employer has different powers in relation to ensuring the appropriate functioning of the workplace. The employer has the power to manage, to regulate and to discipline, while the employee must respect the instructions of the employer.[593] The power to manage comprises several elements in order to organise work and is implemented through the right to give detailed orders. Giving instructions is not only a right: the employer is also obliged to do this, as it is his/her task to tell the employee how to perform the work. At the same time, it is also his/her right and obligation to control work and maintain work discipline.[594] In accordance with these powers/rights, the employee shall perform work according to the instructions of the employer.[595]

Both the French Labour Code[596] (hereinafter referred to as: FLC) and the Hungarian Labour Code[597] (hereinafter referred to as: HLC) contain some *general provisions*, which are present in both jurisdictions. The FLC states that the contract has to be executed in good faith,[598] specify the employee's obligation of loyalty[599] and contain provisions relating to the declarations of employees.[600] French labour law declares that the employee has to perform work with diligence and obligation of discretion.[601] The employer shall provide the necessary working conditions,[602] which connects back to his/her authority: he/she shall adequately organise the work, shall manage, instruct and inform employees regarding work, shall provide the necessary knowledge for work, shall control work and shall discipline employees. In both countries – in accordance with EU regulation[603] – the employer has important obligations in the field of workplace safety and health: he/she shall ensure the conditions of occupational health and safety,[604] while the employee shall respect safety instructions.[605] The FLC also expressively regulates the issue of psychological[606] and sexual harassment,[607] making it the employer's obligation to prevent these issues.

In French law, the employer, who is responsible for the organisation, management and the general functioning of the workplace,[608] has certain powers to ensure its effective functioning.[609]

---

592 Article L3121-1 of the FLC

593 Article L3121-1 of the FLC

594 Casaux-Labrunée 2012. p. 335.

595 Article L3121-1 of the FLC

596 Code du travail

597 Act I of 2012

598 Article L1222-1 of the FLC and Subsection (2) of Section 6 of the HLC

599 Subparagraph 3 of Article L1222-5 of the FLC and Section 8 of the HLC

600 From Article L1222-2 to Article L1222-4 of the FLC

601 Hess-Fallon – Maillard – Simon 2015. pp. 106–107.

602 Hess-Fallon – Maillard – Simon 2015. p. 106.

603 European Union: Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC)

604 Subparagraph 1 of Article L4121-1 of the FLC

605 Subparagraph 1 of Article L4122-1 of the FLC

606 From Article L1152-1 to Article L1152-6 of te FLC (Also from Article L1154-1 to L1154-2 and from Article L1155-1 to Article L1155-2)

607 From Article L1153-1 to Article L1153-6 of the FLC (Also from Article L1154-1 to L1154-2 and Article L1155-1 to Article L1155-2)

608 Cass. soc., 25 février 1988, N° 85-40821

609 Originally, two theories aimed to define the source of these powers. According to the "*théorie contractuelle*", these powers originate from the employment contract itself, where the employee accepts the subordination

Originally, in the Brinon decision, the employer was perceived – as he/she is the one having responsibility – as the "*only judge*" to determine what decisions to make as regards the employees and the functioning of the workplace while complying with the legal regulations,[610] which granted extensive powers to the employer. Later, these powers were limited, especially by the adoption of the Act Auroux in 1982, which regulated, and therefore imposed limitations on the internal regulations and sanctions.[611] The next significant act in the subject was the act of 31st December 1992,[612] which (inspired by the "Lyon-Caen report"[613]) inserted the famous article L120-2 into the FLC, guaranteeing the general protection of the employee's liberties and rights – at the same time imposing limitations on the employer's powers. With this article, the legislator laid down the foundations of the protection of the employee's rights and freedoms. Three different employer prerogatives are distinguished: power to manage ("pouvoir de direction"), power to regulate ("pouvoir législatif" or "pouvoir réglementaire") and power to discipline ("pouvoir disciplinaire").[614]

The *power to manage* suggests two different elements: the management of the company and the management of the personnel. It follows from the principle of the entrepreneurial freedom that the employer has the prerogative to decide how to manage his/her business. As presented above, the Brinon decision acknowledged the employer's power to freely – while complying with the legal regulations – take decisions regarding his/her business.[615] Resulting from the subordinate relationship between the parties, the employer has the power to manage not only the undertaking itself, but also the personnel: he/she can decide who to hire or who to dismiss, can give instructions, can determine the tasks, can organise workflow and (not only can, but is also obliged to) control, monitor the execution.[616]

The employer's *power to regulate* means that the employer is empowered to establish general and permanent rules, norms relating to the functioning of the workplace, notably through the adoption of an internal regulation.[617] Strict limitations were imposed on the internal regulation by the act of 4 August 1982, detailing the requirements set towards an internal regulation. Especially Article L. 122-35 inserted into the FLC is significant for the subject of the monograph. This article (inspired by the Corona decision of the State Council)[618] stated that "*[the internal regulation] may not limit the rights of the individual or individual or collective liberties by any restriction which is not justified by the nature of the task to be performed and proportionate to the aim sought.*" The Act of 31 December

by contracting, while according to "*théorie institutionnelle*" – notably represented by Paul Durand – these powers are born from the reality that the employee is part of the undertaking. Source: Peskine – Wolmark 2016. p. 161.

610 Cass. soc., 31 mai 1956, N° 56-04323

611 Act No. 82-689 of 4 August 1982 on the freedoms of employees in the workplace ("Loi n°82-689 du 4 août 1982 relative aux libertés des travailleurs dans l'entreprise")

612 Act No. 92-1446 of 31 December 1992 on employment, the development of part-time work and unemployment insurance

613 Lyon-Caen 1992.

614 Durand – Jaussaud 1947. p. 423.

615 Cass. soc., 31 mai 1956, N° 56-04323

616 Waquet – Struillou – Pécaut-Rivolier 2014. pp. 33–39.

617 Petit 2011. p. 275.

618 In the *Corona decision* the State Council stated that the examined provisions of the internal regulation in question were not justified because when the employer exercises his/her powers to ensure workplace health and safety, he/she can only limit employees' rights by a restriction necessary to achieve the aim sought. Conseil d'Etat N° 06361, 1980, Section, 1 février

1992 extended this protection by changing the expression internal regulation to "no one". The prerogative to adopt an internal regulation has also become an obligation for employers who usually employ at least 20 employees.[619] The internal regulation shall regulate the question of health and safety and work discipline (with special regard to the nature and scale of the possible sanctions).[620] The FLC also addresses in detail the procedure of adopting an internal regulation[621] and the rules relating to the administrative and judicial control over the internal regulation.[622, 623]

The *power to discipline* is inherent to the employer[624] and is a necessary complement to enforcing the other prerogatives.[625] The employer has the power to apply sanctions for the wrongful acts of the employees.[626] The act of 4 August 1982 also introduced several limitations, creating a legal framework for the employer's power. When exercising this power, the employer has to respect procedural rules.[627] Also, it is forbidden to impose monetary sanctions on employees,[628] or to impose a sanction which was not prescribed by the internal regulation.[629]

With regard to SNSs, following from the rights and obligations of the parties, the above means that employers do have the power to regulate how employees can use SNSs and control whether they have complied with such a regulation. The exact outlines of this power are to be addressed in detail in Part II. dealing with certain aspects of SNS use.

(B) Hungary: the employer's legitimate interests

The HLC defines the employment contract as a contract where the employee is required to work *as instructed by the employer*, while the employer is required to provide work for the employee and to pay wages.[630] As such, an employment relationship supposes the employee's subordination and dependency.[631] In order to determine the existence of an employment relationship, a joint administrative directive issued by the Ministry of Labour and the Ministry of Finance in 2005 provides certain primary and secondary criteria. The primary criteria – which can be in themselves decisive when determining the existence of an employment relationship – contain subordination, the obligation to perform work

---

619 Subparagraph 1 of Article L1311-2 of the FLC

620 Item 1° of Subparagraph 1 of Article L1321-1 of the FLC

621 Submission for the opinion of the social and economic committee and communication to the labour inspector and to labour courts and making it available to every person who has access to the place where work or recruitment takes place. Article L1321-4 and Article R1321-2 of the FLC

622 From Article L1322-1 to Article L1322-3 of the FLC; Article L1322-4 and Article R1322-1 of the FLC

623 The Court of Cassation ruled that in the absence of the required consultation, the dismissal of an employee based on the infringement of the provisions of the internal regulation was considered to be void of real and serious cause. Source: Cass. soc., 9 mai 2012, n° 11-13.687

624 Cass. soc., 16 juin 1945

625 Durand – Jaussaud 1947. pp. 436–437.

626 Article 1331-1 of the FLC

627 They are contained in the FLC from Article 1332-1 to Article 1332-5

628 Subparagraph 1 of Article L1331-2 of the FLC

629 Cass. soc., 26 octobre 2010, N° 09-42740

630 Subsection (2) of Section 42 of the HLC

631 Hajdú – Kun 2012. p. 108.

personally, the obligation to provide work and the nature of the activity, the specification of the tasks to be performed in the job.

In this context subordination supposes a hierarchal relation between the parties, where the employee performs work while being integrated into the business, resulting in the employer's right to direct and to give orders. The secondary criteria – which, not in themselves but together with the presence of other criteria, can indicate the existence of an employment relationship – contain indicators such as the employer's right to direct, to give orders and to control; the determination of the duration of work and the schedule of working time by the employer, the determination of the place of employment/work by the employer; remuneration for the work; use of the employer's assets, resources and raw materials; the employer's obligation to ensure the conditions for occupational safety and health and contract in writing.[632] *György Kiss* argues that legal subordination and the long-term nature of the employment relationship are the two crucial criteria.[633] *Tamás Gyulavári* emphasizes as well that the most important characteristic of the employment relationship is dependency,[634] which is manifested in the hierarchal relationship between the employer and the employee, resulting in the wide-ranging right of the employer to direct, to give orders and to control,[635] meaning that the employer can give orders relating to any aspect of the employment: he/she can define the means, place and time of working.[636] However, giving orders is not without limits, other provisions of the HLC must be respected.[637] Employees perform work in a subordinate and dependent manner, according to the employer's instructions: as the work is done on the behalf of the employer, the employer bears the risks and results of the work, the employee simply offers his/her workforce.[638]

Similarly to French law, the rights and obligations of the parties are interconnected: what is a right on one side will be an obligation on the other side.[639] The main obligations consist of providing work for the employee,[640] who has to work[641] and be at the employer's disposal;[642] and of providing remuneration for the work – while the employee has the right to be remunerated.[643] Following from the criteria of subordination, the employer is entitled and at the same time obliged to create the conditions necessary for work, which includes

---

632 7001/2005. (MK 170.) FMM-PM együttes irányelv a munkavégzés alapjául szolgáló szerződések minősítése során figyelembe veendő szempontokról. Although this directive has since been repealed, its main principles still remain valid.

633 Kiss 2015. p. 5.; Kiss 2017. p. 273.

634 Also stated in the explanations relating to Section 42 of the HLC in *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről*, 2011.

635 Gyulavári 2017. p. 34.

636 Kardkovács 2012. p. 91.

637 Radnay 2003. p. 64.

638 Lehoczkyné Kollonay 1997. pp. 8-9.

639 Gyulavári 2017. p. 235.; Prugberger 2011. p. 283.

640 Subsection (1) of Section 51 of the HLC

641 The HLC [Item c) of Subsection (1) of Section 52] defines it among the main obligations of the employee as the obligation to perform work in person with the level of professional expertise and workmanship that can be reasonably expected, in accordance with the relevant regulations, requirements, instructions and customs.

642 Item a) of Subsection (1) of Section 52 of the HLC (on the obligation to appear at the place and time specified by the employer, in a condition fit for work) and Item b) of Subsection (1) of Section 52 of the HLC (on the obligation to be at the employer's disposal in a condition fit for work during their working time for the purpose of performing work)

643 Item b) of Subsection (1) of Section 42 of the HLC

organizing the work, managing employees, giving instructions and information, controlling work and maintaining work discipline.[644] In accordance with these rights, the employee must perform work according to the instructions of the employer.[645]

Similarly to the FLC, the HLC also stipulates that the contract has to be executed in good faith [Subsection (2) of Section 6] and the employee is subjected to an obligation of loyalty (Section 8). In addition, the HLC regulates among the common rules of conduct the requirement of what can reasonably be expected in the given circumstances ("általában elvárhatóság"),[646] the respect of the principles of fairness, mutual cooperation,[647, 648] the requirement of taking into account the interests of the employees[649] and the requirement of providing information.[650] Moreover, the abuse of rights is prohibited.[651]

The HLC also adds that the employee has to behave in a way that demonstrates the trust vested in him/her for the job in question:[652] when exercising his/her rights, the employee has to take into consideration the employer's interests, not only during working hours but also beyond them.[653] Also, he/she shall not jeopardize the legitimate economic interests of the employer.[654] The employee shall also cooperate with co-workers.[655] The employer shall provide the necessary working conditions,[656] which connects back to his/her authority: he/she shall adequately organise the work, shall manage, instruct and inform employees regarding work, shall provide the necessary knowledge for work, shall control work and

---

644 Gyulavári 2013. p. 247.

645 Kajtár 2014. p. 215. and Subsection (2) of Section 42 of the HLC

646 Subsection (1) of Section 6 of the HLC "*Employment contracts shall be executed as it might normally be expected in the given circumstances, unless any legal provision exists to the contrary. A person may not rely, in support of his or her claim, on an unlawful act he or she has committed. A person who himself or herself engaged in an unlawful act may rely on the wrongful act committed by others.*"

647 Subsection (2) of Section 6 of the HLC "*In exercising rights and discharging obligations, the parties involved shall act in the manner consistent with the principle of good faith and fair dealing, they shall be required to cooperate with one another, and they shall not engage in any conduct to breach the rights or legitimate interests of the other party. The requirements of good faith and fair dealing shall be considered breached where a party's exercise of rights is contradictory to his or her previous actions which the other party had reason to rely on.*"
For example, adopting a workplace communication style according to the rules of civilized human behaviour or adopting a behaviour that takes into account mutual respect and human dignity fall under the obligation of cooperation. (Kozma 2013. p. 8. and BH2006. 201.)

648 In the employment relationship both the employer and the employee must actively contribute to the legal relationship: the employer organizes and directs the work, gives instructions, while the employee performs the work itself; which makes cooperation between the parties indispensable. Source: Miholics 2015. p. 247.

649 Subsection (3) of Section 6 of the HLC "*Employers shall take into account the interests of workers under the principle of equitable assessment; where the mode of performance is defined by unilateral act, it shall be done so as not to cause unreasonable disadvantage to the worker affected.*"

650 Subsection (4) of Section 6 of the HLC "*The parties falling within the scope of this Act shall inform each other concerning all facts, information and circumstances, and any changes therein, which are considered essential from the point of view of employment relationships and exercising rights and discharging obligations as defined in this Act.*"

651 Subsection (1) of Section 7 of the HLC. On these common rules of conduct see more in: Miholics 2015

652 Item d) of Subsection (1) of Section 52 of the HLC

653 Gyulavári 2013. p. 262.

654 Ember 2015. p. 113.; Section 8 of the HLC. These provisions will be addressed in detail in Part II.

655 Item e) of Subsection (1) of Section 52 of the HLC

656 Subsection (1) of Section 51 of the HLC

shall discipline employees.[657, 658] Also, he/she is obliged to ensure conditions of occupational health and safety,[659] while the employee shall respect safety instructions.[660]

The right to direct comprises several elements in order to organise work and is implemented through the right to give detailed orders. Giving instructions is not only a right: the employer is also obliged to this, as it is his/her task to tell the employee how to perform the work.[661] The employer's right to give instructions covers every aspect of working, during the whole lifetime of the employment relationship and he/she can exercise complete and detailed control over their implementation.[662] At the same time, it is also his/her right and obligation to monitor work[663] and maintain work discipline.[664] As explained above, the employee shall perform work according to the instructions of the employer.[665]

Internal policies[666] can be understood as the employer's instruction.[667] The employer is entitled to *regulate* in internal policies matters covered by his/her right to instruct.[668] Internal policies, the employer's power to regulate originate from the right to give instructions, which can be traced back to the hierarchal relation present between the parties.[669] In consequence, the matters regarding which an internal policy can be drafted are various, such as regulating conflict of interests, behaviour at work, norms relating to clothing or even behaviour outside the workplace – [670, 671] resulting in the employer being able to control, impose limitations on the behaviour of employees.

According to Hungarian labour law regulation, the employer shall provide the necessary working conditions,[672] which means that he/she shall adequately organise the work, shall manage, instruct and inform employees regarding work, shall provide the necessary knowledge for work, shall control work and shall discipline employees.[673] It follows from the employer's obligation to ensure safe working environment and the obligation to organize work that he/she is also entitled to monitor whether employees comply with the given

---

657 Gyulavári 2013. p. 247.

658 On the rights and obligations of the parties see more in: Prugberger, Tamás – Nádas, György: *Európai és magyar összehasonlító munka- és közszolgálati jog*. Wolters Kluwer, Budapest, 2014. pp. 199–208.

659 Subsection (4) of Section 51 of the HLC

660 Section 1 of Article 60 of Act XCIII of 1993 on labour safety

661 Kardkovács 2016. p. 135.

662 Gyulavári 2013. p. 38.

663 Szűcs 2013. p. 15.

664 Gyulavári 2013. p. 249.

665 Subsection (2) of Section 42 of the HLC

666 Subsection (1) of Section 17 of the HLC: "*(1) Employers shall be able to implement the legal acts referred to in Sections 15–16 [relating to Unilateral acts, statements and commitments] by means of internal rules established of its own accord or by way of a procedure formulated unilaterally (hereinafter referred to as: 'employer's internal policy').*"

667 Kiss 2005. p. 80.

668 Gyulavári 2017. p. 98.

669 Gyulavári – Kun 2013. p. 557.

670 Berke – Kiss 2014. p. 91.

671 Additional provisions require that "*[e]mployers shall consult the works council prior to passing a decision in respect of any plans for actions and adopting regulations affecting a large number of employees*." [Subsection (1) of Section 264 of the HLC] The processing and protection of personal data of employees and the implementation of technical means for the surveillance of workers are among the matters concerned by the obligation of consultation. [Items c) and d) of Subsection (2) of Section 264 of the HLC]

672 Subsection (1) of Section 51 of the HLC

673 Gyulavári 2013. pp. 238–239.; Kajtár 2014. p. 214.

orders.[674] As such, monitoring employees will not only be a right of the employer,[675] but at the same time it is an obligation as well.[676] However, such a monitoring cannot be unlimited: as it will be explored later, employees' rights, notably rights relating to the personality,[677] limit the enforcement of the employer's right to monitor to a certain extent.

The employer is entitled to issue a warning to an employee, in case he/she founds that the employee is committing a breach of duty.[678] It follows from these rights and obligations that the employer is entitled to *discipline* employees through different sanctions in case of wrongful breach of obligations.[679] Detrimental legal consequences – proportionate to the breach of duty – may be applied if the employee infringed an obligation arising from the employment relationship, he/she was culpable and the detrimental legal consequence is prescribed by a collective agreement, or – if the employer or the employee is not covered by the collective agreement – by the employment contract.[680] The employer can modify the sphere of duties or the salary of the employee, withdraw benefits or impose fines – while respecting the employee's right to dignity and personality rights.[681] In the most serious cases the employer can terminate the employment by dismissal.[682]

In conclusion, following from the specific rights and obligations imposed on the parties, the employer's rights/powers in the field of control and monitoring enable him/her to control employees, to give them instructions, and to monitor compliance. It means that on the one hand, the employer can determine certain rules in relation to the use of SNSs (e.g. maintaining work discipline, defending his/her reputation, etc.), and on the other hand, he/she can verify whether the employee complies with instructions and legal obligations imposed on him/her, such as obligation of loyalty, obligation of work, etc. (e.g. monitoring whether the employee surfs on Facebook instead of working during working hours, or inspecting SNS profiles to ascertain whether the employee damages the employer's reputation through a post, etc.).

Section 2: Legal rules relating to employee monitoring

Besides the already presented general data protection framework, it also became necessary to adopt employment specific regulations in order to effectively ensure employees' right to data protection. The data protection regulation recognizes the legitimacy of employee monitoring, by not prohibiting the processing of employees' data in relation to monitoring, but by channeling it through requiring the respect of certain privacy and data protection measures. Although the right to privacy and the right to data protection are both concerned, it is mainly through the data protection approach that the different organizations and institutions, as well as national jurisdictions approached this question.[683]

---

674 Horinka 2018. p. 627.; Ember 2012. p. 30.
675 Hajdú – Kun 2014. p. 88.
676 Szűcs 2013. p. 15.
677 Horinka 2018. p. 627.
678 Cséffán 2018. p. 206.
679 Gyulavári 2013. p. 249.
680 Subsection (1) of Section 56 of the HLC
681 Kardkovács 2016. pp. 144–145.
682 Gyulavári 2017. p. 240.
683 As the ILO stated, technological development made it necessary to create data protection rules for the employment context "*[…] in order to safeguard the dignity of workers, protect their privacy and guarantee*

The Section will examine the international organizations – notably the EU and the CoE – which already addressed the question of processing employees' data and adopted legal norms and documents in this field. These documents already addressed the traditional forms of monitoring – e.g. CCTV monitoring, monitoring of e-mail and Internet use, geo-localisation, etc. However, new innovations challenge the established rules, and raise several questions. The most recent international documents already touched upon the question of SNSs, but they only devote brief provisions to the subject.[684] An exhaustive regulation of data processing and SNSs in the employment context has not yet been elaborated, neither by the CoE nor by the EU.

Although focus will be put on the European legal order, because of its significance, the *International Labour Organization* must also be mentioned briefly. At the universal level, in 1997, the ILO issued a code of practice regulating the processing of employees' personal data.[685] The code of practice is an instrument without binding force; however, it contains detailed regulation regarding the processing of employees' personal data.[686] Despite the lack of binding effect, given the ILO's importance and the rapid adopting of such an instrument, it was by the adoption of a code of conduct that the ILO could quickly and effectively join the growing international conversation on data protection.[687] The Code underlined the importance of the sectoral regulation of data processing in the employment context and regulated the most important rules, definitions and principles regarding the processing of personal data and employee monitoring.[688]

---

their fundamental right to determine who may use which data for what purposes and under what conditions." (*Protection of workers' personal data. An ILO code of practice*. International Labour Office, Geneva, 1997. p. 1.). The CoE in Recommendation No. (89) 2, – similarly to an almost identical phrasing in recommendation (2015)5 – stated that "*[…] the use of automatic data processing methods by employers should be guided by principles which are designed to minimise any risks which such methods could possibly pose for the rights and fundamental freedoms of employees, in particular their right to privacy[.]*" [*Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*, 1989, Preamble] A similar formulation also appeared in the EU's *Second stage consultation of social partners on the protection of workers' personal data*. The document noted that studies were prepared with the aim of assessing whether existing regulations "*[…] provide appropriate protection of workers' fundamental rights and freedoms, and in particular the right to privacy or whether there is a need to further particularise and complement them, with regard to the particular context of the processing: the employment context.*" (European Commission 2004. p. 4.) The exception might be the ECtHR's case law, which approaches the question of employee monitoring from a more privacy related perspective, based on the right to respect for private life guaranteed by Article 8.

684 CoE: *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, 2015 and WP29: Opinion 2/2017*

685 *Protection of workers' personal data. An ILO code of practice*. International Labour Office, Geneva, 1997

686 *Spiros Simitis* explained this by pointing out that by choosing the form of a code of practice, the ILO gave up on adopting a document with binding force, but in exchange it did not have to make compromises regarding the content. As a result, compared to other international documents in the field, this Code succeeded in regulating the question of employee monitoring in a more detailed way. Simitis 1998. pp. 362–363.

687 Simitis 1999. p. 50.

688 For example: the Code applies to both the public and the private sector and both to manual and automated processing of employees' (and job candidates') personal data. (Article 4.) As concerns the purpose limitation principle, the Code clarifies with regard to employment that processing can only be conducted for reasons directly relevant to the employment of the worker. (Article 5. 1.) The Code expressly states that "*[w]orkers may not waive their privacy rights[,]*" (Article 5. 13.) meaning that consent cannot be considered as a legal

Since the adoption of the code of practice, the ILO did not adopt a document explicitly aiming employee privacy.[689] What it did was contributing to the professional development of judges and staff, by organizing meetings in order to provide a platform for exchange relating to common challenges.[690] Notably, the *Meeting of European Labour Court Judges* should be mentioned, which at its 17th meeting examined the question of privacy, where participating countries all noted in their national reports that, providing certain safeguards are respected, it is possible to interfere with employees' privacy.[691] The 22nd meeting addressed the question of the impact of information communication technologies on the world of work. National reports by the 11 participating countries were issued, covering the fields of both individual and collective labour law, and addressing subjects such as the use of ICT in the hiring process, during employment, ICT activity and termination of employment, etc.[692]

As both France and Hungary are members of the *CoE* and the *EU*, emphasis will be put on these two international organizations. These organizations addressed the question of privacy and/or data protection with special regard to employment on several forums, making it a very important subject. In the following parts *(A)* the CoE's and *(B)* the EU's relevant regulation will be discussed in detail, presenting the European rules on employee monitoring and privacy.

(A) Council of Europe

Just like the ILO, the CoE has also recognized the importance of data processing in the employment context. For decades now, the ECHR's Article 8 has had great significance: *(a)* the ECtHR developed a very important case law regarding the field of workplace privacy (data protection), also dealing explicitly with the question of employee monitoring. The Committee of Ministers also adopted certain documents, explicitly addressing the question of employee data protection – which will be dealt with under section *(b)*. This led to the adoption of sectoral regulation addressing explicitly the issue of the processing of personal data related to employees. Finally, although up to now they do not have a key role regarding employee privacy and data protection, *(c)* the (Revised) European Social Charter and the European Committee of Social Rights also have a (moderate) link to data protection.

---

ground for legitimate processing of personal data. The Code also states in Article 5.3. that when "*personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context[,]*" taking into consideration that an employment relationship is often a long-term relationship. Source: De Hert – Lammerant 2013. p. 20. See more in: Ibid. pp. 19–22.

689 Fritsch 2015. p. 156.

690 http://www.ilo.org/global/about-the-ilo/how-the-ilo-works/departments-and-offices/governance/labour-law/judges/lang--en/index.htm (Accessed: 1 May 2018)

691 XVIIth Meeting of European Labour Court Judges 2009

692 National reports. Topic 1. "Impact on Information Technologies (IT) on industrial and employment relations" – review of national case law (2014). Dublin, Ireland: XXIInd Meeting of European Labour Court Judges

(a) ECtHR case law related to workplace monitoring

When it comes to employee privacy/data protection, the *ECtHR's jurisprudence* has paramount importance, as for decades now the ECtHR has regularly had to deal with the question of employee privacy. In its jurisprudence, the ECtHR adopts a privacy approach, instead of a more technical data protection analysis, and deals with the question whether the monitoring of certain aspects of the employees' life fell under the notion of "private life" [Article 8 (1)] and whether the infringement was necessary in a democratic society [Article 8 (2)]. This Section will present the key cases relating to employee monitoring, which are important to be discussed as they designate – to a certain extent – what the limits of employees' private life are.

In the case *Niemietz v. Germany* (1992) the ECtHR applied the protection provided by Article 8 to the workplace, by stating that "*[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings[,]*"[693] and pointing out that during the working life, the greatest opportunity to establish relationship with others happens at the workplace, blurring the boundaries of personal and professional life.[694, 695] By this the ECtHR made clear that the right to respect for private life must not be interpreted narrowly, instead it covers the social aspects of one's life, even at the workplace: therefore the employer shall respect employees' privacy even at the workplace.[696]

A few years after the Niemietz case, the ECtHR had to decide in another significant employee monitoring case. In the case *Halford v. the United Kingdom* (1997) the applicant, Miss Halford worked as a police officer and brought discrimination claims against her employer for being refused a promotion and alleged that her telephone calls were intercepted in order to obtain information against her for the proceedings.[697] Miss Halford was provided two telephones: one for work purposes and one for private purposes; and received no restrictions on their use.[698] Moreover, she was told that she could use her office telephone in her sex-discrimination case.[699] As concerns the applicability of Article 8, the ECtHR stated that phone calls made from business premises (as well as from home) fall under the notion of "private life" and "correspondence" mentioned in Article 8.[700] Naturally, it does not mean that the employer cannot monitor these calls, but when conducting such a monitoring, he/she shall respect the provisions laid down in Paragraph 2 of Article 8.[701]

In the case *Copland v. the United Kingdom* (2007) the applicant, Ms. Copland, worked at a college and alleged that her phone calls, e-mails and Internet use were monitored by her employer. The ECtHR found that from its precedent case law stating that phone calls made

---

693 ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.

694 ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.

695 This is especially the case in liberal professions, where separating the two fields can be extremely challenging. Source: Lambert – Rigaux 1993. p. 478.

696 Rijckaert – Lambert 2012. p. 19.

697 ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 9–12.

698 ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 16.

699 Hendrickx 2002a. p. 54.

700 ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 44.

701 In this case the ECtHR stated the violation of Article 8 as regards calls made from the office telephone, as domestic law did not guarantee adequate protection for the applicant. However, it did not state the violation of Article 8 in relation to the calls made from the home telephone. ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 51. and par. 60.

from business premises are covered by Article 8, "*[i]t follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage*."[702] With this statement the ECtHR interpreted Article 8 in the light of the technological development,[703] and guaranteed protection against the new types of interferences.[704] The ECtHR held that the interference was not in accordance with the law, as there was no domestic law regulating the case of monitoring and stated the violation of Article 8.[705]

In the *Bărbulescu v. Romania (2017)* case, for the first time, the ECtHR had to decide in a case regarding the electronic monitoring by a *private* employer.[706] The applicant, Mr. Bărbulescu was dismissed for using the Internet and a Yahoo account, created at the initiative of the employer, for private purposes against the prohibition of the employer. The employer found this out by monitoring the use of the equipment. Although Mr. Bărbulescu was informed that the personal use of IT equipment is prohibited, he was not informed as concerns the details of the implementation of the monitoring – which turned out to have registered all the content of his communication for a certain period. Reversing the fourth section's decision from 2016,[707] the ECtHR's Grand Chamber ruled in 2017 that Article 8 was violated and the national authorities could not provide an effective protection of the applicant's right to respect for private life.[708] In accordance with the ECtHR's previous case law, the ECtHR held that the applicant's communications conducted from the workplace fell under the scope of Article 8.[709]

In accordance with the ECtHR's previous case law, the ECtHR held in the *Bărbulescu* case as well that the applicant's communications conducted from the workplace fell under the scope of Article 8.[710] In this case the ECtHR acknowledged the existence of "social private life" and ruled that "*[…] an employer's instructions cannot reduce private social life in the workplace to zero.*"[711] However, it is important to emphasize that it does not mean that employers cannot monitor the activities of employees: they can exercise discretion when it comes to determining the regulations relating to private communications at the workplace. However, they have to respect certain requirements arising from the already existing privacy and data protection regulation.[712]

In this context private social life means the possibility for the individual to develop his/her social identity,[713] and instant messaging services constitute one form of leading a private social life.[714] The ECtHR also stated that restrictions on an individual's professional life may fall within Article 8 in the case that they have "*repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others*".[715] Even

---

[702] ECtHR: *Copland v. the United Kingdom*, application no. 62617/00, 2007. par. 41.
[703] Kéfer – Cornélis 2009. p. 785.
[704] Baugard 2010. p. 37.
[705] ECtHR: *Copland v. the United Kingdom*, application no. 62617/00, 2007. par. 48–49.
[706] ECtHR, Press Unit 2017. p. 2.
[707] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2016
[708] On the details of the case see more in: Gheorghe 2017 and Rózsavölgyi 2018
[709] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 81.
[710] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 81.
[711] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 80.
[712] Kállai 2017. p. 101.
[713] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 70.
[714] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 74.
[715] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par 71.

in the workplace, respect for private life and for the privacy of correspondence continues to exist, but they may be restricted to a necessary extent.[716] Therefore the complete ban of personal communication seems to restrict the private social life of employees to an unreasonable extent.

The ECtHR elaborated in paragraph 121 of the *Bărbulescu judgement* what relevant factors should be taken into account when assessing whether the employee monitoring was lawful or not.[717] These are:

- whether the employee has been notified of the possibility of monitoring correspondence and other communications, and of how this monitoring is implemented,
- the extent of the monitoring and the degree of intrusion into the employee's privacy (e.g. whether only the flow of information was monitored or the content too, or whether the scope of monitoring was limited in time and space),
- whether the employer has legitimate reasons to justify the monitoring and the access to their content,
- whether the use of less intrusive methods would have been possible (e.g. instead of accessing the content of communication),
- the consequences of the monitoring and how the result of the monitoring will be used by the employer,
- whether the employee was provided adequate safeguards.

This case is significant because it specified the rules in relation to employee monitoring and using the obtained information in disciplinary proceedings.[718, 719] The decision did not only define the general principles to be considered during finding a balance between the two sides, but also found a reasonable balance between employees' rights and the margin of discretion available to the Member States in relation to reasonably limiting the private use of the Internet in the workplace.[720] The ECtHR laid down detailed criteria making monitoring legitimate[721] – the detailed rules applying to employee monitoring will be reviewed in Part II.

The *Libert v. France (2018)* case – relating to the storage of personal files on the employer's computer – contains some important observations, in which the ECtHR did not question the established French rules.[722] The case related to the opening of personal files stored on a professional computer. The applicant, employee of the French national railway company (SNCF), was dismissed after the seizure of his work computer revealed that he

---

716 ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par 80.

717 Costes 2017. p. 35.

718 Costes 2017. p. 35.

719 While recognizing the importance of establishing these "Bărbulescu criteria", *Jean-Pierre Marguénaud* and *Jean Mouly* also draw attention to certain uncertanties regarding the application of these criteria. Notably, they question whether they are cumulative criteria or if not, what hierarchy is between them, how they should be taken into consideration when assessing whether Article 8 of the ECHR was breached. Marguénaud – Mouly 2017. p. 1996.

720 Andriantsimbazovina 2017. p. 2. (Page number referring to the online version of the article downloaded from: https://www.lextenso.fr)

721 Colonna – Renaux-Personnic 2017. p. 2. (Page number referring to the online version of the article downloaded from: https://www.gazette-du-palais.fr)

722 Loiseau 2018. p. 11. (Page number referring to the online version of the article downloaded from: https://www.lexis360.fr); Nasom-Tissandier 2018. p. 14.

stored a considerable number of pornographic files and forged documents. The applicant argued that the employer violated Article 8, by accessing those files in his absence.

The ECtHR reminds that the employer has the right to ensure that employees use the equipment provided by him/her for executing their work in compliance with their contractual obligations and applicable regulation,[723] confirming the existence of the employer's right to monitor.[724] The employee's files identified as personal receive more protection, as according to French law they can only be opened if there is a risk or a particular event and in the presence of the employee, or if he/she has been properly notified of it – contrary to files presumed to be of professional nature.[725] The ECtHR confirmed the principle that the employee is entitled to the right to respect for private life even within the workplace, and that files obviously identified as personal, stored on the computer provided by the employer for work purposes, might pertain to the private life of the employee,[726] and confirmed that the relevant part of French law is in accordance with the ECHR.[727]

From the case law of the ECtHR several conclusions can be drawn. *First*, the ECtHR made it clear that employees are entitled to the right to privacy, and they do not cease to have this right even within the workplace. *Second*, the ECtHR interpreted the right to privacy in a flexible way, taking into account the changes that had occurred in technology and society; through interpreting correspondence in a broad way and affording protection to a wide range of communication means. *Third*, in the field of employment as well, the ECtHR went beyond a narrow interpretation of privacy limited to secrecy: it recognized the importance of workplaces in establishing and developing relationships with other human beings. *Fourth*, the ECtHR made it clear that employees' right to privacy is not an absolute right, and it can be limited if certain requirements are met. In its case law, in the *Bărbulescu* judgement the ECtHR provided detailed criteria in order to be able to trace a balance between employees' and employer's rights and clarified the most important requirements in relation to employee monitoring.[728]

(b) Recommendations of the CoE

Early in 1989 the CoE adopted a *Recommendation on the Protection of Personal Data Used for Employment Purposes*,[729] [hereinafter referred to as: Recommendation No. (89) 2] representing a shift towards sectoral regulation. Recommendation No. (89) 2 covers data processing both in the private and in the public sector.[730] *Spiros Simitis* identified five key principles of the document:[731] (1) the data should be obtained directly from the

---

723 ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 46.

724 Sipka – Zaccaria 2018. p. 47.

725 Cass. soc., 17 mai 2005, N° 03-40017

726 ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 25.

727 Porta et al. 2018. p. 17.

728 It is worth noting that in the 2018 case of *Denisov v. Ukraine* the ECtHR further specified and systematised case law relating to the private life of employees. (Sudre 2018. p. 1054.) Despite holding that in the given case no breach of Article 8 of the CEHR was established, the ECtHR recalled the criteria which must be met. (ECtHR: *Denisov v. Ukraine*, application no. 76639/11, 2018. par. 92–134.)

729 *Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*, 1989

730 Article 1 of the *Recommendation No.(89) 2*

731 Simitis 1998. pp. 361–362.

employee,[732] (2) the personal data should only be processed for the purposes of the employment relationship, (3) employees should be informed regarding the most important characteristics of the processing, (4) the employee should have a right to access, to rectification and to erasure and (5) the personal data should only be kept as long as they are needed for the purposes of the processing. In addition, the data stored should be accurate, kept up-to-date and "*represent faithfully the situation of the employee*".[733] Recommendation No. (89) 2 also contains provisions regarding the communication of data (Articles 7–8), the transborder flow of personal data (Article 9) and special categories of data (Article 10).

Since then, the changes in technology, the employers' tendency to collect personal data outside of the workplace and the appearance of processing carrying specific risks made it necessary to *revise* the existing framework on employee data protection.[734] These were the main reasons underlying the adoption of *Recommendation on the processing of personal data in the context of employment*[735] in 2015. Despite the changed context, the core values of Recommendation (89) 2 still remain valid, however, the profound changes in technology and the world of work need to be taken into consideration.[736] Similarly to the ILO's Code of Practice, these recommendations – as their denomination suggests – are also soft law instruments. It is important to state that in contrast to the previous documents, provisions related to SNSs appeared in this document.

They are discussed in one paragraph stating "*[e]mployers should refrain from requiring or asking an employee or a job applicant access to information that he or she shares with others online, notably through social networking*."[737] It is clear that the provision covers both employees and prospective employees, and prohibits the employer from accessing information shared on these platforms – unless the user decides to share it. The explanatory memorandum highlights that the employer should not use intermediaries, another name or a pseudonym in order to obtain access to personal data without the knowledge of employees or job candidates.[738] The explanatory memorandum also explicitly states that employers shall not ask for employees' or job candidates' password, in order to access content on their profiles.[739] This article can be interpreted as follows: the employer cannot access in any way content on SNSs which are not accessible to him/her (e.g. because the employee uses privacy settings.) He/she cannot ask a co-worker, create a fake profile or ask for login credentials in order to obtain access. However, this would also imply that information publicly available on these sites can be processed by the employer – naturally respecting the existing data protection requirements, such as proportionality or purpose limitation, etc.

---

[732] In addition, the data processed should also be relevant and not excessive. This requirement should be enforced also during the recruitment process. Article 4 (1)–(3) of *Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*, 1989

[733] Article 5 (2) of *Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*, 1989

[734] CoE 2015. pp. 1–2.

[735] CoE: *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 2015.

[736] Buttarelli 2010. p. 5.

[737] CoE: *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 2015. 5. 3.

[738] CoE 2015. p. 7.

[739] CoE 2015. p. 7.

(c) (Revised) European Social Charter and the European Committee of Social Rights

When it comes to the CoE and fundamental rights, the (Revised) European Social Charter (hereinafter referred to as: ESC),[740] the "Social Constitution of Europe"[741] must also be mentioned. This document guarantees the most important social and economic rights – just as the ECHR guarantees the fundamental civil and political rights. However, neither the European Social Charter, nor the Revised European Social Charter regulates expressively the right to privacy or the right to data protection.

Still, the *European Committee of Social Rights* (hereinafter referred to as: ECSR), an independent body responsible for monitoring compliance with the ESC, has already expressed itself in this field and identified legal fundaments of the right to privacy. The ECSR recognized that technological development has made it possible for employers to constantly supervise employees, blurring the boundaries of work and personal life. More severe intrusions – even after working hours and outside the workplace – have become possible.[742]

The ECSR found that Article 1:2 § of the ECS, guaranteeing the right to undertake work freely, comprises the right to privacy and acknowledges the importance of ensuring workers' right to privacy.[743] In its 2016 report, the ECSR states in a straightforward manner that Article 1:2 § concerns the right to privacy at work.[744] In its observations relating to Article 1:2 § the ECSR recognized the relevancy of protecting employees' private or personal lives against unlawful infringements. It linked the fundaments of the protection to the right to freely engage in occupation, meaning that employees remain free, which imposes a limit on employer's powers. It also evoked the principle of dignity and its relation to the right to privacy and the possible cases of infringement (such as asking certain questions from prospective employees or employees and processing personal data).[745, 746] Still, the ESC and the ECSR do not have a prominent role in ensuring employees' right to privacy and data protection in spite of their importance in the protection of employees' rights – compared to the ECtHR.

(B) European Union

Like other international organizations, the EU as well has developed certain employment specific data protection requirements in addition to the general EU data protection framework. Similarly to the CoE and the ECtHR, the EU's court's, *(a)* the *CJEU*'s relevant case law in relation to employee privacy/data protection will be addressed. Then, *(b)* the *WP29*'s and

---

740 *European Social Charter*, 1961 and *European Social Charter (revised)*, 1996

741 https://www.coe.int/en/web/european-social-charter (Accessed: 12 August 2019)

742 European Committee of Social Rights 2013. p. 26.

743 European Committee of Social Rights 2013. p. 26.

744 European Committee of Social Rights. p. 32.

745 European Committee of Social Rights 2006

746 On the possible protection provided by the ESC see more in: Perraki, Panagiota: *La protection de la vie personnelle du salarié en droit comparé et européen [étude comparative des droits français, hellénique, britannique et européen]*. Thèse en droit. Université de Strasbourg, 2013. pp. 75–79.

the *European Data Protection Supervisor*'s relevant documents will be examined as – in spite of not having binding force – they provide important guidance in specific fields as well.

(a) CJEU

From amongst the case law of the CJEU notably three cases must be mentioned, dealing with the applicability of data protection rules in the employment context: the Rechnungshof v. Österreichischer Rundfunk case, the V and European Data Protection Supervisor v. European Parliament case and the Bodil Lindquist case.

In the *Rechnungshof v. Österreichischer Rundfunk case* the CJEU had to take a stand on regarding the applicability of the DPD to the processing of information (salaries and pensions) related to civil servants.[747] In the case, the Austrian regulation required certain public bodies to communicate the salaries and pensions of civil servants to the Court of Audit, who would create an annual report and transfer them to the Parliament and later make them available to the general public.[748] The CJEU linked the applicability of the DPD to whether there was an interference with private life, and whether that interference was justified according to Article 8 of the ECHR.[749] The CJEU states that while the mere recording of data relating to the salaries by the employer does not constitute in itself interference in the private life of the employees, the communication of that data to third parties infringes the right to privacy of the employees.[750]

In the case *V and European Data Protection Supervisor v. European Parliament* the applicant contested at the European Union Civil Service Tribunal the use of a previous medical opinion – declaring her unfit for a previous position at the European Commission – which resulted in her rejection at the European Parliament. She alleged that her right to respect for private life was violated.[751] Referring to the *Rechnungshof v. Österreichischer Rundfunk* case, the CJEU ruled that the transfer of personal data constituted an interference with the right to respect for private life enshrined in Article 8 of the ECHR.[752] Although the processing of the sensitive medical data served a legitimate interest, it does not justify the transfer of medical data from one institution to another, without the consent of the data subject, and it would have been possible to achieve the legitimate objective by less interference.[753]

In the case of *Bodil Lindquist* the applicant worked at a parish, and set up web pages at home – "in order to allow parishioners preparing for their confirmation to obtain information they might need"[754] –, where she – without the knowledge or consent of her colleagues – uploaded personal data (such as hobbies, family members, phone numbers) related to them.[755] Although the case primarily concerned the applicability of the DPD in the online environment,[756] it has three potential implications for employment. First, it confirms that

---

[747] Otto 2016. p. 98.
[748] CJEU: *Joined Cases C-465/00, C-138/01 and C-139/01*, 2003. par. 2.
[749] CJEU: *Joined Cases C-465/00, C-138/01 and C-139/01*, 2003. par. 72.
[750] CJEU: *Joined Cases C-465/00, C-138/01 and C-139/01*, 2003. par. 73–74.
[751] CJEU: *Case F46/09*, 2011. par. 65.
[752] CJEU: *Case F46/09*, 2011. par. 111–112.
[753] CJEU: *Case F46/09*, 2011. par. 125.
[754] CJEU: *Case C-101/01*, 2003. par. 12.
[755] CJEU: *Case C-101/01*, 2003. par. 12–14.
[756] One of the questions referred to the CJEU for preliminary ruling was whether the exemptions provided in the DPD apply to the processing concerned. For the subject of the monograph, the household exception has

employment-related information falls under the category of personal data under the DPD.[757] Second, it questions employers' practices to publish personal data on company websites. Third, it provides no possibility to bypass the DPD by employers, as employees' activities are also covered (for example, he/she cannot ask an intern to process employees' personal data in order to be qualified non-profitable).[758]

The above cases show that several acts might constitute an interference in the employees' private life and infringe his/her right to data protection. However, – in contrast to the ECtHR's jurisprudence – these cases are more remote from employee monitoring, they rather concern whether there was an interference and are more concentrated on data processing. For this reason, it is necessary to further examine the specific matter of employee monitoring – which was explicitly addressed by the WP29.

(b) The Article 29 Data Protection Working Party and the European Data Protection Supervisor

In its documents the WP29 basically translated the general provisions set in the DPD to the special context of employment, offering concrete solutions in the field of data protection and employee monitoring.[759] They did not have legally binding force, however, partly due to the WP29 being composed of representatives from each national data protection authority (hereinafter referred to as: DPA), they provided useful guidance for Member States, and national data protection authorities took these opinions into consideration when it came to the enforcement of the national data protection rules.[760] As such, the findings made by the WP29 have importance for France and for Hungary as well, as national DPAs took them into account during the enforcement of national data protection regulation.[761]

Among the already regulated cases of monitoring, the monitoring of e-mail and Internet use are need to be discussed in detail, as they have the closest connection and relevancy when it comes to SNSs. The most important documents issued by the WP 29 are *Opinion 8/2001 on the processing of personal data in the employment context*,[762] *Working document on the surveillance of electronic communications in the workplace* (2002)[763] and *Opinion 2/2017 on data processing at work*,[764] which provide guidance regarding the regulation and the monitoring of employees' Internet use. In these documents the WP29 emphasized that the general data protection principles also apply to the case of processing employee

relevancy. The CJEU ruled that this exception "*[…]must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*." CJEU: *Case C-101/01*, 2003. par. 47.

757 CJEU: *Case C-101/01*, 2003. par. 24.

758 Otto 2016. p. 101.

759 Fritsch 2015. p. 155.

760 Otto 2016. p. 97. and Retzer – Lopatowska 2011. p. 2.

761 It must not be forgotten that due to the EU's data protection reform, the WP29 was replaced by the European Data Protection Board. However, at the time of closing the manuscript, the EDPB has not yet addressed any document relating to data protection in the context of employment.

762 WP29: *Opinion 8/2001 on the processing of personal data in the employment context*. 5062/01/EN/Final WP 48, 2001

763 WP29: *Working document on the surveillance of electronic communications in the workplace*. 5401/01/EN/Final WP 55, 2002

764 WP29: *Opinion 2/2017 on data processing at work.* 17/EN WP 249, 2017

data, and within this case, to employee monitoring, and provided guidance on how exactly these general provisions shall be translated into the employment context. *Opinion 8/2001* addresses the question of processing in the employment context in general, without detailing how the general rules should be applicable to specific cases of employee monitoring. The *Working document* focuses on the question of surveillance and monitoring of electronic communication, with special regard to e-mail monitoring and the monitoring of Internet access. *Opinion 2/2017 on data processing at work* complements Opinion 8/2001 and the Working document and takes into consideration the societal-technological and legal changes that occurred since and provides guidance regarding several types of processing and monitoring.

In the light of these general rules, the rules to be applied to certain types of employee monitoring are already elaborated in the "practice" of the WP29. Such monitoring includes, for example, closed-circuit television or video surveillance,[765] or the collection of location data.[766] In this part the focus will be on the WP29's documents relating to monitoring of e-mail and Internet use, followed by SNSs.

Although the principles laid down in Opinion 8/2001 are valid in the case of e-mail and Internet monitoring, it was in the 2002 Working document that the WP29 addressed in detail the question of monitoring of e-mail and Internet use at the workplace. The Working document also points out the importance of the general data protection requirements, and then addresses the question of e-mail and Internet monitoring. In its Opinion 2/2017 the WP29 takes into account the technological development that occurred since the adoption of its previous documents, while stating that the conclusions laid down in the Working Document still remain valid.[767] The Working Party emphasizes the importance of proportionality, transparency (e.g. through the way of adopting policies).[768] Under the item "*Processing operations resulting from monitoring ICT usage at the workplace*" the Opinion expressively deals with e-mail and Internet monitoring at the workplace.

As concerns *e-mail monitoring*, it might pose a challenge that two persons' personal data are processed: the recipient's and the sender's. As for the employee, information can be given easily, and as for the third parties, warnings should be included in the messages to inform them about the monitoring. Another solution might be to provide the employee with two e-mail accounts: one for professional and one for personal purposes.[769] For the personal e-mail the monitoring of its content would be possible only in very rare circumstances (e.g. in relation to criminal activities),[770] while for the monitoring of professional e-mail accounts the rules are less severe.

Still, even in these cases, the general principles (necessity, proportionality, etc.) apply,[771] and the monitoring of e-mail should first be limited to monitoring the traffic. Employees

---

765 WP29 (2004) *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*. 11750/02/EN WP 89.

766 WP29 (2005) *Working Party 29 Opinion on the use of location data with a view to providing value-added services*. 2130/05/EN WP 115 and WP29 (2011) *Opinion 13/2011 on Geolocation services on smart mobile devices*. 881/11/EN WP 185

767 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 12.

768 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 14.

769 Otto 2016. p. 105.

770 WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 21.

771 Basically, the WP29 provides an explanation of the application of these general rules to the specific context of monitoring. Source: Kambellari 2013. p. 4.

should not only be informed that a monitoring takes place, but also if there is a detected misuse, putting the emphasis on prevention, rather than detection.[772] In several cases a misuse can be detected by accessing traffic data (e.g. the participants and time of the communication), without accessing the content of the mail.[773] Access to the content of the messages should only be permitted when the legitimate purpose cannot be achieved through less intrusive means.

Regarding the monitoring of *Internet use*, the starting point is that the employer is free to decide whether he/she allows workers to use the Internet for personal purposes, and if so, to what extent. Although the employer is entitled to monitor whether employees comply with the regulation, certain restrictions must be considered. The WP29 expressed its view that instead of monitoring, the emphasis should be placed on preventing the misuse of computers.[774] This could be achieved by using programs that remind the employee of the misuse (e.g. warning windows, which pop up and alert the employee).[775, 776] This can suffice to prevent the misuse and the employee's visit to the website can be avoided. It would also be effective if the employer warned the worker of the misuse as the first step. According to the basic principles the least intrusion possible must be made, so it is advisable that the employer avoid automatic and constant monitoring.[777] It follows from the requirement of subsidiarity that monitoring might not even be necessary, as the blocking of certain websites can prevent employees from the personal use of the Internet; accent should be put on prevention, rather than detention.[778] However, already in 2002 the WP29 underlined that a complete ban on the personal use of the Internet does not seem reasonable, as it does not take into consideration how much employees use it in their everyday lives.[779] The WP29 even referred to employees' "*legitimate right to use work facilities for some private usage*".[780]

Although the question of processing of employees' personal data obtained from SNSs is not exhaustively regulated, in Opinion 2/2017, the WP29 addressed the question of SNSs in two regards: processing during the recruitment process and in-employment screenings.

Under the title "*Processing operations during the recruitment process*" the WP29 expressively refers to personal data obtained from SNSs.[781] The WP29 acknowledged the phenomenon of the growing use of SNSs, and the employer's belief according to which during the recruitment he/she is free to use these – because of the lack of using the privacy settings – publicly available personal data. The WP29 stresses that just because these data might be publicly available, it does not mean that the employer can freely process this

---

[772] Retzer – Lopatowska 2011. p. 2. and WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. pp.4–5.

[773] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. pp. 17–18.

[774] Otto 2016. p. 105. and WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 24.

[775] Retzer – Lopatowska 2011. p. 2.

[776] According to the EDPS, it is more useful to watch the indicators (for example, volume of data downloaded) than the visited websites themselves and to take further steps only when there is a strong suspicion of misuse. Source: Buttarelli 2009.

[777] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 17.

[778] WP29: *Opinion 2/2017*. p. 15.

[779] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 4.

[780] WP29: *Opinion 2/2017*. p. 14.

[781] WP29: *Opinion 2/2017*. p.11.

data for his/her own purposes. Just like in the case of processing other data, the existence of a valid legal ground (such as legitimate interest), the application of the necessity and relevancy principle is required. The employer should consider in advance whether it is a profile related to personal or business purposes. The inspection of these profiles is only permitted when it is necessary and relevant to the performance of the job that the candidate is applying for. The personal data should only be stored for a limited period (until it becomes clear that the candidate will not be employed) and it is crucial that candidates are informed of the processing. If the employee used the privacy settings, and therefore the employer cannot access the profile, he/she cannot ask the prospective employee to friend him/her or gain access to the profile through another way.[782]

The WP29 also refers to the issue of *in-employment screening* (as from a technological point of view the employer is able to continuously screen and gain information relating to the personal lives, opinions, beliefs, etc. of employees by inspecting their social network profiles). The body states that such a screening should not take place on a generalized basis and should be limited in scope. Also, if an employee limits the access to his/her profile, the employer should not gain access to it. If in the limited cases when the employee is required to use a social network profile created by the employer (e.g. spokesperson), the employee should retain the possibility – specified in the terms and conditions of the employment contract – of having a non-work related profile that he/she can use.[783]

The significance of the above documents is to be found in concretizing the abstract data protection rules to the context of modern-day employment and, despite the lack of their binding force, they provide useful guidance when it comes to employee monitoring and data protection. Therefore, they provide guidance not only to Member States and legislators, but also to employers who process employees' personal data or conduct some kind of monitoring.

The *European Data Protection Supervisor* (hereinafter referred to as: EDPS) was established by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.[784] The EDPS is an independent supervisory authority, responsible for monitoring whether EU institutions and bodies respect rules regulating the processing of personal data, and give advice to them and to data subjects regarding data protection.[785]

As concerns processing in the employment context, the EDPS's guidelines should be mentioned. Even though these documents relate to processing conducted by EU institutions and bodies, the EDPS itself stated that it does not mean that these documents are only useful for them, as Regulation 45/2001[786] is similar to the DPD and the GDPR in many regards.[787]

---

[782] WP29: *Opinion 2/2017*. p.11.

[783] WP29: *Opinion 2/2017*. p.12.

[784] Paragraph 1 of Article 41 of *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*

[785] Paragraph 2 of Article 41 of Regulation (EC) No 45/2001

[786] Which was replaced by Regulation *(EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*

[787] European Data Protection Supervisor 2016. p. 3.; European Data Protection Supervisor 2015. p. 1.

The EDPS adopted guidelines – amongst others – on the electronic communication,[788] on the use of mobile devices,[789] on camera surveillance,[790] on the processing of health data[791] and on processing related to recruitment.[792]

In conclusion, the adoption of international regulations and the relevant cases in the field of employee data protection and monitoring demonstrates the importance of this specific subject. As it was seen, the question of employee monitoring and data protection is not new, as the first relevant documents date back to decades. In consequence, early documents did not address the challenges raised by SNSs. What is more precisely elaborated by them and also has a direct connection to the main subject of the research is the monitoring of e-mail and Internet use, in that respect that SNSs are also web-based services and also allow the user to communicate. As SNSs have a growing importance, the most recent documents already address them explicitly. However, they only deal with one aspect of the subject (notably pre-employment) – the exhaustive regulation of SNSs in the field of employment is yet to be elaborated.

The rules established by the above-examined international institutions and bodies provide the Member States with an important guidance, which can therefore have an important impact on national legal systems. The following Paragraph will explore how France and Hungary have decided to regulate the question of employee privacy and data protection in their respective legislations.

§2. Workplace privacy/data protection in France and in Hungary

Similarly to the international regulations presented above, employment specific rules appeared in Member States' legal orders as well. On the following pages it is going to be examined, as opposed to the already discussed employer's rights/powers, how the protection of employees' rights appears in national legal systems. These (labour law) rules constitute the conceptual fundaments of protecting employees' rights. The exact rules of monitoring employing a given technology are deducted from these general rules. Both the FLC and the HLC contain a general clause declaring the protection of employees' rights (which rights include, for example, the right to privacy and the right to data protection). Also, both labour codes contain certain provisions providing more detailed principles for data processing.

From this background it was already elaborated how these general requirements must be applied to existing forms of employee monitoring. In France, notably the courts and the CNIL, while in Hungary the doctrine and the NAIH (and the former Data Protection

---

[788] European Data Protection Supervisor 2015

[789] EDPS: *Guidelines on the protection of personal data in mobile devices used by European institutions*. 2015. Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-17_Mobile_devices_EN.pdf (Accessed: 12 August 2019)

[790] EDPS: *The EDPS video-surveillance guidelines*. 2010. Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf (Accessed: 12 December 2016)

[791] EDPS: *Guidelines concerning the processing of health data in the workplace by Community institutions and bodies*. 2009. Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf (Accessed: 12 December 2016)

[792] EDPS: *Guidelines concerning the processing operations in the field of staff recruitment*. 2008. Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/08-10-10_Guidelines_staff_recruitment_EN.pdf (Accessed: 12 December 2016)

Commissioner) have already worked out how they should be applied to specific types of monitoring. Therefore, the rules relating to the areas of telephone monitoring, CCTV monitoring, geolocalisation, the use of electronic badges, etc. are already elaborated.[793, 794] The monitoring of the use of work computers, Internet and e-mail will be further addressed in detail in Part II. as they have a closer connection to SNSs compared to the other forms of monitoring. It will be Part II. which will address in detail how these general rules are to be applied to the case of SNSs – the present sections will provide the conceptual background for that analysis.

Besides these already regulated, "traditional" forms of employee monitoring, several other matters have also been regulated, which gain a new light in the SNS era. These matters are subjected to detailed existing regulation – which will be analysed in Part II. For example, in the field of *dismissals*, the protection of private life must be ensured: in French law the starting point is that dismissal cannot be based on an element pertaining to the personal life of the employee. The HLC ensures the same principle through stating that as a main rule, an employee may be dismissed only for reasons in connection with his/her behaviour in relation to the employment relationship, with his/her ability or in connection with the employer's operations.[795] Or in the field of *employees' freedom of expression* – again, to be addressed in detail in Part II. – the already elaborated rules are considerably challenged by SNSs, giving rise to a multitude of questions to be answered. The following sections will focus on the more general rules of privacy and data protection, leaving the discussion of the more specific rules to Part II.

(A) Protecting employees' rights in the labour codes

Both the FLC and the HLC declare the protection of employees' rights. The key provision enouncing this protection is Article L1121-1 of the FLC, regulating the limitation of the rights and individual liberties of the individual. The HLC contains a similar paragraph: Section 9 proclaims the protection of personality rights. These two provisions constitute the cornerstone of protecting employees' rights.

(a) Article L1121-1 of the French Labour Code

Besides accepting the co-existence of the personal sphere and the professional sphere, employees' rights in general have seen an important evolution. Before 1982 the employer had a quasi-unlimited power when it came to the drafting of internal regulations.[796] It was the State Council's *Corona decision* in 1980 that first declared the principle that provisions of the internal regulation can be annulled due to the threat they can pose to the rights of the person.[797] This principle was legitimized by Article L.122-35 of the Act of 4 August 1982

---

[793] See more in: Féral-Schuhl 2018; Waquet – Struillou – Pécaut-Rivolier 2014

[794] In general, see more on employee monitoring in Hungary in: Arany-Tóth 2016; Hajdú 2005; Szőke 2012; Szőke et al. 2012; NAIH-4001-6/2012/V. and NAIH 2016

[795] Subsection (2) of Section 66 of the HLC

[796] For example, the internal regulation of Air France stipulated that if a flight attendant gets married, the marriage will automatically result in the cessation of the functions of the employee – which provision seems unimaginable nowadays.

[797] Collomp 2010. p. 40.

(the "loi Auroux"),[798] which stated that the internal regulation "*may not limit the rights of the individual or individual or collective liberties by any restriction which is not justified by the nature of the task to be performed and proportionate to the aim sought.*" This was a first, as hitherto the idea of civil liberties entering the workplace was unknown. Also, Article L. 122-45 stated that "*[n]o employee may be punished or dismissed because of his or her origins, sex, morals, family situation, membership in an ethnic group, in nation or race, political opinions, trade union or mutual activities, religious convictions.*"

In 1990, *Gérard Lyon-Caen* was asked by the Ministry of Labour Law to prepare a report in order to find a balance between the employees' and job candidates' individual liberties and the employer's powers, in the light of the development of new technologies.[799] As a result, he drew up his famous report, entitled "*Civil liberties and employment*",[800] which is the origin of legitimizing the protection of employees' rights.[801] In his report he addressed two main subjects: hiring (what the limits of asking for information relating to job candidates are) and the evaluation of employees and the control of work (with regard to the subordination between the parties, to what extent the liberties and rights of the employee are restricted). He drew attention to the development of emerging technologies and its repercussions: the threat posed by their capacity to provide powerful means of knowledge, power and control to the employer.[802]

Originating from his report, with Article L. 120-2 of the Act of 31 December 1992[803] the legislator laid down the foundations of the protection of the employee's rights and freedoms. Its text (*Article L1121-1* of the FLC in force) reads as follows:

> *"No one may limit the rights of the individual or individual or collective liberties by any restriction which is not justified by the nature of the task to be performed and proportionate to the aim sought."*[804]

By this provision, the extent of the employer's powers – without denying their existence – was considerably narrowed. The legislator expanded the protection by replacing the previously used word "internal regulation" with the expression "no one", which includes not only the internal regulation, but also the collective agreement, the employment contract, the unilateral acts of the employer, etc.,[805] and besides the employer, social partners, too.[806]

According to *Philippe Waquet* it is not possible, nor desirable, to draft an exhaustive list of what rights and liberties the text aims to protect. Under the rights of the individual, the right to dignity and the right to equality are protected, while under individual liberties, the right to respect for private life is included.[807] The protection of the right to respect

---

[798] Loi n°82-689 du 4 août 1982 relative aux libertés des travailleurs dans l'entreprise

[799] Lyon-Caen 1992. p. 3.

[800] Lyon-Caen 1992.

[801] Lyon-Caen 2014. pp. 386–390.

[802] Lyon-Caen 1992. p. 10.

[803] Act No. 92-1446 of 31 December 1992 on employment, the development of part-time work and unemployment insurance

[804] "*Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*."

[805] Waquet 2003. pp. 101–109.

[806] Waquet 2003. pp. 86–88. Although as J*ean-Emmanuel Ray* pointed out, originally this "no one" aimed to protect only job candidates. Source: Ray 2010. p. 6.

[807] Waquet 2003. pp. 93–96.

for private life also has a connection with regulations relating to non-discrimination,[808] a founding principle for the protection of the rights of the person.[809]

Also, the text speaks about *restriction* of rights and liberties – suggesting that it is not possible to place a complete limitation on them[810] – based on two principles: the necessity principle and the principle of proportionality. The *necessity principle* means that conciliation between the employer's interests and the employee's rights must be made, and only the restriction which is indispensable for protecting the employer's legitimate interests is justified. It means that the restriction must have a defined and legitimate purpose. The *principle of proportionality* limits excessive restrictions, by demanding to compare the employer's advantage with the employee's disadvantage. If there is an available method which restricts the rights and liberties of the employee less, this method shall be used. Also, the method chosen cannot be excessive.[811]

Although today the respect of employees' personal life is an important requirement of contemporary law,[812] critical spirit should be adopted, as certain authors have raised the question of the necessity of re-examining the question from the employer's point of view. Without questioning that the employee is entitled to protection of personal life, *Lise Casaux-Labrunée* asks whether the opposite question should be asked, namely how employees can respect "business life" in the workplace. By taking advantage of the protective legal framework and the possibilities offered by modern means of communication, aren't employees bringing a bit too much of their personal life to the workplace?[813] This question is particularly pertinent in the age when employees spend a daily 1 hour 15 minutes of working time by surfing on the Internet (and in a large part on social media).[814] Also, social media introduced a new paradigm regarding extra-professional life: employees often feel free to say anything on these sites – supplying a quite rich case law of "Facebook firings" –, seriously compromising the employer's legitimate interests. These must be considered as well when determining the balance between the employer's and employees' rights.

(b) Protection of rights relating to personality in the Hungarian Labour Code

The *HLC* came into force in 2012 and it brought fundamental changes to workplace data protection.[815] Declaring the protection of personality rights is also a novelty of

---

808 Article L1132-1 of the FLC

809 Tissot 1995. p. 227.

810 Waquet 2003. p. 90.

811 Mouly 2012. p. 117. See also: Mazeaud 2014. pp. 339–340.; Peskine – Wolmark 2016. pp. 221–224.; Waquet – Struillou – Pécaut-Rivolier 2014. pp. 235–236.

812 Loiseau 2011. p. 1568.

813 Casaux-Labrunée 2012. p. 334.

814 According to a study prepared by Olfeo regarding Internet use at the workplace in 2015. https://www.euromedia.fr/public/2016/12/etude-olfeo-2016-realite-utilisation-web-au-bureau.pdf (Accessed: 20 January 2019)

815 The previous HLC (Act XXII of 1992) contained only very brief provisions regarding workplace privacy and data protection. It stated in Subsection (1) Section 77 that "*[a]n employee shall only be requested to make a statement, fill out a data sheet, or take an aptitude test which does not violate his or her personal rights and which essentially provides substantive information for the aspects of the establishment of an employment relationship[,]" and in Subsection (4) of Section 3 that "[e]mployers may only disclose facts, data and opinions concerning an employee to third persons in the cases specified by law or with the employee's consent*". Source: Balogh et al. 2012. p. 99.

the HLC in force: the previous Labour Code did not set the general protection of these rights.[816, 817] After the entering into application of the GDPR, the Hungarian legislator adopted Act XXXIV of 2019 on legislative amendments required for the implementation of the European Union's data protection reform (hereinafter referred to as: Enforcing Act) in April 2019, aiming to adapt the Hungarian legal system to the GDPR, by amending more than 80 acts. The Enforcing Act also concerned the HLC, as in accordance with Article 88 of the GDPR, specific rules were introduced. These novelties will be presented in the corresponding places.

Subsection (1) of Section 9 declares the protection of personality rights, referring explicitly to the Hungarian Civil Code,[818] resulting in the joint application of labour law and civil law provisions.[819] As Items b) and e) of Section 2:43 of the Hungarian Civil Code expressly specify the right to respect for private life and the right to data protection, these provisions are to be applied to these rights as well. Although it is regulated under a separate title, the respect of personality rights is considered to be a general requirement and belongs to the common rules of conduct of labour law.[820] Limiting employees' personality rights to a certain extent is a natural characteristic of labour law: the exact content of personality rights protection in labour law can be determined in the light of labour rights and obligations.[821]

Although according to *Subsection (3)* an employee may not waive his/her rights relating to personality in advance, it does not mean that no limitation of these rights can take place: *Subsection (2)* lays down the conditions for restricting these rights – which are very similar to those established by the FLC. This restriction has three concurrent conditions: it shall be absolutely necessary, directly related to the purpose of the employment relationship, and proportional to its objective.

A restriction is *absolutely necessary* if without it the employer would not be able to fulfil his/her obligations ensuing from the employment relationship.[822] The requirements of necessity are met if the restriction is objectively necessary. The *purpose of the employment relationship* shall be interpreted narrowly, and the restriction shall relate exclusively and directly to this purpose.[823] The purpose of the employment relationship shall be identified from the rights and obligations of the parties. In accordance with the main obligations of the parties (the employee shall work while the employer shall provide work and remuneration), the purpose of the employment relationship is employment in order to achieve the employer's legitimate economic interest. This must be interpreted narrowly and is limited by the HLC

---

816 Arany-Tóth 2008. p. 131. The lack of the general declaration of protection did not mean that no protection at all was afforded to employees: the majority of the doctrine identified within this the protection of personality among the employer's duty of care. Source: Arany-Tóth 2008. p. 131., p. 129.

817 A reference was made to them in Subsection 2 of Article 8 stating that "*[a]n employee shall not waive his/her rights in protection of his/her wages and his/her person in advance, nor shall he/she conclude an advance agreement which may prejudice his/her rights to his/her detriment.*"

818 Subsection (1) of Section 9 of the HLC: "*Unless otherwise provided for in this Act, the provisions of Sections 2:42-2:54 of Act V of 2013 of the Civil Code shall apply to the protection of the personality rights of employees and employers, with the proviso that in the application of Subsections (2) and (3) of Section 2:52 and Section 2:53 of the Civil Code the provisions of this Act relating to liability for damages shall be applicable.*"

819 Kardkovács 2016. p. 53.

820 Miholics 2015. p. 245.

821 Arany-Tóth 2008. p. 131., p. 134.

822 Kardkovács 2016. p. 52.

823 *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről*, 2011. p. 100.

and by the personality rights of the employee.[824] Regarding *proportionality*, the employer's objective and the employee's disadvantage must be balanced.[825]

In addition, Subsection 2 of Section 9 regulates the question of *informing employees* on the limitation of their personality rights. The Enforcing Act made this provision more severe, as it broadened the scope of the employer's obligation regarding his/her obligation to inform employees: the information should relate not only to the methods, conditions and length of limiting personality rights, but also to the circumstances justifying the necessity and proportionality of the limitation.[826]

(B) Data protection and employee monitoring

Besides the general declaration of the protection of rights and personality rights, both labour codes contain additional rules, expressively focusing on (certain aspects of) employee data protection. While the FLC regulates the most important rules in relation to the processing of personal information of employees and prospective employees, the HLC focuses on data protection rules, and then contains specific rules regarding employee monitoring.

(a) Principles applicable to the processing of personal information[827] *in the French Labour Code*

Besides the declaration of the general respect of rights and liberties, the FLC contains other rules relevant to the subject of the monograph. Articles L1221-6 to L1221-9 relate to recruitment, regulating what information can be asked, how it should be processed and what requirements apply to the methods of recruitment. Articles L1222-3 to L1222-4 relate to the information asked from employees, and mirrors the former provisions relating to recruitment. The requirements set towards the processing of employees' and prospective employees' personal information echo those laid down in the FDPA, such as purpose limitation, proportionality or transparency.[828] Through these principles, a more dominant data protection approach is reflected. This part will review the relevant principles: first their formulation in the FLC and then their appearance in the data protection framework.

The *principle of purpose limitation* also explicitly appears in labour law, limiting the scope of processing to matters relating to the professional life: Article L1222-2 states that information requested from an employee – regardless of its forms – shall only have the aim to assess the employee's professional competence, while Article L1221-6 states that information requested from a job candidate– regardless of its forms – shall only have the aim to assess his/her fitness for the proposed employment or his/her professional competence. The purpose shall be determined prior to the processing.[829] Although it is not expressly referred to, by stating that the aim of collecting shall relate to the professional capacities, the legislator indirectly refers to the protection of the (prospective) employees' personal life.

---

[824] Berke – Kiss 2014. p. 58.

[825] Kardkovács 2016. p. 52.

[826] Rátkai 2019.

[827] The FLC does not employ the expression personal data. Instead, it uses the expression "information relating personally to a candidate/employee" ("information concernant personnellement un candidat/un salarié").

[828] Bouchet 2004. p. 8.

[829] CNIL: *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010. p. 3.

The purpose limitation principle is also enshrined in the data protection regulation.[830] If the employer decides to monitor employees, first, he/she has to define its purpose.[831] There are several legitimate aims that can justify monitoring: to determine whether an aim is legitimate the technological context also has to be taken into consideration. Often aims such as preventing damage to goods and persons, enhancing productivity, or ensuring the security of the network are referred to.[832] Or, as a specific example, telephone monitoring might be mentioned, where listening to the phone calls of employees can be conducted for the purpose of training or evaluating employees, ameliorating the quality of the service or to provide proof in certain limited cases.[833]

Besides its general formulation in Article L1121-1, the *principle of proportionality* requires that the information requested from job candidates or from employees shall have a direct and necessary link with the aimed purpose, and candidates and employees shall reply in good faith.[834] Article L1222-3 adds that means and techniques of evaluation shall be relevant in regards of the purpose. The CNIL stated that as a main rule, during recruitment it is not compatible with these provisions to collect personal data relating to nationality, social security number, housing conditions, information concerning family members, etc.[835]

This principle requires that personal data shall be adequate, relevant and do not exceed the purpose for which they are processed.[836] This principle provides that no intrusive monitoring shall take place, only the strict minimum of data shall be processed. When assessing the principle of proportionality, the given circumstances of the case shall be taken into consideration.[837] For example, the use of permanent videosurveillance[838] or the systematic search of employees' bags[839] was considered to be disproportionate. The same is true for the use of keylogger programs: the CNIL stated that as they can constantly and permanently record every keystroke, they pose an unproportionate threat to employees' rights and their use is allowed only in very strict cases.[840]

The general principle of *transparency* (and the employer's obligation to inform employees of the processing of personal data) appears in the FLC, both in regards of employees and candidates. It holds that no information relating personally to an employee/candidate can be collected through a measure that has not been brought to his/her attention (Article L1222-4 and Article L1221-9) and employees/candidates shall be explicitly informed of methods and techniques used for professional evaluation/recruitment, prior to their application (Article L1222-3 and Article L1221-8).

This is closely related to the *principle of fairness* ("principe de loyauté" enshrined also in Paragraph 1 of Article 4 of the FDPA), prohibiting the collection of personal data by all fraudulent, unfair or unlawful means.[841] The Court of Cassation ruled already in 1991

---

[830] Item b) of Paragraph 1 of Article 5 of the GDPR, Paragraph 2 of Article 4 of the FDPA
[831] Wolton – Pompey 2013. p. 218.
[832] Wolton – Pompey 2013. p. 218.
[833] CNIL: *L'écoute et l'enregistrement des appels*. Fiches pratiques: Travail & données personnelles, 2018
[834] Article L1222-2 and Article L1221-6 of the FLC
[835] CNIL: *Délibération n°02-017* du 21 mars 2002
[836] Item c) of Paragraph 1 of Article 5 of the GDPR, Paragraph 3 of Article 4 of the FDPA
[837] Wolton – Pompey 2013. p. 219.
[838] CNIL: *Délibération n°2012-475* du 3 janvier 2013
[839] CA Rennes 6 février 2003 n°02-2859
[840] http://www.cil.cnrs.fr/CIL/spip.php?article1954 (Accessed: 1 October 2018)
[841] Benalcázar 2003. p. 35.

that although the employer has the right to control and monitor the activity of employees during working hours, any recording of their image or words, for any reason, without their knowledge, will constitute illegal proof.[842] It means that no secret monitoring is allowed,[843] which was also confirmed by the Court of Cassation, who stated in a case relating to the monitoring of telephone calls that "*the employer has the right to control and to monitor employees' activities during working hours, only the use of covert monitoring is unlawful*."[844, 845]

Besides informing the employees individually, *collective transparency* is also required: the social and economic committee shall be informed prior to the application (and all modifications) of methods or techniques used for recruitment and of automated processing in the field of HR management and they shall be informed and consulted before deciding of the adoption of means or techniques allowing to monitor employees' activities.[846] Regulating questions relating to the work discipline in the internal regulation[847] are also subject to certain conditions such as submission for the opinion of the social and economic committee, communication to the labour inspector, labour courts and persons accessing the workplace, or administrative and judicial control.[848]

In order to ensure the enforcement of the rights of the individuals, the FLC also contains a provision on *whistleblowing* (Article L2313-2): if staff representatives notice that there exists a threat to the rights of individuals, to physical and mental health or to individual liberties, which is not justified by the nature of the task to be performed and is not proportionate to the aim sought, they have to contact the employer immediately. The employer has to investigate the case and remedy the situation by taking the necessary measures. If the employer does not act, or there are different opinions regarding the veracity of the threat and there is no solution found, the matter is taken to the labour court.

(b) Data processing and employee monitoring in the Hungarian Labour Code

In 2019 the Enforcing Act introduced some important changes in the field of data protection, considerably increasing the number of provisions dealing with this matter. Now these matters

---

842 Cass. soc., 20 novembre 1991, N° 88-43120

843 For example, hiring a private detective (Cass. soc., 22 mai 1995, N° 93-44078) or the use of letter bombs at the post in response to the high number of letters opened by the employees without their knowledge (Cass. soc., 4 juillet 2012, N° 11-30266) is considered to be an unlawful means of collecting evidence.

844 Cass. soc., 14 mars 2000, N° 98-42090

845 Naturally, even without prior information of employees, their simple surveillance by their supervisors (Cass. soc., 26 avr. 2006, n° 04-43.582) and, even in the absence of prior consultation, the simple surveillance by the employer or in-house service entrusted with this task (Cass. soc., 4 juillet 2012 N° de pourvoi: 11-14241) will not be considered unlawful.
However, in a case relating to the personal use of telephone, the Court of Cassation ruled that the simple verification of the length, cost or the phone numbers of the calls made from work phones is not considered to be illegal monitoring just because it was not previously brought to the attention of the employer. (Source: Cass. soc., 29 janvier 2008, N° 06-45279). *Grynbaum [et al.*] are of the opinion that this decision was due to the circumstances of the case, and this principle should not be extended to other types of employee monitoring (e.g.: Internet). Source: Grynbaum – Le Goffic – Morlet-Haïdara 2014. p. 895.

846 Article L2312-38 of the FLC

847 Or in-service notes or in any other document containing general and permanent obligations. (Article L1321-5 of the FLC)

848 Article L1321-1 of the FLC; Article L1321-4 of the FLC; from Article L1322-1 to Article L1322-3 of the FLC; Article L1322-4 of the FLC; Article R1321-2 of the FLC; Article R1322-1 of the FLC

are regulated under a separate title ("Title 5/A: Data processing") containing three Sections: *Section 10* regulating employee statements, disclosure of information and aptitude tests, *Section 11* on the processing of sensitive data (biometric and criminal personal data) and *Section 11/A* relating to employee monitoring. Section 10 and Section 11/A existed before the amendment as well, although the Enforcing Act modified them and enlarged them with additional rules. Section 11 on sensitive data is completely new. Also, its analysis will not be part of the monograph as it does not relate to the main subject of it, since there are no biometric data or criminal personal data on SNSs.

Section 10 regulates the question of data protection, through regulating disclosure of information and aptitude tests. As regards *employee statements and disclosure of information*, it declares that "*[a] worker may be requested to make a statement or to disclose certain information only if deemed necessary for the conclusion, fulfilment or termination of the employment relationship or for the enforcement of the need ensuing from this act*."[849] In data protection terminology, the latter condition is asserted by the purpose limitation principle, by requiring that personal data can only be processed if without processing the conclusion, fulfilment or termination of employment would not be possible,[850] only to the extent that is essential to achieve those purposes.[851] In the employment context processing can have numerous purposes, such as the administration of working time, ensuring workplace safety requirements or exercising the employer's right to monitor, choosing the best job candidate, etc.[852]

Regarding *aptitude tests*, the HLC contains two restrictions: it states that only an employment regulation can prescribe an aptitude test, or the test shall be necessary in order to exercise rights and to fulfil obligations in accordance with employment regulations.[853] Employers often use different tests in order to assess employees' or prospective employees' competences or personality traits. Such tests might reveal sensitive traits of the individual; therefore, it is crucial that the individual's rights are ensured during their application.[854]

As a new provision, Subsection 2 of Section 10 of the HLC also states that the employer, trade unions and works councils can demand the employee to give a statement or disclose information in order to exercise their rights or comply with their duties in the field of labour relations.[855] Subsection 3 regulates the presentation of documents – however, this matter does not have direct relevance to the subject of SNSs. As it was already mentioned, the same is valid for Section 11 regulating the processing of certain sensitive data.

Section 11/A regulates data processing resulting from the employer's right to monitoring and contains rules regulating the monitoring of electronic devices used by the employee. Subsection 1 declares employees' behaviour can be monitored to the extent pertaining to the employment relationship and the employer can employ technical means to conduct such a monitoring.

It follows from the employer's right to monitor that he/she has the right (it is even an obligation) to monitor whether employees are following the orders as the employer has not

---

[849] Subsection (1) of Section 10 of the HLC
[850] Péterfalvi 2012. p. 292.
[851] Péterfalvi 2012. p. 293.
[852] Arany-Tóth 2016. p. 29.
[853] Subsection (1) of Section 10 of the HLC
[854] Berke – Kiss 2014. p. 61.
[855] Rátkai 2019

only a right, but also an obligation to ensure the order and discipline within the workplace.[856] Prior to the Enforcing Act, the HLC contained three restrictions as regards employee monitoring: the monitoring could not go beyond the extent pertaining to the employment relationship, it could not infringe human dignity and the private life of employees could not be monitored.[857] The latter two conditions were removed from the HLC. The legislator justified this removal by reminding that both the respect of human dignity and the prohibition of monitoring private life can be deduced from general rules, therefore repeating these requirements is not necessary.[858]

The employer's right to monitor the employees' behaviour in relation to the employment relationship is quite extensive: it can relate both to behaviour within the workplace and beyond the workplace[859] – with respect to the requirements set in the HLC. It is important that the employee does not have the right to private life only outside the workplace: they are entitled to it inside the workplace as well.[860] The behaviour is in relation to the employment if it is connected to the fulfilment of his/her obligations or to the exercise of his/her rights originating from the employment relationship.[861] Defining the scope of behaviour related to employment or the limits of the employee's private life is increasingly challenging in the social media context, for reasons already presented.

The employer is also entitled to define the aim of monitoring, the time, the methods used, etc.[862] However, he/she has to respect certain requirements. The methods applied should be suitable to achieve the purpose, namely the legitimate interests and rights that the employer aims to enforce.[863] Necessity and proportionality should apply not only to the scope of the data processed, but also to the time period of processing and to the persons having access to that data.[864] The monitoring must in every case respect employees' dignity.[865] The right to monitor shall not be exercised abusively, it shall not intend to restrict the enforcement of employees' rights, or to constitute harassment or the suppression of employees' opinion.[866]

As a completely new provision, the Enforcing Act enacted a Section to the HLC (Subsection 2 of Section 11/A) stipulating that electronic devices provided by the employer can be used exclusively for professional purposes – unless the parties agree otherwise. It is also regulated how the employer can verify such a use, through stating that when monitoring compliance, the employer can only monitor data in connection with the employment – aiming to grant protection to the private life of the employee. The latter rule is also to be applied when the employee uses his/her own device for work. These rules will be examined in detail in Part II.

The HLC specifies the employer's *obligation of information*. In consequence, the employer shall inform employees regarding the processing of employees' personal data[867]

---

856 Kardkovács 2016. p. 136.
857 Subsection (1) of Section 11 of the HLC
858 *T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról*, 2019. p. 102.
859 Cséffán 2018. p. 44.
860 NAIH 2016. p. 6.
861 Arany-Tóth 2016. p. 74.
862 Arany-Tóth 2016. p. 74.
863 NAIH 2016. p. 6.
864 NAIH 2016. p. 6.
865 NAIH 2016. p. 6.
866 Subsection (1) of Section 7 of the HLC
867 Subsection (2) of Section 10 of the HLC

and the technical means used for their surveillance.[868] The explanatory memorandum of the HLC emphasizes the importance of the obligation of information and its increased importance in a world where personal life flows into professional life and vice versa.[869]

Additional provisions require that "*[e]mployers shall consult the works council prior to passing a decision in respect of any plans for actions and adopting regulations affecting a large number of employees*."[870] The processing and protection of personal data of employees and the implementation of technical means for the surveillance of workers are among the matters concerned by the obligation of consultation.[871]

In conclusion, as a result of the above analysis, it can be concluded that the similarities between the two labour codes are that they both contain a general declaration of protecting employees' rights, followed by the enunciation of certain data protection rules. The difference between the two regulations is that while the HLC contains these rules in a unique title, the relevant provisions are to be found in a more fragmented way in the FLC. Also, while the HLC contains data processing provisions relevant in the field of employee monitoring, the FLC regulates the question in a more general way. Also, the FLC explicitly deals with job applicants' rights, while such a provision is not to found explicitly in the HLC.

In both of them these rules are quite general and do not explicitly address concrete methods of monitoring. An exception is the recently introduced provision in the HLC on the use of computer devices, declaring that unless agreed otherwise, these devices must be used exclusively for professional purposes. In any case, these constitute the rules that must be reinterpreted in the light of SNSs, which raises several questions to be addressed in detail in Part II.

---

[868] Subsection (2) of Section 11 of the HLC

[869] *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről*, 2011. pp. 102–103.

[870] Subsection (1) of Section 264 of the HLC

[871] Items c) and d) of Subsection (2) of Section 264 of the HLC

Title 2: Blurred boundaries of work and personal life in the digital age

The collision between the employer's and the employees' rights is not new. The employee's subordination is present in the employment relationship, regardless of the current technological status. Rights and obligations arising from this subordination are the same (e.g. right to give orders, to control, to monitor), but can take different shapes according to the given circumstances. These circumstances can be highly influenced by technology: physical surveillance manifested through the watching eyes of a supervisor raises different questions compared to digital surveillance monitoring every step employees make in the online world.

In Title 1 the collision between the employees' and the employer's rights was addressed, examining in detail the different rights that must be balanced against each other. However, the development of ICT exerts a fundamental effect on this collision by making the boundaries of professional and personal life increasingly blurred; new information and communications technologies had a great impact – amongst others – on the notions of working time and working place.[872, 873] Technological change is one of the several factors that can have an effect on work-life balance.[874] Determining the boundaries between personal and professional spheres is crucial, as the enforcement of the parties' rights and interests is *mainly* concentrated within the professional life for the employer and within the personal life for the employee.

Hitherto the separation of these two spheres did not pose fundamental challenges: a key observation is that formerly work and personal life could be separated (and the applicability of labour law could be determined) more easily through the assessment of place and time: the concepts of "outside" and "inside" of the workplace, as well as "before" and "after" work still existed. However, the appearance of the Internet fundamentally altered such separation.[875] The blurring of this boundary is two-way: not only work is omnipresent, but personal life is everywhere as well.[876]

As a result, the already presented collision of employees' and the employer's rights arise in a more intense form as regards SNSs. As the employer can gain unprecedented insight into the employees' private life (either through self-revelation or through the disclosure of other users), employees are increasingly interested in being able to effectively enforce and exercise their right to privacy and right to data protection. Also, as now employees are able to share various items of information that can have a connection with their employment with an extremely wide audience reaching far beyond their offline social network, employers are also increasingly interested in effectively protecting their rights, such as, for example, the right to reputation.

Title 2 will examine the existence of (mutually) blurred boundaries due to ICT and SNSs, and is based on the assumption that the issue of the enforcement of rights and interests is

---

872 Ray 2001. p. 83.

873 In addition to physical and temporal boundaries, *Wafa El Wafi* also mentions psychological boundaries as an important factor in the separation of work and private life. Source: El Wafi 2016. p. 13.

874 Wilkens et al. 2018

875 Verkindt 2010

876 Ray 2010. p. 4.

more pronounced compared to the traditional forms of monitoring. As a result, on the one hand, the employer can gain "access" to the employee's personal life to a deeper extent. On the other hand, personal life has also gained ground to an unprecedented extent within the professional sphere, making both parties increasingly interested in enforcing their rights.

First, *Chapter 1* will focus on ICT in general and will address how new technologies have blurred the boundaries of personal and professional life. Then, *Chapter 2* will focus on SNSs: first, by adopting a mainly descriptive approach, the basic functioning of these sites will be presented in order to be able to then appropriately assess the legal implications of such platforms and the questions in relation to the separation of these two spheres.

Chapter 1: Information and communication technology and blurred boundaries of work and personal life

The expansion of digital tools has fundamental effects on individuals' lives.[877] Today, due to the development of ICT, the boundaries of work and personal life are increasingly blurred: personal life flows into professional life and vice versa.[878] As SNSs are products of the information communication technologies, it is worth examining first in general how ICT affects the separation of work and personal life, before addressing the specific questions raised by SNSs.

Technology has not only blurred the lines of the physical workplace: it also blurred the lines of employment. The concept of employment itself is more and more blurred, as the employment contract is not the only way to perform work. Due to gig economy, platform economy, new forms of work have appeared (e.g. gig work, crowdworking, etc.).

Section 1: New forms of employment

In its *Digital Single Market Strategy for Europe*, the European Commission recognized that ICT, and amongst them Internet and digital technologies have a fundamental effect on the lives of individuals – including the world of work as well.[879] As a response to the changes occurring due to societal and economic factors, *Eurofound* published a report[880] in 2015 adressing new forms employment,[881] which have increased importance nowadays. The expression "new forms of employment" refers to cases when the number of employer and employee differs from the usual (the usual is considered to be 1:1), when the work is not performed on a regular basis, when it implies increased networking and cooperation between self-employed, when it is not performed from the employer's premises or when the use of ICT is strong and widespread.[882] Among these new forms of employment ICT-

[877] Ray – Bouchet 2010. p. 46.
[878] Kajtár 2015b. p. 269.
[879] European Commission 2015. p. 3.
[880] Mandl et al. 2015
[881] In the report Eurofound identified and examined nine types of "new forms of work". These are: employee sharing, job sharing, interim management, casual work, ICT-based mobile work, voucher-based work, portfolio work, crowd employment and collaborative employment.
[882] Mandl et al. 2015. pp. 4–5.

based mobile work[883] and crowdworking[884] have high relevance to the subject, as they are characterised by the use of ICT technology – being conducted anywhere and anytime, regardless of time and place.[885]

The report acknowledged the advantages of these forms of employment and identified the main challenges that they represent. With regard to privacy, in relation to the use of ICT, on the one hand it was recognized that they provide more flexibility and improve the work-life balance of employees, through enabling them to perform work when it is the most suitable for them.[886] However, on the other hand, it was also recognized that implications on the boundaries of work and private life can occur as well, manifested for example in the requirement of being always available.[887, 888]

These issues were also addressed by the European Commission's *European agenda for the collaborative economy*,[889] which notably raised the question of what effects collaborative economy[890] has on the boundaries of employment and in accordance with what criteria the existence of an employment relationship can be established.[891] The report entitled *Working anytime, anywhere: the effects on the world of work*, published jointly by the ILO and Eurofound,[892] examined the effects that the use of ICT for work purposes exercises on the world of work outside the workplace.[893] It emphasized that such work can represent advantages both for employers and employees, for example, regarding work-life balance, creating new jobs, contributing to economic growth, etc.[894] One of the main driving forces of ICT-based work is flexibility and the better work-life balance that can be constructed through it.[895] However, while ensuring flexibility, ICT can also contribute to the expansion of working hours,[896] which can have detrimental effects on the separation of work and private life, as well as on availability and on the consequences associated with it.[897] In

---

883 The report identifies ICT-based mobile work as referring to "*[…] work patterns characterised by the worker (whether employee or self-employed) operating from various possible locations outside the premises of their employer (for example, at home, at a client's premises or 'on the road'), supported by modern technologies such as laptop and tablet computers. This is different from traditional teleworking in the sense of being even less 'place-bound'*." Source: Mandl et al. 2015. p. 7.

884 The report refers to crowdworking as a not place-bound form of employment, where "*[v]irtual platforms match a large number of buyers and sellers of services or products, often with larger tasks being broken down into small jobs*." Source: Mandl et al. 2015. p. 7.

885 Mandl et al. 2015. p. 72.

886 Mandl et al. 2015. pp. 76–77.

887 Mandl et al. 2015. p. 79.

888 Since then, the report was updated in 2018. In this document problems relating to supplementary working time (e.g. working during nights or weekends) was identified as one of the most challenging aspects of ICT-based mobile work.) Source: Mandl – Biletta 2018. p. 11.

889 European Commission 2016

890 In the agenda collaborative economy is defined as "*business models where activities are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods or services often provided by private individuals*." Source: European Commission 2016. p. 3.

891 European Commission 2016. pp. 11–13.

892 Eurofound – International Labour Office 2017

893 Eurofound – International Labour Office 2017. p. 1.

894 Eurofound – International Labour Office 2017. p. 9. Moreover, the report addresses several areas where the use of ICT might have a considerable impact on working conditions. These include working time, individual and organisational performance, work–life balance and occupational health and well-being.

895 Eurofound – International Labour Office 2017. p. 9.

896 Eurofound – International Labour Office 2017. p. 21.

897 Eurofound – International Labour Office 2017. p. 23.

relation to work-life balance,[898] the report found that controversial results were observed in countries participating in the report: while certain ones stated that their work-life balance improved due to ICT, others (or even the same individuals) also reported negative effects due to the blurring of the boundaries.[899]

Working with ICT can have consequences for *occupational safety and health*.[900] The health of the employees can be detrimentally influenced not only by physical risks: working conditions, such as work intensity or work duration, also play an important role with respect to the employees' health. While having the possibility to work beyond working hours can have positive effects through increasing employees' autonomy, it can also cause detrimental health issues to employees.[901] ICT also exercise important effect on workplace safety and health, particularly by resulting in stress due to the blurred boundaries and constant availability for work.[902] According to the European Working Conditions Survey, performing work beyond the regular working hours can increase employees' autonomy, but at the same time makes employees more exposed to work-related health issues.[903]

The importance of ensuring adequate rest period is guaranteed by different international documents, such as the CFREU,[904] the CoE's Revised European Social Charter[905] or the EU's European Pillar on Social Rights.[906] Also, within the EU, notably the Working Time Directive must be mentioned, which has the aim of laying down minimum safety and health requirements for the organisation of working time.[907] However, this aim might be compromised due to the constant availability of employees and its effects on the boundaries of work and personal life, raising important questions with regard to occupational safety and health.

Technology has not only blurred the lines between professional life and personal life, but also made the boundaries of the employment relationship itself porous, challenging the concepts of wage earners, subordination, occupational safety and health etc.[908] Standard employment seems not to be the norm anymore.[909] Platform work,[910]

---

[898] Principle 9 of the European Pillar of Social Rights (2017) also determines the principle of work-life balance through declaring that "*[p]arents and people with caring responsibilities have the right to suitable leave, flexible working arrangements and access to care services. Women and men shall have equal access to special leaves of absence in order to fulfil their caring responsibilities and be encouraged to use them in a balanced way*."

[899] Eurofound – International Labour Office 2017. p. 29.

[900] In addition to its effects on employees' health, it was also observed that a better work-life balance can increase mental well-being and engagement in the job (resulting in a better workforce) and thus has advantages both for the employer and for employees. Source: Wilkens et al. 2018. p. 2.

[901] Kubicek et al. 2019. pp. 15–16.

[902] Eurofound – International Labour Office 2017. p. 36.

[903] Kubicek et al. 2019. p. 16.

[904] Article 31 on fair and just working conditions stipulates that: "*1. Every worker has the right to working conditions which respect his or her health, safety and dignity. 2. Every worker has the right to limitation of maximum working hours, to daily and weekly rest periods and to an annual period of paid leave*."

[905] See Article 3 on the right to safe and healthy working conditions

[906] Declaring workers' right to healthy, safe and well-adapted work environment.

[907] Article 1 of *Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time*

[908] Bidet – Porta 2016. p. 328.

[909] International Labour Office 2015. p. 13. and ILO 2017. p. 8.

[910] "*Platform work is an employment form in which organisations or individuals use an online platform to access other organisations or individuals to solve specific problems or to provide specific services in exchange for*

clickworking[911] and crowdworking[912] challenge the existing concepts, and at first sight they might seem to escape from the scope of the employment relationship.[913, 914] As the existence of an employment relationship does not depend on the will expressed by the parties or on the designation the parties gave to their agreement but on the conditions in which the activity is performed,[915] it must be carefully analysed whether the conditions in order to qualify as an employment relationship are met.[916]

Section 2: "ATAWAD": AnyTime, AnyWhere, AnyDevice – eroding physical boundaries of the workplace

The blurring of the boundaries between professional and personal life can be effectively described by the acronym of ATAWAD (also a registered trademark by *Xavier Dalloz* since 2002) referring to a connection possible from AnyTime, AnyWhere, AnyDevice.[917] In accordance with the three aspects included in this expression, the blurring of boundaries will be presented through these three interconnected aspects, which were all shaken by technological advances: place of work, working hours and equipment used for work. However, as a preliminary point it must be emphasized that this phenomenon is mainly relevant for employees performing office work, and especially knowledge work.[918]

---

payment." https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/platform-work (Accessed: 13 August 2019)

911 They are "*digital laborers who perform micro tasks via the platforms with the unique, main or secondary aim to receive an income or additional income*." Julien – Mazuyer 2018. pp. 195–196.

912 "*[Crowdworking] refers to a form of work done by a "crowd" via a digital intermediary based on the outsourcing of activities, with piece rate payments. It is about calling a multitude of persons to do a task, the crowdworkers offering their labour force.*" Julien – Mazuyer 2018. p. 190.

913 Julien – Mazuyer 2018. p. 191.

914 For example, in the case of platform work, at first sight it is the client who gives orders, evaluates and controls the service, fixes the price, etc. while the platform "only" ensures a place to make the deal between the parties. The worker is free to accept or decline work. However, *Mathilde Julien* and *Emmanuelle Mazuyer* argue that these are just appearances and further analysis of the real conditions of the execution of the relationship is needed in order to apprehend the true role of platforms. Source: Julien – Mazuyer 2018. p. 191.

915 Cass. soc., 17 avril 1991, 88-40.121; Cass. soc., 19 décembre 2000, 98-40.572; BH2005. 102; 7001/2005. (MK 170.) FMM-PM együttes irányelv

916 Although analysing whether these new forms of work qualify as employment or not raises several interesting questions, its analysis would be beyond the scope of the monograph, as the main subject is how (prospective) employees' right to privacy and to data protection can be protected on SNSs, and not on who is considered to be an employee.
On the boundaries of employment and on who is considered to be an employee see more in: Desbarats, Isabelle: Quel statut social pour les travailleurs des plateformes numériques ? La RSE en renfort de la loi. *Droit social*, (11), 2017. pp. 971–983.; Fabre, Alexandre – Escande-Varniol, Marie-Cécile: Le droit du travail peut-il répondre aux défis de l'ubérisation ? *Revue droit du travail Dalloz*, (3), 2017. pp. 166–174.; Kun 2018

917 https://www.definitions-marketing.com/definition/atawad/ (Accessed: 15 May 2018); http://www.e-marketing.fr/Definitions-Glossaire/ATAWAD-240581.htm (Accessed: 11 May 2018); Griguer – Schwartz 2017. p. 51.

918 Eurofound – International Labour Office 2017. p. 3. The report acknowledges that certain kinds of occupations require the physical presence at the workplace or simply do not involve the use of ICT. Source: *Ibid*. pp. 17–18.

§1. "Any time": working hours

To put it simply, earlier, *working time* was easy to determine by the place of the employee: when the employee was in the workplace, he/she had to work, but when he/she was at home (or outside the workplace) he/she was not working. However, technological developments have shaken up the world of work in this regard, too. Personal life flows into professional life, as employees do not spend their working time exclusively working. The personal use of the employer's (or their own) equipment at the expense of working time is a growing issue: it is a growing phenomenon that employees often surf the Internet or are connected to their SNS at work, at the expense of working hours.[919]

On the other hand, professional life also flows into the personal life of the employee, as in the hectic 21st century it is often an expectation towards employees to instantly answer a work e-mail, phone call, instant message – even after working hours. Today it is not uncommon that work is not finished when working hours are over: work e-mails, calls, messages can be received and sent literally any time.[920] This 24 hour connectivity poses challenges not only to the separation of work and personal life, but also to the health of employees,[921] as it can lead to permanent stress by putting the expectation on employees to be available and react rapidly, at any time.[922] With the advent of the "*Homo connectus*" and the widespread use of technology, the rethinking of work-life balance must be considered.[923, 924]

Although the question of the boundaries of work and personal life was already addressed by courts,[925] the development and widespread use of ICT raises this question with new intensity. France addressed this challenge by introducing[926] to its legislation the *right to*

---

[919] The time spent on social media during working hours can represent a considerable amount of time. According to a report prepared by Bambu by Sprout Social (US), 18 % of the surveyed spend less than 15 minutes per day on these sites, however, 20 % spend more than an hour on these sites (and 10 % amongst them spend more than 2 hours.) According to a study prepared by Olfeo, French employees surf the Internet for private purposes for 2 hours 10 minutes daily, and connecting to Facebook is one of the most popular activity. According to the results of the PAW (Privacy in the workplace) project in 2012, 39 % of the Hungarian employees participating in the survey check social networks at the workplace. Sources: https://getbambu.com/blog/data/downtime-to-work-marketing-report/ (Accessed: 20 January 2019); https://www.euromedia.fr/public/2016/12/etude-olfeo-2016-realite-utilisation-web-au-bureau.pdf (Accessed: 20 January 2019); Szőke 2012. p. 173.

[920] Ray – Bouchet 2010. p. 45.

[921] INFOREG 2017. p. 71.

[922] Mettling 2015. p. 35.

[923] Moreira 2016. pp. 6–7.

[924] However, ICT can have beneficial effects as well, as these activities might equilibrate themselves through transitioning into an implicit give-and-take: it is true that today an employee might spend a part of his/her working time buying, for example, a train ticket for the weekend, but the same employee might respond to urgent work messages on a Saturday morning. Source: Combrexelle 2010. p. 12.

[925] The Court of Cassation stated in 2001 that "*the employee is obliged neither to accept to work from home, nor to install there folders and work equipment*". In 2004 the Court of Cassation confirmed this principle by stating that "*the fact that the employee could not be reached on his personal phone outside working hours is devoid of wrongfulness*" therefore could not constitute a legitimate reason for disciplinary dismissal. (Cass. soc., 2 octobre 2001, 99-42.727 and Cass. soc., 17 février 2004, 01-45.889)

[926] However, *Clément Cailleteau* further nuanced this statement through referring to already existing appearances of this right, such as the right to rest, and was also the subject of certain initiatives of social partners. Source: Cailleteau 2018. p. 2. (Page number referring to the online version of the article downloaded from: http://www.lexbase-academie.fr.)

disconnect ("le droit à la déconnexion"),[927] which means "*the employees' right to not to be connected to a professional digital tool during periods of rest and leaves*".[928]

According to the FLC, the annual negotiation on professional equality between men and women and on quality of worklife has to address the terms of exercising the employees' right to disconnect and the measures that employers adopt regarding the use of digital tools in order to ensure the respect of working time and periods of rest and leaves and the respect of personal and family life. In the lack of an agreement, the employer shall adopt a charter addressing the question of the right to disconnect.[929] However, when it comes to implementation, the regulation is deficient: although the employer faces sanctions if he/she does not negotiate on this question as prescribed by the law, there is no sanction if these negotiations do not finish with the adoption of a charter.[930] Still, protection can arise from the employer's obligation regarding the health of employees – connected to the overwork and stress caused.[931]

The realisation of this right might take several forms, starting from the blocking of professional messaging services, through pop-up windows, to sending the messages with delay. The *Mettling report* in 2015[932] drew attention to the fact that the right to disconnect is not only a right but also an obligation, and emphasised the co-responsibility of employers and employees in this regard.[933] However, it shall not be forgotten that although the right to disconnect aims to ensure the respect of working hours, it also contributes to more flexibility and certain employees choose it on purpose to work outside working hours.[934]

§2. "Anywhere": place of work

Traditionally, the place of work and time of work were mutually connected: while the place of work implied working hours, non-working hours were automatically associated with outside of the physical workplace.[935] Especially the latter is questioned by the development of ICT and through the increase of certain atypical forms of employment, such as homework or

---

927 This right was inserted into the Labour Code by the Act No. 2016-1088 of 8 August 2016 on labour, the modernization of social dialogue and securing professional pathways (loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels). In entered into force on the 1st January 2017.

928 Definition provided by Jean-Emmanuel Ray cited in: Griguer 2017. p. 5.

929 Subparagraph 7 of Article L2242-17 of the FLC

930 Bourgeois – Touranchet – Alas-Luquetas 2017. p. 17.; Griguer – Schwartz 2017. p. 52.

931 Bourgeois – Touranchet – Alas-Luquetas 2017. p. 17.

932 The Mettling report addressed the question of the impacts of digital technology on the world of work and recognized that the digital revolution caused a change of paradigm in the world of work, affecting a wide range of its fields. (p. 5.) The report (1) identified the main impacts of digital technology and (2) the consequences that can be drawn from them and (3) proposed solutions to these new challenges. Amongst others, the report proposed the acknowledgment of the right and obligation of disconnect, but also addressed the questions of management, new forms of performing work, etc. For a summary of the report see: Reymann, Alexandre: Transformation numérique et vie au travail. *Les cahiers du DRH*, (225), 2015. pp. 61–65. and Pontif, Valérie: "Transformation numérique et vie au travail" : les pistes du rapport Mettling. *Revue droit du travail Dalloz,* (3), 2016. pp. 185–187.

933 Mettling 2015. pp. 20–21.

934 For example, it is the case when an employee deliberately chooses to work on a Sunday night in order to be able to have a calmer Monday morning at work. Loiseau 2017. p. 464.

935 Morgenroth 2016. p. 29.

telework. These atypical forms of employment are more affected as they have (completely) demolished the physical separation of work and personal life. Personal life also flows into professional life, as the use of SNSs is – from a technical point of view – not limited to outside of the workplace. As their use is not dependent on the exact geographical position of the employee (but on an Internet connection and a device), they can be accessed from anywhere, even from the workplace.

The traditional methods of employee monitoring were only capable of "keeping an eye on" employees while they were at the workplace, during working hours, whereas now, due to technological innovations, monitoring is not limited anymore to the physical workplace, it is now possible to watch employees' every step not only within the workplace, but to "follow them home" and monitor their activities outside the workplace.[936] It is enough to think of the portable devices that the employee takes outside the workplace (work computers, work cell phones, GPS systems) or of the use of SNSs, during which the employee provides insight into his/her personal life, conducted beyond the boundaries of the workplace.

§3. "Any device": equipment used for work

Before, most of the necessary *work equipment* was in the factory/office/etc. and no or very few employees possessed at home the equipment necessary for work. Today, a change can be observed regarding the use and spread of these technologies: for the first time since the industrial revolution, ICT impacts the personal lives of employees as individuals, just as much as their professional lives as employees. Moreover, employees often start to use these tools in the course of their personal lives, before entering the professional sphere.[937] Employees can bring their devices used for personal purposes (e.g. smartphone) or they can bring their devices to the workplace for the purpose of working, instead of the employer providing equipment. An example of the latter is the bring your own device (hereinafter referred to as: BYOD) phenomenon.[938] Professional devices also enter the personal sphere of the employee: employees often take home with them the devices provided by the employer (e.g. company phone, company laptop). Also, outside the workplace employees might use their personal devices for professional purposes (e.g. sending an e-mail, receiving a phone call).

Such uses might result in a complete blurring of professional and private use: employees might use their own devices for work purposes, while those possessing a company owned equipment potentially use it for private purposes (e.g. checking Facebook from the company's computer). It raises data protection questions of separating personal and professional use of the device when the employer intends to exercise his/her right to monitor. One of the most important questions arising in relation to privacy and data protection is whether/how the employer can access and control these personal devices that are also used for work or control the use of equipment provided by him/her while respecting employees' right to privacy and data protection?

---

[936] Bibby 2016. p. 2.

[937] Mettling 2015. p. 5.

[938] On the data protection requirement during the implementation of BYOD practices see more in: WP29: *Opinion 2/2017*. pp. 16–17.

To conclude, the proliferation of ICT has fundamentally altered the way individuals live their lives – including their professional lives as well. Amongst the different advantages and disadvantages in relation to ICT and the world of work, Chapter 1 focused on how ICT has contributed to the blurred boundaries of work and private life, how it challenges and blurs the previously established boundaries through breaking down physical, temporal and material separation of work and personal life – as the analysis of ATAWAD illustrated. Such a phenomenon raises important questions in relation to the monitoring or the control of employees' work, to defining working hours, to the health of employees, etc. However, besides the difficulties in separating professional and personal life, ICT can provide possibilities and facilitate performing working as well. For example, they provide more freedom to the employee and can allow performing work in a way which is more convenient to him/her: the employee can work from home, sparing hours of public transportation, or can choose his/her working hours in accordance with his/her most productive period. Employees in difficult situation (e.g. individuals with disability) might also benefit from these innovations.

As regards ICT use for work, the dichotomy between France and Hungary is not considered to be significant for the subject of the research, as its proliferation is present in both countries. Naturally, differences in the exact appearance and use of ICT might occur between these two countries, but the phenomenon in itself is present in both of them – and for the main subject the latter has particular importance, as the possible differences in their use do not change the basic characteristic of ICT in relation to blurring the boundaries of work and personal life.

Through stating that due to ICT the boundaries of professional and personal life have become increasingly blurred, the analysis in Chapter 1 set the general context necessary for the further examination of SNSs. As SNSs belong to ICT as well, the statements of Chapter 1 are adequately applicable to them as well – however, their specificities must be addressed in detail in Chapter 2.

Chapter 2: The rise of social network sites and its effects on employment

SNSs are worldwide phenomena: in 2017, 71 percent of Internet users were social network users.[939] Given their extreme popularity and their embeddedness in individuals' lives, they naturally affect employment as well. With the collision between privacy and data protection and the employer's legitimate interests at the focal point of Part I, Chapter 2 aims to examine how employees' right to privacy and data protection are affected by SNSs.

The primary objective of Chapter 2 is to examine what privacy means in the context of SNSs, and in what regards SNSs increase the blur between the boundaries of professional and private life. It was demonstrated that the right to privacy protects against interference in the private life of the individuals. *Jean-Emmanuel Ray* recalls the phenomenon of the individualisation of private life ("l'individualisation de la vie privée") referring to the thoughts of the sociologist *Daniel Cardon*, who holds that although the right to privacy is traditionally conceived as a protective right, today it is more and more conceived as

[939] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (Accessed: 20 January 2019)

an (individual) liberty, which gains incredible importance in the age of social media self-exposure.[940] Regarding privacy protection today, the traditional "protective" nature of the right to privacy (e.g. the right to be let alone) remains valid, but it has to be reconsidered and co-exist with people's interests in living in a networked society.[941]

In order to provide answers to these questions, first the conceptual foundations of SNSs should be clarified. Therefore, *first*, the main attributes of SNSs will be examined, such as their definition and functioning. *Second*, the legal implications of SNSs will be addressed, with the focus being on the right to data protection. *Third*, privacy issues will be treated, through determining, in addition to ICT in general, how SNSs affect the boundaries of privacy and the boundaries of personal and professional life.

Section 1: Conceptual foundations

In order to be able to assess the legal implications of SNSs, it is necessary to understand what SNSs are and how they function. After presenting the history and providing a definition of SNSs, their functioning will be described in detail. Naturally, the aim of Section 1 is not to provide guidance merely on how these sites work, it rather serves as a preparatory Section for addressing privacy and data protection questions: it aims to regroup the mainly descriptive presentation of the characteristics of these sites that can possibly gain importance when it comes to employees' rights. It will also contribute to better understanding the facts of the relevant cases, analysed in Part II.

§1. The rise of social network sites

The following Paragraphs will focus on *(A)* the history of SNSs, starting with the brief presentation of two basic concepts inseparable from the functioning of SNSs: Internet and Web 2.0. The topicality and significance of the subject will be illustrated through presenting how popular these services have become. After placing SNSs in this context, *(B)* it will be defined what exactly SNSs are.

(A) History of social network sites

According to the statement of *András Szekfű*, *Internet* is where computer communication on a global and universal network occurs, in a packet switched system – by the use of TCP-IP protocol – and from the beginning of the 1990s, in a graphic user interface: in the system of World Wide Web.[942] The appearance and the proliferation of the Internet have completely transformed the way people can access information. The Internet as we know today was preceded by various military researches from the 1960s. The World Wide Web was created in 1989 by *Tim Berners-Lee* in the Conseil Européen pour la Recherche Nucléaire (CERN). From 1991 the access to the network was available to basically any

[940] Ray 2015. p. 521.
[941] Bylund et al. p. 142.
[942] Szekfü 2007. p. 124.

user in education and research and from 1993 anyone could develop the network.[943] Since then, the Internet has conquered the world: while in 1995 it had 16 million users worldwide, this number increased up to 3,675 million by September 2016.[944]

In addition to the proliferation of the Internet, the appearance and widespread use of *Web 2.0* technologies must be mentioned. Compared to its predecessor, Web 1.0, Web 2.0 enables users to create and share content as opposed to the structure of the static Web 1.0.[945] Social media and SNSs are connected to Web 2.0 as users themselves fill them up with content within the limits ensured by the server host.[946] Like technological innovations in general, the Internet and Web 2.0 affect privacy and data protection, by placing the sharing of information data to their centre. As *Spiros Simitis* noted, Internet has redefined how personal data is processed; such processing is shifted to the Internet, as more and more areas of life are taking place online.[947] *Robert Sprague* also points out how the use of technology changed; today, instead of being merely a source of accessing information, the information sharing nature of the Internet is thriving.[948] The Internet goes beyond being merely a technological innovation and influences everyday life: it revolutionized the way individuals live, share, communicate and consume.[949]

Although the first SNS, SixDegrees appeared back in 1997,[950] SNSs only became truly widespread in the first decade of the 21st century. Today's most known SNSs were launched during the 2000s (for example, MySpace and LinkedIn were launched in 2003, Facebook in 2004, YouTube in 2005, Twitter in 2006, Instagram in 2010 and Snapchat in 2011), and by the 2010s they "conquered the world", the most popular of them having several millions of users worldwide.[951] Even though there exists no legal obligation to create a profile on an SNS, the importance of being present on these platforms suggests that it is questioned whether the individual has a true choice regarding engaging in such an activity – especially in certain communities, such as in schools.[952]

Employees do not make an exception from the "SNS fever": employees and prospective employees use these sites just like any other individual. Today not only students are present on these sites (who will grow up and become young employees one day), but also people of all generations are users of these sites.[953] It must also be mentioned that SNS use constitutes a "supraglobal" phenomenon: the most popular SNS platforms are available in

---

943 http://hvg.hu/tudomany/20041203interhist (Accessed: 22 September 2017); Szűts 2015. p. 28.

944 http://www.internetworldstats.com/emarketing.htm (Accessed: 16 December 2016)
Regarding users in Europe, *Viviane Reading* vice president of the EU's Commission stated that in 1995 at the time of the adoption of the DPD, less than 1% of Europeans used the Internet. European Commission 2012

945 The next step of development is the appearance of Web 3.0 (also the so-called semantic web), which is based on the semantic tagging of content, integrated and integrable data. Source: Bányai 2016. p. 11.

946 Bozarth 2010. p. 11.

947 Simitis 2010. p. 2003.

948 Sprague 2008a. p. 396.

949 Falque-Pierrotin 2012. p. 31.

950 Boyd – Ellison 2008. p. 214.

951 https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed: 4 January 2018)

952 Sífthigh 2008. p. 83.

953 On the distribution of Facebook users of different ages see these statistics of 2014: https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/(Accessed: 17 January 2017)

most countries worldwide – with very few exceptions.[954] Although labour law regulations are mainly established at the national level, the behaviour in which employees engage is "supraglobal": everywhere where employees engage in SNSs, they behave in a similar way – although differences might arise in the legal response according to the given country's labour law regulations.

In contrast to the popularity of SNSs, certain interesting observations were made in relation to the migration of users towards other platforms, and also in relation to quitting social media completely. According to a social media use forecast of *eMarketer*, teenagers and young adults will start to leave Facebook in favour of other social media sites, such as Instagram, or Snapchat.[955] *Dailymail* has also released an interesting article, describing how teenagers have got tired of social media, wishing it had never been invented and what steps they made towards decreasing their dependence on these platforms.[956] Although with the amount of users they have today it seems unlikely that SNSs will suddenly disappear from one day to another, it should be kept in mind that changes in their use (e.g. migration from one certain SNS to another one) might occur.

(B) Delimitation of social media and social network sites

Social media and social network sites are similar, but not synonymous concepts. Both of them are based on Web 2.0 and are centred around *user-created content*.[957] However, their exact delimitation might differ based on the opinion of different authors, but usually SNSs are considered to be one form of social media.[958]

When attempting to find a universal definition describing SNSs, one comes across numerous *definitions*.[959] The situation is exacerbated given that different sites can serve

---

[954] These countries include, for example, China, North-Korea and Iran. https://www.thewindowsclub.com/list-of-countries-that-have-banned-social-media-for-its-citizens (Accessed: 21 October 2019)

[955] https://www.emarketer.com/Article/Instagram-Snapchat-Adoption-Still-Surging-US-UK/1016369 (Accessed: 10 November 2017)

[956] http://www.dailymail.co.uk/news/article-4950268/Even-teenagers-growing-tired-social-media.html (Accessed: 10 November 2017)

[957] According to the OECD, user-created content is "*i) content made publicly available over the Internet, ii) which reflects a certain amount of creative effort, and iii) which is created outside of professional routines and practices*." Vickery – Wunsch-Vincent 2007. p. 9.

[958] Jue – Marr – Kassotakis 2010. p. 50.; Klausz 2016. p. 71.; Flynn 2012. p. 332.; Kaplan – Haenlein 2010. p. 62.

[959] According to the OECD, social network sites "*enable users to connect to friends and colleagues, to send mails and instant messages, to blog, to meet new people and to post personal information profiles*." Vickery – Wunsch-Vincent 2007. p. 38.
Nancy Flynn defines social networks as "*online platforms where users create profiles, post content, share information, and socialize with others*." Source: Flynn 2012. p. 332.
According to Nathalie Dreyfus, social network sites "*[…] are online communication platforms, which allow the user to join or to create a network of users who share a common interest. They stand as a website which, after a registration which is usually free and requires providing information (name, birthday, e-mail address), allows to access a platform of exchange and dialogue.*" Cited in: Costes 2011. p. 132.
After analysing the arising legal challenges and the given answers in relation to law and social network sites, Valère Ndior proposes the following legal definition, according to which "*the common essential criteria of social networks would be to constitute a web hosting platform, which act as technical intermediate in order to provide to the public, for personal or for professional reasons, means and spaces of communication or interaction with other users. The owner of the social network account act as content publisher on a profile*

different purposes. Establishing one unique definition is also made more difficult by the myriad of the existing SNSs. The thematics of these sites can vary: for example, while *Facebook*, *YouTube*, *Instagram* and *Twitter* are "general" social network sites (they are destined for everyone, without bearing special thematics), *LinkedIn* and *Viadeo* are business centered social network sites, *Academia* and *ResearchGate* are for researchers, *CouchSurfing* is for travellers, etc. National SNSs also exist, destined for people living in a given region or country, such as the late *iwiw* in Hungary, *Copains d'avant* in France, *Weibo* in China or *Mixi* in Japan.[960]

Ludovic Pailler identified two reference definitions: for US scholars it is the one defined by *danah m. boyd*[961] and *Nicole B. Ellison*, while European scholars mostly refer to the definition established by the WP29.[962] According to *danah m. boyd* and *Nicole B. Ellison*, social network sites are "*[…] web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.*"[963, 964] Based on the definitions established in the article of boyd and Ellison, *Dick Stroud* proposes to create a "checklist" with the main elements of these sites. These elements are: a) possibility to create private or public *profiles* b) identifying a *network of contacts* c) *messaging*, communicating with the contacts d) *content sharing* such as photos or videos e) *add-value content*.[965]

According to the WP29, social network services are "*[…] online communication platforms which enable individuals to join or create networks of like-minded users*."[966] The WP29 complements this definition by identifying three common characteristics of social network sites: (1) users share their data in order to create profiles or a description of themselves, (2) possibility of posting user-generated content, such as videos, photos, etc. (3) providing a list of contacts and possibility to interact with these contacts.[967] *Lamia El Badawi* also proposes to identify the common characteristics of SNSs, which are – according to my opinion – consistent with the above-presented definitions: the creation of a profile, the public exposure of contacts and the publishing of content.[968] The three characteristics – profile, content, and contacts – are common to all SNSs, although it can differ which one of them is more emphatic.[969]

However, despite the establishment of these common characteristics, the evolutive nature of SNSs should be taken into consideration. Without questioning the validity of the

---

presumed to constitute a public space, except if the owner demonstrates that the contacts who he/she approved constitute a community of interest within which the data published remains under his/her control." Source: Ndior 2015. p. 35.

960 See more on the different types of social network sites in: Ndior 2015. pp. 17–19. and Clarke 2014. p. 172.

961 *danah m. boyd* writes her name in lower case on purpose. https://www.danah.org/name.html.

962 Pailler 2012. pp. 16–17.

963 Boyd – Ellison 2008. p. 211.

964 Based on this definition, the Council of Europe states that "*[a] social networking service is a platform which enables the building of social relations among people who share interests, activities, backgrounds or real-life connections. It is a web-based service that allows individuals to create a profile, to establish a list of users with whom to share views and to develop contacts within the system*." Source: CoE 2015. par. 45.

965 Stroud 2008. p. 279.

966 WP29: *Opinion 2/2017*. p. 4.

967 WP29: *Opinion 2/2017*. p. 5.

968 El Badawi 2014. pp. 108–109.

969 Pailler 2012. p. 17.

presented "reference definitions", *Valère Ndior* suggests adding other attributes, such as its extent of openness, the ways of connecting to it and its private or institutional nature, in order to better take into consideration the evolutive and hybrid nature of these sites.[970]

Regarding the definition of social media *SocialMediaToday* evokes the definitions provided by the *Merriam-Webster dictionary*.[971] The dictionary defines social media as "*forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)*",[972] while social networking as "*the creation and maintenance of personal and business relationships especially online*".[973] According to *Andreas M. Kaplan* and *Michael Haenlein*, social media are "*[…] a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content[,]*"[974] while social network sites are "*[…] applications that enable users to connect by creating personal information profiles, inviting friends and colleagues to have access to those profiles, and sending e-mails and instant messages between each other.*"[975]

According to *Nancy Flynn*, social media refers to "*[a] category of Internet-based resources that facilitate user participation and user-generated content. Social media include but are not limited to social networking sites […], microblogging sites […], photo- and video-sharing sites […], wikis […], blogs […] and social bookmarking or news aggregation sites […].*"[976]

According to *Clara Shih* – in consistency with the above-presented definitions – the main difference between the two concepts is that while social media are content-oriented (they concentrate on the content – photos, videos, comments, etc. – the user is just a mere contributor), social network sites focus on human relationships (on profiles and relations). Of course, many social network sites also enable users to share content (e.g. likes, comments, photos or videos on Facebook), but their role is secondary, compared to relationships.[977] In contrast to social media, social network sites enable the individual to create his/her own profile, establish and develop relationship with others and to "live in the community" through the different services provided by these sites.[978] In sum, while content sharing is in the centre of social media, social network sites, as a form of social media, have a more personal character and focus on establishing and maintaining relationship between users.

To sum up, social media and SNSs are closely related: they are both web-based platforms, based on Web 2.0 technologies, where user-generated content plays a crucial role in their functioning. SNSs are often considered as a type of social media, and even overlaps can be observed.[979] For the purpose of the monograph, their greatest difference is the emphasis

---

970 Ndior 2015. p. 15.

971 http://www.socialmediatoday.com/social-business/peteschauer/2015-06-28/5-biggest-differences-between-social-media-and-social (Accessed: 22 September 2017)

972 https://www.merriam-webster.com/dictionary/social%20media (Accessed: 22 September 2017)

973 https://www.merriam-webster.com/dictionary/social%20networking (Accessed: 22 September 2017)

974 Kaplan – Haenlein 2010. p. 61.

975 Kaplan – Haenlein 2010. p. 63.

976 Flynn 2012. p. 332.

977 Shih 2011. p. 38.

978 Bányai 2016. p. 70.

979 Certain platforms can be considered social media and social network at the same time (e.g. Facebook). http://www.huffingtonpost.com/fauzia-burke/social-media-vs-social-ne_b_4017305.html%202017%2002%2027 (Accessed: 22 September 2017)

regarding their main purpose: while on social media the focus is on publishing content, social network sites have more personal characteristics and are centred around establishing and maintaining relationships.

Activities both on social media and on social network sites can conflict with the interests of the employer, for example, the employee can jeopardize the employer's reputation in a blog entry (social media) or in a post on his/her Facebook account (social network site). However, focus will be primarily put on the use of *social network sites* for the reason that, since they are centred around relationships, they are more closely connected to employees' personal lives than social media. As the presented definitions highlighted, in contrast to social media, SNSs are even more user-oriented and self-centred, therefore the employee's personal life is more fundamentally influenced by them. Still, social media will not be excluded from the discussion in cases when the publication of certain facts on social media belongs to the personal sphere of the individual.

§2. Functioning of social network sites

It is necessary to present the technical functioning of these sites in order to be able to understand what legal challenges their use can lead to in the employment relationship. In the following paragraphs, the analysis will be conducted through examining different attributes of SNSs, such as what kind of information is available, who can publish content and who can access it.

(A) What can be published?

The first matter that must be examined is the type of content that can be published on SNSs. As a preliminary point it must be noted that content shared on SNSs can either relate directly to the employment (e.g. posting an opinion about someone's supervisor) or can relate to a topic not directly relevant to the employment relationship (e.g. expressing one's political opinion).

The whole idea of SNS is based on the active participation of the user, generating content. The *form of the content* can vary according to the given SNS, as they are structured differently, putting the emphasis on certain forms of sharing content. For example, *Facebook* makes it possible to share different kinds of content, starting with status updates, comments, likes, photos, videos, events, etc. *YouTube* is a video sharing platform, while *Twitter* provides micro-blogging service. On *Instagram*, users can share pictures (and short videos).

The *subject of the content* can also vary: even though it is up to the user to decide what to share, if the SNS has a specific purpose, it is likely that the content will follow that purpose (e.g. *LinkedIn* focuses on sharing information relating to the professional life of the user, while on *Instagram* or *Facebook* the user generally shares more personal information). Typically, on these sites (usually in their profile) users share personal details, such as their name, birthday, e-mail address, workplace, university they attended, relationship status, profile pictures, etc. Besides these descriptive personal data, users can share a wide range of other type of information, such as pictures, status updates, personal entries or videos – it

completely depends on them what they are willing to share.[980] Users can also interact with others and express themselves through comments, posts or likes.

However, personal information about the users can be revealed not only by being actively engaged in SNS and explicitly sharing details of their personal lives. Besides actively publishing content, other "indirect" information created in the course of the normal use of SNSs, such as likes, contact list, events confirmed, membership in groups, etc. can reveal a lot about the individual. In sum, these sites can be extremely revealing as these data offer insight into the life of the individual, into his/her personality, beliefs, relationships, past, interests, current location or mood, etc.[981]

(B) Content relating to whom can be published?

Naturally, a central role is occupied by the users of SNSs, as they constitute the primary actors behind the functioning of SNSs. However, it must also be examined whether information relating to other users or even non-users of these sites can appear on SNSs.

As SNSs are based on the Web 2.0 technology and are centred around the individual, naturally the user himself/herself plays a central role in publishing personal information by filling out the profile, using the services or actively posting content. Nevertheless, it must not be forgotten that it is also possible to publish data relating to third parties (e.g. posting a group photo, or posting a video of someone, checking-in indicating the current location, etc.). Users can tag each other, which means that they can identify someone else in their posts. In these cases, this third party to whom the information relates is usually aware of the publication through tagging. However, it is also possible to post something without (or against) the consent of another user or even without his/her knowledge,[982] or to upload data relating not only to other users, but also to non-users of SNSs. Therefore, it is not necessarily due to the individual's carelessness if (compromising) information is shared, as information can be uploaded by a third party. In such cases the individual loses control over his/her personal data.[983]

(C) Who can access the content?

The visibility of the content depends highly on the use of privacy settings, which enable users to decide to whom they disclose their personal data. These settings can differ from site to site. The settings can either be customized, enabling the user to fine-tune them, or follow the all or nothing approach, when the user can choose between public settings and accessibility only to contacts/friends.[984] *Evan North* differentiated between public (available

---

[980] Except certain strict content that the site's algorithms try to ban, such as violence, nudity, etc.

[981] Users tend to act on these sites as if they were celebrities or public figures. Vallet 2012. p. 171.

[982] See, for example, the story of Graham Mallaghan, working at the library of University of Kent, who found out from an acquaintance that without his knowledge a Facebook group was created, named "For Those Who Hate The Little Fat Library Man" in order to insult him. The group had more than 300 hundred members. https://www.ft.com/content/f6182bc8-85e4-11dc-b00e-0000779fd2ac (Accessed: 9 November 2017)

[983] Although it is possible to report a content uploaded by another user, it does not provide perfect control, as the individual might not be instantly aware of the post or examining the report might take time.

[984] Krishnamurthy – Wills 2008. p. 38.

to the general public), semi-private (available to a certain group, such as friends or friends of friends) and private information.[985] For example, *Facebook* makes it possible to carefully tailor the privacy settings: from making every content public, to sharing them only with some chosen contacts or even with no one. It is also possible to fully customize these settings: theoretically it is possible to define different settings for every contact. *Twitter* and *Instagram* do not offer such detailed settings: either everything is public or everything is available only to friends. The significance of the accessibility of the given content will gain utmost importance when it comes to assessing the private of public nature of these sites in Part II.

However, challenges rise regarding the effective use of privacy settings. In practice, these settings can be difficult for a user to be understood and they are not always aware of the real audience of the content published. Also, service providers often change these settings. Content can even "escape" from the chosen settings, as users can control the visibility of their activity only on certain parts of the site. The privacy settings chosen by the user do not always apply, as usually it is possible to publish data outside of the user's profile. For example, generally it is possible to publish content on another user's profile – e.g. to post a picture or make a comment – and in these cases the privacy settings chosen by this user will apply.

In relation to the setting "available to friends", attention must be drawn to the fact that the concept of "friend" is elusive as in general, a user can have several hundreds of contacts (the average number of friends is 338).[986] Providing access "only" to friends can mean several hundreds of persons, while "friends of friends" can mean several thousands of users, making the given content accessible to an extremely large audience. The expression friend used in the offline world does not necessarily mean the same thing on SNSs: compared to their offline counterparts, online social networks are both vaster and present weaker ties between the individuals, as "*the threshold to qualify as friend on somebody's network is low*".[987]

Usually these "friends" are added to the contact list during years of social media use: (former) classmates from primary school, from high school or from university, colleagues from work, family members, etc. who – in the absence of the use of privacy settings – can all access the user's profile. The matter is further complicated by the fact that as SNSs are a relatively new phenomenon, clear social conventions regarding their use have not yet been established (e.g. when is it impolite to reject a friend request?).[988] Users accept friend requests even from strangers, as it was demonstrated by an experiment conducted by *Sophos*. In this experiment, 41% of the participating users accepted a friend request received from Freddy Staur, who was a profile created for a green frog.[989] However, other researches report increased consciousness from users, who are becoming more active in pruning and managing their accounts.[990]

---

[985] North 2010. p. 1288.

[986] According to Brandwatch.com, in 2016, the average (mean) number of friends was 338, while the median (midpoint) number of friends was 200. https://www.brandwatch.com/blog/47-facebook-statistics-2016/ (Accessed: 7 January 2017)

[987] Gross – Acquisti 2005. p. 73.

[988] Van Eecke – Truyens 2010. p. 536.

[989] https://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx(Accessed: 7 January 2017)

[990] Madden 2012

In the case of *Facebook*, users can post content to another user's so called "wall" or leave comments under content on his/her wall. In this case the visibility will be defined by the privacy settings chosen by the other user. It is also possible to post content in events or groups. The privacy settings of these events and groups will depend on the choice of their creator (or the administrators, if the creator has appointed one).[991] Naturally, if the user creates these platforms, it is the user who decides what privacy settings to apply; otherwise he/she will have to accept the fact that he/she cannot control to whom the content might become available.[992]

Usually, it is also possible to engage in one-to-one communication through sending a message to another user's or users' messaging inbox (e.g. *Facebook Messenger* or *Instagram Direct*). In such a case, the discussion will be available only to the participants, and non-participants cannot access it (unless they receive an invitation). Such messaging systems are very similar to e-mails.

In sum, users can share all kinds of personal data, typically relating to their private or personal life. It is also possible that third parties publish data relating to the user – excluding such content from the control of the employee. Although privacy settings can be applied in order to define which audience can have access to the content, there are two problems with these settings. First, if they follow the all-or-nothing approach, in the best-case scenario they will allow access to contacts or friends, which was proved to be an elusive concept. Second, although customizable privacy settings theoretically enable the user to share the given content with a chosen audience, in practice the mastering of such settings is difficult. In practice, users are often mistaken regarding the audience that can have access to the given content.[993] Understanding the functioning of SNSs is inevitable in order to address the arising legal challenges associated with its use. On the one hand, – as it will be discussed in Section 2 – such a use raises several questions in terms of privacy and data protection law in general. On the other hand, besides these "general" data protection issues, challenges specific to the employment relationship arise as well: as employees are among users as well, their activities on SNSs might raise specific privacy and data protection questions in relation to their employment relationship.

Section 2: Legal implications and social network sites

Even though SNSs are relatively recent, it does not mean that they exist in a juridical vacuum. Discussions regarding the existence of a separate social media law have emerged. *Daniel Solove* aptly phrased it: "*[n]ew technologies rarely give rise to questions we have never addressed before. More often they make the old questions more complex.*"[994, 995]

---

[991] On Facebook an event can be public (everyone sees it) or private (only invited guests see it), while a group can be public (everyone can see the members of the group and the posts in it), closed (the members are visible by everyone, but the posts are not) or secret (only people who have been granted access can see the members and the content).

[992] On the functioning and challenges related to social network sites – such as the content published, the elusive concept of "friends" or the use of privacy settings – see also: Vallet 2012

[993] Sprague 2011. p. 15.; Kajtár – Mestre 2016. pp. 24–25.

[994] Solove 2007. p. 105.

[995] *Bill Thompson* expresses a similar opinion stating that these new innovations of the online world do not raise fundamentally new questions compared to the physical world. Thompson 2007. pp. 222–223.

Indeed, applying existing rules – that were adopted in a different context – to these new phenomena can entail difficulties.[996] However, in the Anglo-Saxon community there is tendency to treat these problems as separate,[997] specific to social media, resulting in the creation of a "social media law".[998] In contrast to this approach, *Valère Ndior* suggests that SNSs should be attached to the already existing legal categories.[999] *George Weir*, *Fergus Toolan* and *Duncan Smeed* also argue that SNSs do not raise fundamentally new challenges but alter already existing threats.[1000] Based on the above, I hold the view that there is no need to create a new social media law for employee privacy; instead, it should be examined whether and with what alterations already existing provisions can regulate the question.[1001]

§1. Documents addressing social network sites and privacy/data protection

Despite the existence of the general data protection framework (such as the DPD or the GDPR), it is welcomed that different organs and institutions have recognized their importance and the need to address them specifically. As a result, they adopted various documents targeting especially social media and data protection law. These documents usually emphasize the topicality and the importance of the subject and raise awareness to the privacy/data protection risks they can cause. However, they do not provide an exhaustive guidance, neither are they legally binding.

Among these documents, the first was the European Union Agency for Network and Information Security's (hereinafter referred to as: ENISA) position paper, entitled *Security Issues and Recommendations for Online Social Networks* (October 2007). In this document, the ENISA recognizes the expansion of SNSs and analyses the different risks posed by them (such as for example data aggregation, secondary collection, identity theft or stalking), and the recommendations given in response to these risks, emphasizing the importance of raising awareness, reviewing the existing regulations or suggesting technical solutions.

In 2009, the WP29 adopted *Opinion 5/2009 on online social networking*.[1002] The Opinion adopts a more practical point of view through the analysis of how the main points of the DPD could be applied to SNSs (such as who the data controller is, data security measures, how data subjects could exercise their rights, what information shall be provided to them, etc.). In 2018, the WP29 expressed its full support for the investigations conducted by national DPAs, taking place to examine recent data protection scandals (e.g. Cambridge

---

[996] Costes 2011. p. 137.

[997] *Eric Goldman* describes what phases Internet (and SNS) regulation went through and what exceptions were applied to it, treating it as a new emerging field of law. https://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm (Accessed: 20 January 2019).

[998] Ndior 2015. p. 11.

[999] Ndior 2015. pp. 11–12.

[1000] Weir – Toolan – Smeed 2011. p. 38.

[1001] Besides the implications for employment and privacy and/or data protection, SNSs raise a multitude of legal questions in fields such as cyber bullying, providing proof in legal proceedings, defamation and libel, etc. For more on law and social media and/or SNSs see in: Stewart, Daxton R. (ed.): *Social media and the law: a guidebook for communication students and professionals*. Routledge, New York and London, 2013.; Lambert 2014.

[1002] WP29 (2009) *Opinion 5/2009 on online social networking*. 01189/09/EN WP 163.

Analytica) and announced the establishment of a *Social Media Working Group* to develop a long-term strategy on the issue.[1003]

In the same year, different major SNS providers signed an agreement, entitled *Safer Social Networking Principles for the EU*, in consultation with the European Commission.[1004] This agreement especially targeted the protection of young users and minors, and aims to give guidance regarding how to minimize potential harm to them by outlining different best practices.[1005] The document outlines the principles by which SNS providers should be guided as they seek to help minimize potential harm to children and young people, and recommends a range of good practice approaches which can help achieve those principles.

Another very important document is the "*Rome Memorandum*", issued by the International Working Group on Data Protection in Telecommunications[1006] (hereinafter referred to as: IWGDPT) in March 2008.[1007] In this document, the IWGDPT enumerates the change of paradigm in the sharing of personal data, both regarding its unprecedented scale and the novelty that they are published at the initiative of the user himself/herself. The Memorandum details the risks related to social network sites (such as the not forgetting nature of the Internet, the deceptive notion of "friends" and community, the possible vetting of these sites by the employer, just to mention a few examples that can have relevance in the employment context, too) and then provides guidance to regulators and to the providers of these services on how these risks could be reduced.

In October 2008, the 30th International Conference of Data Protection and Privacy Commissioners[1008] adopted the *Resolution on Privacy Protection in Social Network Services*. The Resolution briefly describes the new challenges posed by social network sites and provides recommendations not only to service providers but also to users. The recommendations destined for users include a call for increased consciousness from users (notably regarding the use of pseudonyms and considering that they might be later confronted with the shared information, for example, during a job interview) and draw attention to the importance of respecting other individuals' privacy.[1009]

In 2011, the *Council of Europe's* Parliamentary Assembly adopted a resolution on *The protection of privacy and personal data on the Internet and online media*,[1010] in

---

[1003] https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf (Accessed: 20 January 2019)

[1004] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf (Accessed: 20 January 2019)

[1005] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf (Accessed: 20 January 2019) p. 1.

[1006] The International Working Group on Data Protection in Telecommunications (also called Berlin group as the secretariat is provided by the data protection authority of Berlin) was established in 1983 at the initiative of national data protection authorities in the world. It has among its members national data protection authorities, as well as representatives from the private and NGO sectors. https://edps.europa.eu/data-protection/data-protection/glossary/b_en (Accessed: 20 January 2019). Although the IWGDPT adopts proposals and recommendations that are legally not binding, due to its composition, these documents can serve as important guideline to countries as well.

[1007] International Working Group on Data Protection in Telecommunications 2008) *Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" –* . 675.36.5. Rome

[1008] The International Conference of Data Protection and Privacy Commissioners is a global forum of data protection authorities, established in 1979, seeking to provide leadership in reaction to privacy and data protection on an international scale. The Conference is held at least once a year.

[1009] 30th International Conference of Data Protection and Privacy Commissioners 2008. p. 2.

[1010] CoE: *The protection of privacy and personal data on the Internet and online media*. Resolution 1843 (2011)

which the CoE emphasized the importance of privacy and data protection in the age of ICT developments. In 2012, the CoE adopted its *Recommendation on the Protection of Human Rights with Regard to Social Networking Services*.[1011] The Committee of Ministers emphasized the growing role of SNSs in promoting (or hindering) the exercise or enjoyment of human rights. In the Appendixes of the Recommendation attention is drawn to the importance of what measures should be taken in order to make users capable of dealing with these platforms, how children and young people can be protected and how these platforms could operate.

Regarding the *merits and shortcomings* of these international legal documents, these documents are significant in acknowledging the importance of SNSs in modern societies and in recognizing the need to provide legal regulation. They identify the possible risks and suggest different solutions to cope with them, contributing to enhancing privacy and data protection, and also to raising awareness to the issue.

Still, since these documents do not have obligatory force, their enforcement in practice might face certain difficulties. As regards our subject, another significant lack is that these documents dealt with the question of SNSs from a general point of view and did not focus specifically on employment. Despite the lack of a document exhaustively addressing employment and SNSs, it is a great achievement that the latest documents on privacy and data protection at work at least mention social network sites. Still, these documents usually contain only few provisions; they do not regulate the question exhaustively. Among these documents, the *CoE's recommendation of the Committee of Ministers to member States on the processing of personal data in the context of employment* (2015)[1012] and the *Article 29 Data Protection Working Party's opinion on data processing at work* (2017)[1013] should be mentioned. These provisions will be addressed in detail in Part II.

§2. Social network sites and data protection

Despite the fact that the general data protection regime – such as earlier the DPD and now the GDPR – is applicable to SNSs, in practice it is not always obvious how the general data protection rules laid down in different documents should be applied in the context of SNSs. These "general" questions might concern the qualification of data controllers and the application of the household exemption, as well as the lawful ground for processing.[1014] Regarding employment – among the general data protection provisions – the principles of data processing and transparency have special significance.

[1011] CoE: *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*, 2012

[1012] "5.3. Employers should refrain from requiring or asking an employee or a job applicant access to information that he or she shares with others online, notably through social networking."

[1013] See the section "5.1 Processing operations during the recruitment process".

[1014] On these questions see especially: WP29: *Opinion 5/2009*; Van Eecke – Truyens 2010.; Kosta, Eleni et al.: *Data protection issues pertaining to social networking under EU law*. Transforming Government: People, Process and Policy, 4(2), 2010. pp. 193–201.; Van Alsenoy, Brendan et al.: *Social networks and web 2.0: are users also bound by data protection regulations?* Identity in the Information Society, 2(1), 2009. pp. 65–79.; Garrie, Daniel B. et al.: *Data Protection: The Challenges Facing Social Networking*. Brigham Young University International Law & Management Review, 6(2), 2010. pp. 127–152.; Wong, Rebecca –Savirimuthu, Joseph: *All or Nothing: This is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet*. John Marshall Journal of Computer & Information Law, 25(2), 2008. pp. 241–266.

From a general data protection aspect different questions need to be answered regarding *data protection principles*. As data controllers, organizational data controllers must comply with the data protection principles. Different questions arise in relation to the principle of *proportionality* and *necessity*. First, when a user decides to register on an SNS, the question is whether the personal data that the user is obliged to provide in order to create an account are indeed necessary to use the service (e.g. being obliged to use his/her real name, or having the possibility to choose a pseudonym).[1015] As regards the storage of personal data, questions might also arise in relation to necessity and proportionality as infringements are possible. An extreme example is pointed out by *Evelyne Sørensen*, who described how Facebook users could not practice self-censorship because even if they started to type something, then decided not to post but to delete it, Facebook store that information.[1016] *Up-to-dateness* might also be questioned, as on these sites personal data back to several years can be aggregated. A solution might be to set the default settings to delete personal data published by users after a determined period (for example, 3 years), and those users who wish should take active steps and change the default settings.

Transparency is a crucial question as well. SNS operators lay down the rules and the conditions of using their services in their privacy policy in a unilateral document, the terms of which are solely defined by the site operator. The user does not have the possibility to negotiate those terms and conditions and has to accept them when registering to the service. Theoretically, users can learn more about data processing operations from these policies, in practice various difficulties arise: because of the lengthy wording, users usually do not read such policies, and even if they read them, they do not understand its provisions, and even if they understand them, they do not have the necessary background knowledge in order to make an adequate, informed decision.[1017]

Although in the above data protection principles were examined from a general angle, these issues might have relevancy in the employment context as well. Having the possibility to use these sites under a pseudonym might "break" the connection between the employee and the employer, as it would make the identification of the user more difficult to a third party (compared to cases when the employee uses his/her real name and may even identify the employer on his/her profile).[1018] Or, the aggregation of less data by default would result in employers being able to trace a limited past of the prospective employee or the employee. Privacy policies in their present form do not enable an average user to truly exercise control over his/her personal data. Informing users and raising awareness amongst them through a more appropriate, user-friendly way might enable more users to exercise their rights in a more conscious way and might contribute to their better understanding of the functioning of SNSs and the stakes relating to the processing of their personal data.

[1015] WP29: *Opinion 5/2009*. p. 11.

[1016] On this issue see more in: Sørensen, Evelyne J. B.: The post that wasn't: Facebook monitors everything users type and not publish. *Computer Law and Security Review*, 32(1), 2016. pp. 146–151.

[1017] Solove 2013. p. 1888.

[1018] Although it does not mean in any case that hiding under a pseudonym would enable employees to escape from all responsibility.

Section 3: Social network sites and blurred boundaries

In connection with the main subject, SNSs can blur two boundaries: the boundaries of privacy and the boundaries of professional and personal life. On the one hand, *(§1)* it has to be assessed whether and if yes, how SNSs can alter reasonable expectations of privacy, and whether they can influence what is considered to be covered by privacy nowadays. On the other hand, it is necessary to examine *(§2)* that in the light of how ICT contributed to blurring the boundaries between professional and personal life, what specific problems, inherent to SNSs arise in this regard.

§1. Changed expectations of privacy

Before addressing the questions of *(B)* how SNSs altered the boundaries of privacy, what privacy means in the context of SNSs, it is necessary to consider *(A)* what are the significance and the underlying reasons behind the use of SNSs and what role(s) do they play in individuals' lives?

(A) Importance of social network sites

As it was already mentioned, the popularity of SNSs is given by their capacity to fulfill three basic human needs: according to *James Grimmelmann* these needs are self-expression (identity), communication (relationships) and being part of a community. These needs constitute the basic elements of social interaction. First, through shaping their online profiles users can express their identity. Second, on SNSs users can communicate and maintain relations with others in several ways. Third, they can feel that they are part of a community and they can establish their social position within the community.[1019]

Desiring to express one's *identity* and to manage one's perceptions taken of the individual by third parties is not a novelty.[1020] On SNSs users can present an image of themselves in various forms, where each feature provided by the SNS serves as a means for self-expression, be it a (profile) picture, a caption, filters, hashtags, likes, membership in a group, etc.[1021] SNSs allow users to create a carefully shaped identity, where posts might be carefully planned, aiming to reflect the precise image that the user aims to diffuse towards his/her contacts.[1022] SNSs are centred around the individual, creating personal, or "egocentric" networks.[1023]

Leigh A. Clark and *Sherry J. Roberts* note that technology has always had a significant impact on how people *communicate* (e.g.: telegraph, telephone, Internet, etc.) and SNSs should be considered as a next step of human interaction, therefore they shall receive

---

[1019] Grimmelmann 2009. pp. 1151–1159.

[1020] Notably see *Erving Goffman*'s "impression management" describing how individuals aim to control the impressions that others might have of him/her. Goffman, Erving: *The Presentation of Self in Everyday Life*. University of Edinburgh, Social Sciences Research Centre, Edinburgh, 1956

[1021] Grimmelmann 2009. pp. 1152–1153. Creating a perfect post has become an increasingly complex, well-planned act.

[1022] https://www.nytimes.com/2006/02/19/fashion/sundaystyles/here-i-am-taking-my-own-picture.html (Accessed: 20 January 2019)

[1023] Boyd – Ellison 2008. p. 219.

adequate protection.[1024] Ways of communication naturally change over time and since the creation of the Internet, it has changed how users use it. At the beginning of the 21st century, its information-*sharing* nature started to thrive,[1025] and has not stopped since,[1026] leading to the phenomenon that it has become an integral part of everyday life: users share bits of their personal lives, be it pictures of a party, a holiday, Christmas celebration, a meal in a restaurant or drinks in a fancy bar. Today, being (actively) present on SNSs is even a societal expectation, reflected in the mantra of SNSs that if it is not posted to SNS, it did not happen.[1027]

SNSs can let users establish their social position and enable them to be recognized members of the *community*,[1028] which can manifest in several forms – either in the number of contacts, or in the number of likes received. When it comes to the reasons for using SNSs, the (informational) societal pressure is also an important factor. If everyone is present on these sites, staying out of them – in the age of information, when information is in the centre of life – can represent a serious disadvantage, as the user would not be able to use certain services and have the same possibilities as the other users.[1029] Users are bound to these services because they can only leave these sites with difficulties, because if they do so, they would leave all their friends, too.[1030] Also, being present on these platforms and keeping in touch with different contacts is crucial, as today "*[c]onnectedness is social currency*".[1031]

Besides satisfying basic human needs, the Internet and SNSs can also play an important role in promoting the *exercise of human rights*.[1032] The use of SNSs can also constitute a way of exercising fundamental rights. From a legal perspective, the *Council of Europe's Committee of Ministers* emphasized the importance of the Internet and SNSs in promoting the exercise and enjoyment of human rights and fundamental freedoms, stating that they can also enhance participation in social and political life and promote democracy and social cohesion.[1033] *Isabelle Falque-Pierrotin* also emphasized the role of the Internet in promoting the exercise of individual and public liberties – especially freedom of expression and right to information – and argued that the exercise of these rights is inseparable from the question of privacy protection.[1034] One employment specific example can be the exercise of collective labour rights, as communication on SNSs might also serve the activity of trade unions, etc.

Such an enhanced importance of these platforms can raise the question: do individuals have a *right to social media*? With respect to employees' privacy and data protection this

---

[1024] Clark – Roberts 2010. p. 508., p, 509., p. 518.

[1025] Sprague 2008a. pp. 395–396.

[1026] According to the site Brandwatch, in 2016, 6 new Facebook profiles were created in every second and the site generates 4 petabytes of data per day. Users generated 4 million likes per minute and uploaded 350 million photos per day. https://www.brandwatch.com/blog/47-facebook-statistics-2016/ (Accessed: 7 January 2017)

[1027] https://www.theguardian.com/news/2015/feb/26/pics-or-it-didnt-happen-mantra-instagram-era-facebook-twitter (Accessed: 20 January 2019)

[1028] Grimmelmann 2009. p. 1157.

[1029] Cseh 2013. p. 90.

[1030] Mendel et al. 2013. p. 38.

[1031] Grimmelmann 2009. p. 1158., pp. 1151–1159.

[1032] Hiselius 2010. p. 202.

[1033] CoE: *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*, 2012

[1034] Falque-Pierrotin 2012. pp. 34–35.

question is crucial, as it relates to whether and if yes, how employees can be told what behaviour they should adopt on these sites[1035] or whether employees can be ordered to withdraw from the use of social media. Do employees have a "right to social media" in the light of the evolutive concept of private life interpreted as being able to live one's life as one wishes and in the light of the growing role of social network sites in everyday life? The phenomenon of adopting internal social media regulations poses the question whether the employer can restrict – and if yes, to what extent –, employees' use of SNSs? Can the employer order the employee to like certain content on these sites or to friend the employer?

In France, the Constitutional Council's decision on the *Act furthering the diffusion and protection of creation on the Internet*[1036] must be mentioned, in which the Constitutional Council had to take position in a slightly similar case. The act aimed to give the administrative authority, the High Authority for the dissemination of works and the protection of rights on the Internet ("Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet", abbreviated as HADOPI) the power to impose penalties in the form of withholding access to the Internet. The Constitutional Council declared that the right to access to the Internet falls within the scope of the freedom of communication and expression.[1037] Although – in contrast to the US court – it did not acknowledge the existence of a fundamental human right to access to the Internet, it affirmed that the threats to the freedom to access the Internet are regarded as threats posed to the right to the free communication of ideas and opinions.[1038, 1039]

Considering the acknowledgement of public or social private life, the ECtHR's Niemitez decision should be mentioned although the decision did not directly relate to SNSs but to the public aspects of private life in general. Today aren't SNSs one of the principal forums

---

[1035] For example, employers sometimes ask their employees to be actively present on these sites in order to enhance the employer's e-reputation. Source: Ray 2012. p. 936.

[1036] Conseil constitutionnel: décision n° 2009-580 du 10 juin 2009

[1037] The Constitutional Council stated that the freedom of expression is one of the most important human rights, and that "*[i]n the current state of the means of communication and given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, this right implies freedom to access such services.*" Decision n° 2009-580 of June 10th 2009, par. 12.

[1038] Commentaire de la décision n° 2009-580 DC – 10 juin 2009 Loi relative à la diffusion et à la protection de la création sur internet. *Les Cahiers du Conseil Constitutionnel*, (27). Available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009580DCccc_580dc.pdf (Accessed: 6 June 2018) p. 7.

[1039] As an illustrative example a case from the US should be mentioned as it draws attention to the importance of SNSs in everyday life. In the US, in 2017 the Supreme Court of the United States ruled on the existence of the *right to social media*. In 2008 the state of North Carolina adopted a statute making it a felony for registered sex offenders to gain access – amongst others – to social media sites. The Supreme Court stated that "*[North Carolina's] statute here enacts a prohibition unprecedented in the scope of First Amendment speech it burdens. Social media allows users to gain access to information and communicate with one another about it on any subject that might come to mind. […] By prohibiting sex offenders from using those websites, North Carolina with one broad stroke bars access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge. These websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard.*" Therefore, States cannot adopt in their statutes a blanket ban on the use of these sites. Source: Supreme Court of the United States: *Lester Gerard Packingham, Petitioner v. North Carolina*, June 19, 2017

where individuals "*establish and develop relationships with other human beings*"?[1040] Does the right to informational self-determination not go beyond simply protecting privacy but aim to guarantee "*the primacy of the individual, to be able to exercise his/her freedom*"?[1041] Therefore social media raises the question to what extent employees are free to use these platforms and how their behaviour can be restricted by the employer.

Neither in France nor in Hungary is the right to social media *expressis verbis* guaranteed.[1042] However, considering the already presented role that social media plays in personal life and the rights associated with it, it can be deducted from the general rules of both labour codes, namely from the provisions regulating how employees' rights can be limited, that as social media often constitute an important tool in exercising such rights, through the protection of these rights, the use of social media is protected as well. Therefore, employers can only limit the use of SNSs if certain requirements are met – as it will be examined in detail in Part II.

In sum, the use of SNSs is more than a discretionary choice of the individual.[1043] They constitute the 21st century way to fulfil basic human needs. Although it is not obligatory to use them, they have become part of the reality of the modern world, making it hard to completely avoid using these services. Of course, according to the temperament of the given user, the extent of being a silent observer or engaging actively in their use can differ. Naturally, employees are amongst SNS users as well.

While acknowledging that the appreciation of a case depends on the exact circumstances and that the employee can face labour law consequences if he/she oversteps the limits of such a use, it should be noted that for the above reasons the behaviour of employees who engage in SNSs and share a certain amount of personal data during such a use is not automatically considered as illegitimate. However, as their intended use naturally comes with the share of personal information and personal data, the question of what is considered to be private in the context of SNSs is raised.

(B) Social network sites and the boundaries of privacy

It was already demonstrated that privacy is a flexible, ever-changing concept. Besides the individual's attitudes towards privacy, privacy law is closely connected to *technology*, technological advances might call for changes in privacy laws, too. Naturally, SNSs raise different questions than printed letter or e-mails. As *Jon L. Mills* noted, "*[a]n individual living in the 21st century does not have the same reasonable expectation of privacy as a person living in the 1700s*."[1044] *Societal norms* can also have an influence on what can be

---

[1040] ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.
According to *Alejandra Michel*, it follows from the evolutive case law of the ECtHR, which is evolving in the light of the given societal and technological innovations, that it is possible that the individual's right to "*establish and develop relationships with other human beings*" is guaranteed on SNSs as well. Michel 2016. p. 105.

[1041] Conseil d'Etat 2014. p. 268.

[1042] On the potential fundaments of a right to SNS see more in: Pailler 2012. pp. 28–46.

[1043] Del Riego – Sánchez Abril – Levin 2012. p. 23.

[1044] Mills 2015. p. 160.
He also draws attention to the fact that just because in the modern world it is easier to intrude into someone's private life, it does not mean that this intrusion should be considered acceptable and legitimate. According to

considered private, and today it is a normal part of the 21st century – especially for the younger generations – to expose one's private life in the online world.[1045] Unlike in the "pre-SNS era" – it is considered normal to share events that used to be considered private.[1046]

One of the novelties brought by SNSs is not the mere change in the reasonable expectation of privacy, but also the phenomenon that a huge amount of this private information is published at the initiative of the users themselves. As a consequence, many privacy issues are created by the users themselves,[1047] as it is the users' continuous activity that drives SNSs.[1048] As *Woodrow Hartzog* noted, in the age of Warren and Brandeis the sanctity of private life was threatened by external parties, but today the Internet user has become his/her worst enemy.[1049] It is unprecedented to observe during the history of mankind such an extensive and voluntary share of private information.

SNSs standardize and encourage the share of personal data.[1050] Privacy and data protection consequences arise from the very nature of social network sites, as their whole functioning is based on the share of personal data.[1051] Today, self-exposure is the choice of users: they decide to share all that information.[1052] These attitudes have led to the phenomenon that users from all around the globe share their personal data in a quantity and quality never seen before, "*[…] pushing at the boundaries of what societies see as a person's individual space[.]*"[1053]

William A. Herbert describes this phenomenon as electronic exhibitionism, endemic to SNSs, which means "*the increasing worldwide phenomenon of individuals eviscerating their own privacy by affirmatively or inadvertently posting and distributing private and intimate information, thoughts, activities and photographs via email, text messaging, blogs, and social networking pages.*"[1054] The expression exhibitionism has a negative connotation: one should refrain from *automatically* applying this expression to users actively engaging in SNSs.[1055] It is a natural reaction to think that these individuals have given up their privacy; however, in reality this issue is more nuanced.[1056] Even though in this scenario it is the users who decide to voluntarily share personal information, they still expect certain privacy through the limitation of the extensiveness of the exposure.[1057]

---

him, today there is danger in accepting this intrusiveness because of the possible risk of causing far-reaching consequences, namely the disappearance of our collective expectation of privacy. Mills 2015. p. 162.

[1045] Newell 2011. p. 2.

[1046] Henderson 2013. p. 4.

[1047] Qi – Edgar-Nevill 2011. p. 76.

[1048] Stroud 2008. p. 208.

[1049] Hartzog 2013. p. 54.

[1050] Qi – Edgar-Nevill 2011. p. 75.

[1051] North 2010. p. 1288.

[1052] Rey 2012. p. 197.

[1053] International Working Group on Data Protection in Telecommunications 2008. p. 1.

[1054] Herbert 2011. p. 26.

[1055] A possible clue to make a distinction between exhibitionism and the intended use of SNSs might depart from the notions of self-disclosure and self-presentation. While self-presentation is "*communication of self-data an individual might reveal to most any other person*," self-disclosure is the "*explicit communication of self-data another would otherwise not have access to*." (Simms 1994. p. 317.) Such a distinction might contribute to distinguishing between use that necessarily comes with the use of SNSs and use that reveals personal information beyond that extent; and thus determining the "hard core" of privacy on SNSs.

[1056] Solove 2007. p. 198.

[1057] Solove 2007. p. 198.

It comes from the very nature of these sites that, in order to use them properly, the sharing of personal information is needed. Naturally, the individual has the power to decide to what extent he/she is going to provide insight into his/her private life, and to which audiences he/she will grant access. As privacy is also dependent on the individual, it will vary from user to user how they will use these sites.

However, individuals' online presence is dependent not only on the given individual and on his/her choices: other users can also upload personal data relating to third parties. This can either be (ill-)intentioned or can constitute a natural part of self-disclosure. The latter issue is complex because – although individuals do have the right to expose themselves online – in many cases exposing one's own life naturally comes with exposing information relating to another person(s) as well, since the individual's life is necessarily intertwined with that of others.[1058] In any case, an individual does not exercise full control over his/her online presence and reputation.

Therefore, in the light of the above-mentioned factors, the question is: what does privacy mean in the context of SNSs? What is considered to be a reasonable use of SNSs in relation to privacy? Considering that in the European legal order privacy is understood as a flexible concept, which is not limited to secrecy but is also closely connected to self-determination, in the monograph it is understood as the individual's right to decide how to live his/her life. However, in view of the technological and societal changes, should protection be extended to a certain extent to self-disclosing behaviour as well, given the preponderant role SNSs play in establishing and maintaining relationships with others, shaping identity – acknowledged by the European legal order?[1059]

Although *privacy* in public is recognized by the ECtHR, the right traditionally covers cases where the individual's private life is revealed to the public accidentally,[1060] in contrast to SNSs, which are mainly fueled by users' self-disclosing behaviour. In relation to the right to respect for private life, it should be asked whether private life can be extended to social media and if yes, to what extent. Notably relations between "interference" and SNSs should be examined. Historically, the notion of correspondence aimed to cover letters, while today in principle it can cover all kinds of communication, regardless of whether it is a letter, an e-mail, an SMS or a tweet.[1061] However, protection under the right to respect for private life is traditionally granted against "arbitrary interferences", and is not likely to cover cases where the individual himself/herself has decided to publicly share information or a statement – which is often the case when it comes to social media.[1062, 1063]

[1058] Solove 2007. p. 134. Although not naming or identifying the other individual can contribute to preventing privacy issues.

[1059] See, for example, ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992 and ECtHR: *Peck v. the United Kingdom*, application no. 44647/98, 2003

[1060] ECtHR (2004): *Von Hannover v. Germany*, Application no. 59320/00, 24 June; ECtHR: *Peck v. the United Kingdom*, application no. 44647/98, 2003

[1061] Alleaume 2016. p. 459.

[1062] Dupuis 2013. p. 41.

[1063] Labour courts have already addressed the *question of private or public nature* of these sites. Judges had to rule in several cases, and the practice of the courts was not always coherent, till in 2013 the Court of Cassation provided some guidance regarding the private or public nature of these sites, making the protection dependent on the use of privacy settings. Source: Denizeau 2017. pp. 282–284. As a consequence, protection provided by the right to respect for private life is limited when it comes to content publicly shared in social media. These relevant cases will be addressed in detail in Part II.

Even if the right to respect for private life cannot be evoked, it does not mean that these statements do not receive any protection: contrary to the right to respect for private life, the *right to data protection* applies, regardless of whether SNSs are public or private spaces and the fact that the user himself/herself decided to make the information or statement publicly available.[1064] Although the scopes of the right to respect for private life and the right to data protection are not identical, the personal data published often relates to the private life of the individual, making it possible for data protection to provide an alternative protection for the private life of the individual. In my opinion, these observations open the floor for further investigating whether challenges related to SNSs in the employment context can successfully be examined under a dual, privacy-data protection approach. The question of whether employees can freely use these sites, and whether these sites are considered to be a private or public space seems to be more like a privacy-related question. In contrast to the right to respect for private, which is affected by the private or public nature of these sites, data protection requirements shall apply regardless of the nature of these sites or the content, providing protection to employees using these sites. Therefore, the employer regulating or limiting how employees can use these sites would primarily constitute a *privacy-related question*. Using the personal data available on these sites (e.g. dismissing an employee because of a Facebook post), or controlling whether employees comply with the restrictions imposed by him/her can be either a *privacy question* (is that post considered to be a private or a public content?) or a *data protection question* (how can the employer process that data?). This privacy-data protection dichotomy should not constitute a strict separation amongst the legal issues arising, it should rather mean that certain challenges are related to one right to a greater extent than to the other.

In sum, a broad understanding of privacy (see, for example, the already presented ECtHR case law, or the concept of personal life in French labour law) would mean that privacy comprises the individual being able to decide whether to use SNSs and how to use them. He/she can decide on which SNSs he/she is going to be a member and can also decide whether he/she wishes to be an active member of the site (e.g. joining groups or events, liking, posting content), what privacy setting he/she uses. However, as privacy is not an absolute right, admitting that it comprises the free use of SNSs does not empower the user to an unlimited use: the use of SNSs as part of privacy, must be reconciled with other rights and interests.

Examining privacy from a narrower angle focusing upon the concept of secrecy raises different kinds of questions, notably whether such a post can be considered public or private from the viewpoint of intrusion into the private sphere. Data protection can also play its part, as rules laid down by relevant data protection legislations are also applicable – regardless of whether the information itself is public or private – ensuring a different layer of protection during the use of SNSs.

§2. Blurring of work and personal life within social network sites

In addition to the general indistinctness of the place of work, the time of work and the device used for work, the boundaries between professional life and personal life are blurred *within* SNSs as well. The assumption is that SNSs are used in the course of the personal

[1064] Dupuis 2013. p. 44. This is in harmony with the observations of the WP29: *Opinion 2/2017*.

life of the employee, although their use has in many instances become inseparable from the workplace. SNSs have not only altered the limits of privacy but have also provided new methods to investigate people,[1065] as in many cases this information is easily accessible to third parties – such as to employers, for example. The following Sections will examine the main characteristics of SNSs, including the content, the users and the creator of the content, from the angle of blurred professional and personal life.

(A) Content

SNSs a priori suppose a leisure activity pertaining to the personal life of the individual (except for those employees whose job description contains the managing of an SNSs account). However, in certain cases the content published on these sites does not exclusively relate to personal matters, but to matters relating to the employment – making the employer interested (or even entitled) in regulating and or monitoring such activity, as it will be examined in Part II. In such cases the SNS activity of employees can have an effect on their employment relationships. This is particularly the case when the *content directly relates to the employment*. The most obvious way of connecting the workplace to the employee's SNSs activity is to publish something work-related. This can take various forms (such as a post, a comment, liking a page, joining an event, etc.) and substance (e.g. criticising the employer, sharing confidential information, discussing workplace conditions with colleagues, commenting under an article relating to professional matters, etc.).

In addition, even content *without direct connection to the employment* can result in adverse employment decisions, as it can incidentally have a negative impact on the employer. For example, *Ashley Payne*, an American high school teacher was dismissed for posting pictures of herself holding a pint of beer and a glass of wine in her hand during her trip to Europe.[1066] A very similar case was *Stacy Snyder*'s, who was training to be a teacher and was only few weeks from graduation. She uploaded a picture of herself to MySpace, taken of her at a party where she was wearing a pirate hat and was drinking from a plastic cup, while the caption said "drunken pirate". The photo was discovered by her school and supervisor, she was qualified as unprofessional and was denied her teaching degree.[1067]

In addition to the substance of SNS content, changes in relation to *access* to it must be addressed. While earlier employees' personal lives could be separated relatively easily, the novelty that SNSs brought regarding the content is that employees share information that the employer would not have had access to in the pre-SNS era (or only by making great efforts). Therefore, if the employer accesses the profile of the employee (or views his/her activity on SNSs), the employer might have a glimpse into the employee's personal life to an unprecedented extent.

[1065] Qi – Edgar-Nevill 2011. p. 74.

[1066] https://www.californiabusinesslitigation.com/2013/05/high_school_teacher_files_an_a.html (Accessed: 3 May 2018)

[1067] https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html (Accessed: 11 May 2018)

(B) Users

When it comes to *the audience*, on SNSs users usually have colleagues, superiors, clients amongst their connections.[1068] It means that depending on the choice of privacy settings that the given site offers and on whether the employee uses them, published content can become available to them too, giving a glimpse into the employees' online activities, often pertaining to their personal life.

If several *colleagues* are present on these sites, they might discuss work-related matters on these platforms – possibly making negative comments about the employer, as it is demonstrated by growing case law.[1069] Employees continue to express themselves on SNSs just as if they were talking around the coffee machine, often without realizing the risks involved in such online expression.[1070] In this case, due to the change of paradigm in the accessibility of such content, the discussion leaves the working environment and becomes available to *third parties*, such as clients or other users, making it more probable to compromise the employer's reputation.

If the *employer* or the *supervisor* is present on SNSs, they can take a glimpse into the personal life of the (prospective) employee. If the employee does not apply privacy settings, gaining access is evident. In case the employer and the employee are "friends" on the SNS, the employer has the possibility to have access to a vaster amount of personal data. However, it is also worth remembering the existence of the hierarchal relationship between the parties and asking the question: if the employer sends a friend request to an employee, does the latter truly have the possibility to ignore it?[1071]

The novelty brought by SNSs is that the employee has never had the possibility to potentially "reach out" to such a big audience. Perceptions of private and public are elusive, and the employee's post might become available to a considerably wider audience than he/she could potentially reach in the offline world. While formerly only those could do so who were physically present (e.g. gossiping around the coffee machine), today an SNS post can potentially reach a much larger audience and become accessible to several hundreds, even thousands of people.[1072] Therefore, as the employee's online activity can go beyond the workplace, the employer is more intensely interested in ensuring that such posts do not infringe his/her rights or legitimate economic interests.

[1068] According to an article from 2011 written by *Jean-Emmanual Ray*, 55 % of the employees' contacts is composed of colleagues, 16 % of supervisors, 13 % of clients and 11 % of contractors. Source: Ray 2011. p. 132.

[1069] Countless examples could be listed where employees engaged in a discussion about work, such as the case *Barbera v. Société Alten Sir* (Conseil de Prud'hommes de Boulogne-Billancourt, 19 novembre 2010 10/00853), Cour de cassation, civile, chambre civile 1, 10 avril 2013, 11-19.530; CA Rouen Chambre sociale, 1 novembre 2011, n° 11/01827 – These cases and legal questions arising in relation to them will be treated in detail in Part II.) United States District of New Jersey: *Pietrylo v. Hillstone Restaurant Group*, No. 06-05754, 2009; United States Court of Appeals for the Ninth Circuit: *Konop v. Hawaian airlines*, 236 F.3d 1035.

[1070] Duez-Ruff 2012. p. 3. (Page number referring to the online version of the article downloaded from: http://www.lexbase-academie.fr)

[1071] Though J*ean-Emmanuel Ray* notes that it is exceptional that an employee accepts a friend request coming from the employer. Source: Ray 2013. p. 18.

[1072] However, one must stay realistic: in principle indeed, it is possible that a content can reach such a large audience, and indeed there are certain cases that went viral, but in practice most of such posts will stay harmless. Towner 2016. p. 5.

(C) Creator of the content

SNSs can make it easy to *link employees' behaviour to the employer*, as often the user can be identified as the employee of the given employer. This connection between employer and employee can be established in several ways. The most obvious way is if the employee himself/herself identifies the employer by naming him/her in the post or revealing the employer's identity in other ways, such as visual indications. As an example of the latter one, this identification can take place by wearing work uniform. In the *International Union of Elevator Constructors, Local 50 v. ThyssenKrupp Elevator (Canada) Ltd. case* an employee was dismissed after posting a video to the Internet which showed him having his genitals stapled to a wooden plank. The employer was identifiable from the video, as the employees wore their uniform during the recording.[1073] Another example is the case of *Ellen Simonetti*, a flight attendant at Delta Airlines, who was fired for her blog where she uploaded provocative pictures of herself wearing her uniform.[1074]

Usually, users can indicate their place of employment on their profile, in which case it is easier to establish a connection between the employee and the employer than in the pre-SNS era. The audience of the given post might instantly (or just by a few clicks) know which employer the post relates to.[1075] In exceptional cases, it is also possible that even if the employee does not reveal the employer's identity in the post, the employer might be identified later by another user.[1076]

If the given content (post, comment) indicates somehow the affiliation to the employer, he/she might question whether the user published the content as a representative of the employer, or as a simple user –[1077] creating confusion among other users. It is possible, for example, if the employee explicitly refers to his/her affiliation with the given employer, or if it is marked in the profile of the employee – in which cases employees' activities can be associated with the employer. Thus, activity on SNSs can raise the question whether and when the employee can be considered a spokesperson of the employer – and in what regards his/her behaviour can be controlled in order to ensure effective separation between professional and personal use.[1078] The boundaries between professional and personal activity might be blurred by indicating their status as employee.

[1073] https://www.socialmediatoday.com/content/when-your-employees-go-too-far-social-media (Accessed: 11 May 2018)

[1074] https://www.nytimes.com/2004/11/16/business/fired-flight-attendant-finds-blogs-can-backfire.html (Accessed: 11 May 2018)

[1075] For example, Justin Hutchings from London, Ontario was fired in 2012 because he published offensive content ("It's about time this b**** died") to a memorial website of a teenager who committed suicide after being a victim of bullying for years. Mr. Hutchings identified his employer in his profile, and one of the users easily "tracked him down" from that information and reported his behaviour to his employer. http://rabble.ca/columnists/2012/10/employees-beware-perils-posting-facebook (Accessed: 11 May 2018)

[1076] For example, in a case at the *Court of Appeal of Besançon*, the employee took part in a discussion taking place on the wall of a former colleague and though she did not name the employer in the discussion, the employer's identity was revealed later by another employee, after the employee disconnected from the site. (CA Besançon chamber sociale, 15 novembre 2011, 10/02642)

[1077] Such confusion can arise, for example, in cases when in the "bio" part the employer is identified, or when the employee explicitly states in a post or comment that he/she is an employee at the given workplace, or if the logo of the company is used as well as a profile picture or cover picture, making it possible to confuse the employee and the representative of the company.

[1078] This matter will be further adressed in Title 3 of Part II.

The importance of SNSs in this field is that they made it considerably easier to identify the user as the employee of a certain employer, creating a constant link between the employee's online behaviour and the identity of the employer. The offline counterpart of such a link would be to wear a sign on one's back, indicating the place of employment. This results in the phenomenon that today most users are more easily identified as the employee of a given employer, which creates a constant "bridge" between the employee's personal life and place of employment, and dissolves the previous boundaries between professional and personal life.

PART II.
RIGHT TO PRIVACY AND RIGHT TO DATA PROTECTION DURING THE MONITORING AND CONTROLLING OF THE USE OF SOCIAL NETWORK SITES IN THE EMPLOYMENT CONTEXT

After examining the collision of rights and how SNSs have intensified it, it is necessary to address how exactly SNSs challenge the employment relationship. Questions can arise in various areas ranging from employers inspecting job applicants' Facebook profiles, through employees surfing on Instagram instead of performing work, to employees who heavily criticise their managers on SNSs. It is important to emphasize that SNSs did not give rise to fundamentally new questions, as all the examined conducts had existed well before their appearance (even without SNSs job applicants could lie in their CV, employees could waste working hours or could criticise their employer), and were subject to legal regulation as well. Rather, SNSs put these already existing legal rules into a new perspective:[1079] they raise questions in relation to *how* the existing data protection and labour law rules can be applied to them. Part II. provides a deep analysis of the "old" problem, through examining it during the whole existence of the employment relationship, focusing on the law of France and Hungary.

Throughout the employment relationship, the personal life of the individual can be affected in several ways. To address them in a systematic way, the individual's right to privacy/right to data protection will be contrasted against the employer's various rights throughout the lifetime of the employment relationship. During *recruitment*, it will be examined how inspecting job applicants' SNS profiles in order to enforce the employer's freedom of contract can collide with applicants' rights. SNSs can seriously compromise *working hours*: it will be examined how their use (simply the fact of spending time on SNSs during working hours) can be controlled and monitored in accordance with the employer's right to monitor. Finally, besides the mere fact of using these sites, it will be addressed what kind of questions the employees' presence raises (typically their *off-duty conduct*, covering cases when they post something to SNSs beyond working hours) in relation to the employer's right to reputation, protection of business secrets, etc.

Both privacy and data protection are crucial in ensuring the protection of the employee's personal life, during the whole employment relationship. However, depending on the given field of the employment relationship, either the right to privacy or the right to data protection can appear in a more emphatic way, giving rise to more substantial questions. This double approach is assessed through the division of regulation and monitoring: regulation mostly relates to imposing limitations on employees' *use* of SNSs, while monitoring aims to cover the *processing* and the use of personal data obtained from SNSs.

As such, the monograph holds the view that *recruitment* can be more effectively assessed through data protection. The reason for this is that during this phase it is the monitoring of job applicants' online presence and the processing of their personal data which are more emphatic, and not the employer's potential to restrict such a use or to interfere with their

[1079] Maier 2013. p. 282.

personal lives. In the case of the use of SNSs *at the expense of working hours*, both the privacy and the data protection approaches are equally significant: the privacy approach is connected to the possible ban of the personal use of these sites, while data protection relates to the monitoring of such a ban. However, when it comes to employees' *off-duty conduct*, the right to privacy gains more importance, notably through the employer's possibility to sanction employees because of their conduct outside working hours.

Part II. is composed of three titles, each covering a significant area of SNSs and labour law where questions regarding privacy and data protection arise. *Title 1* will address questions relating to prospective employees and will examine the phase of recruitment. Then, *Title 2* will discuss SNS use at the expense of working hours and will examine SNS use during working hours in detail. In *Title 3*, focus will be put on the employees' activity and presence on SNSs, particularly outside working hours and on how such an activity can conflict with the employer's different rights.

Title 1: Concluding an employment contract in the context of online social network sites

Issues of privacy and data protection do not arise in relation to employees only, but are present in the pre-employment phase as well. *Spiros Simitis* emphasized the importance of regulating prospective employees' right to data protection, noting that they constitute one of the groups mainly affected by the employer's need to obtain as much information as possible.[1080] The specialty of pre-employment background checks is given by the fact that although there is no existing employment relationship between the parties, several data protection and labour law provisions are applicable to them.[1081] Also, this relationship is characterised by a disparity between the parties: although formally the employment contract is concluded between two equally autonomous parties, *de facto* there is no equality between them: the applicant is in a more vulnerable position.[1082]

When it comes to SNSs, employers often turn to these services in order to find out as much as possible about applicants. However, when conducting such screenings, they can also access information relating to the personal life of the applicant, which leads to potential privacy and data protection issues. As a main rule, for the purposes of the monograph, what is meant by these screenings is the employer accessing the publicly available information on these sites – the case when he/she accesses concealed information will be addressed separately. Since in these cases the information is publicly shared at the initiative of the user, privacy issues are less dominant than data protection issues – which are independent of the individual's behaviour. Therefore, the question of pre-employment SNS screenings will be primarily dealt with from the aspect of data protection.

SNSs have become a popular tool when it comes to recruitment, as they provide quick, easy and inexpensive access to a multitude of information, allowing one to draw conclusions about the applicants' character.[1083] Before the widespread proliferation of SNSs, the employer had to assess a job candidate's aptitude for the job through the way of conducting interviews, ability or aptitude tests, questionnaires (or in extreme cases by hiring a private investigator), while today it might be sufficient to check the candidate's Facebook profile in order to have easy and cost-free access to a rich and significant amount of information relating to the capacities of the prospective employee. The ease, the cost-effective nature and the wide range of information potentially make SNSs a powerful tool during the recruitment process – however, the legality of such screenings must be examined.[1084]

To date, there exists no "Facebook Act" – either in France, or in Hungary – regulating explicitly the labour law and privacy/data protection aspects of SNSs. The alternative legislation to be applied in this case is the relevant provisions of the labour law regulations and data protection regulations: SNSs are not "*terra nullius*", the general principles of recruitment laid down in the labour codes, such as non-discrimination, transparency, relevancy and confidentiality, apply to every method of recruitment, regardless of the

[1080] Simitis 1999. p. 54.
[1081] Kun 2018. p. 132.
[1082] Hajdú 2004. p. 26.
[1083] Suder 2014. p. 124.
[1084] Brown – Vaughn 2011. p. 220.

technology used.[1085] Besides the data protection regulation, the labour codes of both countries regulate the recruitment process, imposing limitations on the possible methods used. This protection applies regardless of the method used, therefore they include SNS background checks, too.[1086] These provisions incorporate the most important data protection principles, such as purpose limitation, proportionality and prior notification.

The Title is composed of two parts: Chapter 1 will focus on recruitment and the relevant labour law provisions, while Chapter 2 will deal with the arising data protection issues. *Chapter 1* will be based on the comparison of the French and Hungarian systems, as it is possible under the GDPR to adopt Member State specific data protection regulation in the field of employment, giving room for certain differences between the legal systems. *Chapter 2* will focus on data protection, and since the EU has a unified data protection law, there are basically no problems specific only to French or to Hungarian law. Therefore, the presentation of the issues itself will stay on an analytical ground from a more general scope, paying special attention to the solutions proposed by French and Hungarian legislation and case law.[1087]

Chapter 1: Labour law aspects of recruitment

Challenges arising in relation to pre-employment SNS screenings must be assessed in the light of the already established rules regarding recruitment. Both in France and in Hungary, limitations were placed on the "traditional" hiring methods (e.g. conducting a job interview or collecting references from the previous employer), addressing data protection questions under the auspices of labour law. However, these rules were elaborated when the methods mainly consisted of using personality tests, graphology tests, interviews, etc. – providing completely different kinds of personal data than SNSs nowadays. As a consequence, it must be examined whether SNSs affect the existing legal landscape.

Section 1: Identifying the best candidate

The main aim of the employer during the recruitment is to identify and hire the best applicant. In order to achieve this aim, *(§1)* the employer is entitled to choose with whom he/she wishes to contract and is interested in obtaining as much information as possible regarding applicants in order to make this decision. *(§2)* SNSs can serve this information hunger of the employer and can highly contribute to identifying the right applicant.

[1085] Tricoit 2013. p. 10.

[1086] In contrast, approaching the question from a "privacy point of view", when the employee *publicly* shares some information, it goes beyond the protection offered by the right to respect for private life. Source: Tshilembe 2015. p. 700.

[1087] In this context, not only the court's jurisprudence is meant by case law, but also the practice of DPAs.

§1: The employer's side: freedom of contract

(A) The employer's interests in obtaining information

The employer's aim during the recruitment process is to identify and hire the most suitable candidate who would fit into the organisation. In order to achieve this aim, the employer is interested in knowing as much as possible about the candidate. The employer can either "screen in" for desired characteristics, or "screen out" possible unsuitable applicants.[1088]

Having a profound knowledge on not only the candidate's education and professional experience, but also on his/her personality and beliefs can contribute to assessing whether he/she could easily identify with the values of the specific employer.[1089] Pre-employment background checks can contribute to higher productivity, increased quality and lower employee turnover, and can also help to detect whether the employee has a history of misconduct.[1090] The reason for wanting to explore the applicant's background is the employer's belief according to which "past performance is the best predictor of future behaviour."[1091]

Naturally, information on the education, previous work experience, language skills, computer literacy skills or leadership skills is undoubtedly connected to the professional life of the employee. Knowing whether the employee has the necessary qualification and experience, where he/she pursued his/her studies and worked prior to applying for the job is indispensable for deciding who is going to be employed. It goes without saying that the employer is interested in obtaining as much information as possible in these fields.

Besides information bearing professional character, employers are interested in having a widest possible pool of information on applicants, including their personal lives. Though this interest can be distinct from the employer's rights in this field, as legal regulations aim to protect employees' personal lives, it does not mean that the assessment of the personal traits is to be completely excluded during the decision-making. Besides the professional capacities of the applicant, employers are also interested in assessing whether the personal traits of the applicant make him/her suitable for the given post.[1092] When concluding an employment contract, the *personality of the prospective employee* has a key, determining importance, as it can highly influence his/her successful integration into the undertaking. SNSs can largely contribute to gaining information regarding the personality of the applicant.

Usually, traditional background searches focused on matters like résumé accuracy, educational backgrounds, driving records, and reference verification, etc.[1093] In addition to formally assessing submitted CVs or conducting interviews, through background checks employers are interested in assessing the personal traits of the applicant – such as whether he/she is lazy or antisocial, or has provided false information during the application – in order to know whether they are going to be a good choice for the workplace or for the job.[1094]

[1088] Befort 1997. pp. 367–368.
[1089] Sprague 2011. citing *Alan Finder* (https://www.nytimes.com/2006/06/11/us/11recruit.html)
[1090] http://www.sweeneyinc.com/files/benefits_preemployment_screening.pdf (Accessed: 3 May 2018) p. 2., p. 3.
[1091] Sprague 2008a. p. 399.
[1092] Lehoczkyné Kollonay 1997. p. 91.
[1093] Jones – Schuckman – Watson 2007. pp. 53–54.
[1094] Peebles 2012. p. 1399.

With (SNS) background checks, employers can assess the applicant's personality in order to assess whether they are going to integrate well into the company.[1095] The employer is interested in knowing whether the employees would fit well into the existing work community and would be able to effectively cooperate with colleagues. Also, personal sympathy can play a role: the employer is interested in employing someone with whom he/she can imagine working with.

Employers might also be concerned about the lifestyle (e.g. drug or alcohol consumption, expressing extreme political or religious views, etc.) and the reputation of the applicant, as the applicant's questionable conduct or poor reputation can have a negative impact on the employer.[1096]

(B) Freedom of contract

From a legal perspective, the employment relationship is considered to be a *personal*, long-term legal relationship,[1097] where the identity of the parties plays an important role: performing work in person is one of the primary qualifying attributes of the employment relationship,[1098] having crucial importance. The HLC also defines among the employee's main obligations the obligation to perform work *personally*.[1099] The employee cannot use a replacement, as the education, work experience, professional aptitudes are all connected to the person of the employee.[1100]

The *intuitu personae* character, meaning that the identity of the contracting parties is the essential element of the contract,[1101] plays an important role in concluding the employment contract.[1102] It means that the employer can take into consideration the person of the applicant, in order to ensure the good functioning of the workplace.[1103] Although legal regulations impose limits on the extent of the information that can be asked (such as rules relating to the prohibition of discrimination, or respecting personal life); considering certain subjective characteristics, such as the personality of the applicant, cannot be fully eliminated from the employment relationship.[1104]

The importance of the identity of the parties is manifested in the *freedom to contract*: a general principle of civil law stipulated both by the French[1105] and by the Hungarian[1106] civil codes. It means that the parties can freely decide whether they wish to contract, with whom to contract and on which terms to contract.[1107] With regard to our main subject, deciding the person of the contracting party has special importance.

[1095] Baumhart 2015. p. 508.
[1096] Del Riego – Sánchez Abril – Levin 2012. p. 18.
[1097] Gyulavári 2012. p. 19.
[1098] 7001/2005. (MK 170.) FMM-PM együttes irányelv
[1099] Item c of Subsection 1 of Section 52 of the HLC
[1100] Hajdú – Kun 2014. p. 194.
[1101] "*[A] personal service contract where the particular individual cannot be replaced*". Source: Canadian National Railway Co. v. Norsk Pacific Steamship Co., [1992] 1 SCR 1021, 1992 CanLII 105 (SCC)
[1102] Rivero – Savatier 1978. p. 62.
[1103] Péano 1995. p. 3. (Page number referring to the online version of the article downloaded from: www.dalloz.fr)
[1104] Péano 1995. p. 4. (Page number referring to the online version of the article downloaded from: www.dalloz.fr)
[1105] Article 1102 of the French Civil Code
[1106] Subsections (1) and (2) of Section 6:59 of Act V of 2013
[1107] Vékás 2013. p. 545.

This freedom of contract covers the conclusion of the employment contract: the employer can decide with whom to conclude an employment contract and the future employee can choose where to apply.[1108] Identified as a principle with constitutional value in French law, the employer has the freedom to choose his/her collaborators:[1109] he/she has the possibility to have preferences when it comes to choosing between applicants.[1110] The employee also has the freedom to choose whether he/she is going to apply for or accept a position, and can decide where to apply.[1111]

As a result, the interests of the employer demand to consider not only the candidate's professional capacities,[1112] but also his/her personal traits.[1113] He/she is legally entitled to take into consideration certain extra-professional elements of the applicant's life,[1114] although legal regulations impose serious limitations regarding the *intuitu personae* character of the employment (e.g. discrimination, equality, individual freedoms).[1115]

§2: Methods of recruitment: Internet and social network sites

Different methods of selection help to provide the HR manager with a complete view of the candidate's aptitudes or inaptitudes,[1116] through which the employer can obtain an extensive range of information regarding the candidate's professional aptitudes, his/her personality or even his/her private life. Besides the traditional methods of recruitment, such as conducting an interview, polygraph test, aptitude test, graphological tests, personality tests, medical tests, collecting references, etc., online background checks have gained considerable importance.

The advent of the Internet and SNSs has considerably changed what kind of information employers can discover regarding job candidates. They have become a popular recruitment method and gained ground in the phase of recruitment.[1117] The rich amount of personal data and information present on SNSs can contribute to the identification of the most suitable candidate. However, in the recruitment process a difference should be made between professional SNSs and personal SNSs. *Professional SNSs* (e.g. LinkedIn, Viadeo) have the aim to maintain a professional identity, make useful contacts and search for opportunities. In contrast, their *personal* counterparts (e.g. Facebook, Instagram) are primarily used for entertainment and to engage with the "friends" of the user.[1118]

[1108] Kiss 2002. p. 268.; Radnay 2008. p. 88.

[1109] Conseil constitutionnel: décision n° 88-244 DC du 20 juillet 1988

[1110] Lyon-Caen 1992. p. 57.

[1111] Lyon-Caen 1992. pp. 57–58. Article XII of the Fundamental Law of Hungary

[1112] The employer can verify whether the applicant truly has the professional capacities necessary for the given job and whether information in the applicant's CV is authentic. Source: Cantero – Coupez 2014. p. 39.

[1113] Teyssié 1988. p. 375.; Arany-Tóth 2008a. p. 112.

[1114] Jacquelet 2008. p. 64.

[1115] Péano 1995. pp. 132–133.

[1116] Bokor et al. 2007. p. 150.

[1117] https://business.lesechos.fr/directions-ressources-humaines/ressources-humaines/recrutement/030656487193-85-des-recruteurs-font-des-recherches-en-ligne-sur-les-candidats-314060.php (20 June 2019).; Szűts 2015. p. 29.

[1118] https://econsultancy.com/personal-versus-professional-social-networks-infographic/ (Accessed: 13 August 2019)

Professional SNS profiles contain information primarily relating to the professional life of the individual: often information also present in the CV (education, work experience) completed with information typically not present in a CV but still having professional characteristics (work contacts, articles written by the individual, etc.). The professional or personal nature of the given SNS – together with the use(/lack) of the privacy settings – can have major importance when it comes to evoking the employee's right to respect for private life.[1119] Naturally, the candidate's personal life is concerned to a lesser extent when it comes to the inspection of professional SNSs,[1120] due to the fact they primarily contain information relating to the professional life of the individual, in contrast to personal SNSs, such as Facebook. For this reason, the following analysis will concentrate on personal SNSs, as their inspection might raise more severe privacy and data protection challenges or even infringements.

Conducting such background checks can be beneficial to the employer for two reasons. *First*, as it was already demonstrated in Part I, SNSs provide an unprecedented access to a wide range of information on prospective employees – both regarding information relating to professional capacities and personal traits. Applicants are often inaccurate or even dishonest when writing a résumé and have rehearsed answers to interview questions that hide their true personality traits.[1121] However, SNSs can reveal a multitude of information.

The information obtained in such a way can be of interest to the employer in several regards. A study from 2010 conducted by *Cross-Tab* on the attitudes relating to "online reputation"[1122] searches reveals that the following – quite extensive – reasons were considered in the recruitment process and led to the rejection of a candidate: concerns about the candidate's lifestyle; inappropriate comments and text written by the candidate; unsuitable photos, videos, and information; inappropriate comments or text written by friends and relatives; comments criticizing previous employers, co-workers, or clients; inappropriate comments or text written by colleagues or work acquaintances; membership in certain groups and networks; discovering that information the candidate shared was false;[1123] poor communication skills displayed online and concerns about the candidate's financial background.[1124]

Second, these searches are extremely easy to be conducted, entail minimal costs and allow the employer to obtain a rich pool of information beyond the candidate's professional capacities, which in the pre SNS-era would have been more difficult and less cost-effective to obtain through the traditional methods.[1125] They require only an electronic device capable of connecting to the Internet and an Internet connection. Then, the employer can easily inspect the candidate's profiles through a simple Internet search.

[1119] Tshilembe 2015. pp. 699–700.

[1120] Instead of leading to issues, (especially) a professional account treated with due care can highly enhance the individual's chances of getting employed. Byrnside 2008. pp. 457–458.

[1121] Mooney 2010. p. 737.

[1122] Meaning by online reputation the "*[…] publicly held social evaluation of a person based on his or her behavior, what he or she posts, and what others (such as individuals, groups, and Web services) share about the person on the Internet*." https://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf. (Accessed: 3 May 2018) p. 3.

[1123] According to certain surveys, nearly half of the job applicants lie about their work history and education. Source: Sprague 2008a. p. 398.

[1124] https://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf (Accessed: 3 May 2018) p. 9.

[1125] Brown – Vaughn 2011. p. 220.

Despite providing such a huge amount of information with minimal costs and efforts, SNS background checks present certain risks as well. In particular, several legal issues arise during their use, with special regard to the right to privacy and the right to data protection and relating to discrimination as well.[1126] These legal issues will be dealt with in detail in Chapter 2. Also, beyond legal arguments, conducting SNS background checks can have a detrimental effect: the employer's perception by job candidates might also be adversely affected: especially young job seekers would feel frustrated if the employer conducted a detailed online background check.[1127]

Section 2: The traditional recruitment procedure

Differentiation must be made between the information that the employer would like to obtain (as much information as possible) and between the information that he/she is legally entitled to obtain (regulated by labour law and data protection regulations). Despite the existence of the employer's right to choose with whom to contract, this right is not limitless.[1128] Section 2 will examine the rules imposing limitations on the employer's information thirst.

Rules relating to the "traditional" recruitment procedure (e.g. tests, job interviews) were already elaborated especially by the doctrine and the practice of the data protection supervisory authorities. The following paragraphs will limit themselves to the presentation of the data protection rules in general during the recruitment phase, while their application and the specific data protection questions relating to SNSs will be discussed under Chapter 2.

§1: Labour law and applicants' rights

As it was already referred to in Part I, both the FLC and the HLC contain provisions regulating employment and data protection. They also regulate the recruitment phase as well. Even though these provisions do not explicitly aim SNSs, they are adequately applicable to them as well.

(A) Provisions of the labour codes

Prior to discussing the issues specific to SNSs, it is necessary to review the data protection provisions of the labour codes. Before addressing *(b)* the data protection requirements laid down in the labour codes, it must be examined *(a)* whether these provisions are applicable to job applicants at all.

[1126] Del Riego – Sánchez Abril – Levin 2012. pp. 18–21.

[1127] Byrnside 2008. p. 475. Although back in 2008 (and in 2006, as the source referred to it) a pre-employment social media vetting might have been considered outrageous by candidates, today it has become a mainstream phenomenon, so it might be judged differently.

[1128] Arany-Tóth 2008a. p. 112.

(a) Applicability to job candidates

Naturally, when it comes to the recruitment process, the subjects of the different recruitment methods are *prospective* employees and not employees. As these individuals are not yet employees, the question of the applicability of the labour law regulations might be raised and therefore should be clarified. The question whether the provisions of the labour code are applicable only to employees or they include prospective employees as well is not raised in French legislation. France was the first country in the European Economic Community to adopt a legislation specifically aiming to regulate recruitment methods:[1129] since 1992, due to the act relating to employment, the development of part-time work and unemployment insurance,[1130] the FLC contains provisions explicitly regulating the recruitment process (Article L1221-6 – Article L1221-9), making it unquestionable that job applicants are covered by these provisions.[1131]

In contrast to the FLC, the HLC contains no expressed provision regarding the hiring procedure, leaving room for certain questions. The HLC does not mention the expression "job applicant", it uses the term of employee. Even when determining the personal scope of the HLC, the word employee is used.[1132] With respect to the recruitment phase, only a reference can be found in Subsection 1 of Section 10, which regulates statements and disclosure of information and states that "[an] employee may be requested to make a statement or to disclose certain information only if it does not violate his/[her] rights relating to personality, and if deemed necessary for the *conclusion […] of the employment relationship[.]*"[1133]

These provisions raise an important point of law, such as: *does the personal scope of the HLC cover the candidate, too*? Opinions differ regarding this question. When examining this section,[1134] *Tibor Breznay* mentions only the employee and not recruitment,[1135] while *Katalin Berki [et al.]* stipulate that this provision only aims employees.[1136] According to the Equal Treatment Advisory Board, the HLC's provisions are only applicable to employees and employers and therefore do not cover the recruitment process.[1137] In contrast, according to *Csilla Lehoczkyné Kollonay*, the provisions aiming to ensure the protection of employees are applicable to the selection process, too.[1138] *Mariann Arany Tóth*, and *József Hajdú* and *Attila Kun* are of the same

---

[1129] Ray 1993. p. 109.

[1130] Act No. 92-1446 of 31 December 1992 on employment, the development of part-time work and unemployment insurance ("Loi n° 92-1446 du 31 décembre 1992 relative à l'emploi, au développement du travail à temps partiel et à l'assurance chômage")

[1131] Not to mention the general formulation of Article L1121-1 of the FLC, not only aiming to protect employees, but every person.

[1132] Subsection (1) of Section 2 of the HLC

[1133] Subsection (1) of Section 10 of the HLC. Emphasis added by the author.

[1134] It should be mentioned that the sources below concern the previous HLC (Act XXII of 1992), which contained a similar provision. (Section 77)

[1135] Breznay 2002. p. 115.

[1136] Berki et al. 2008. p. 278.

[1137] Az Egyenlő Bánásmód Tanácsadó Testület 1/2007. TT. sz. állásfoglalása az állásinterjún feltehető munkáltatói kérdésekről

[1138] Lehoczkyné Kollonay 1997. p. 91.

opinion, namely that the personal scope of the provisions mentioned covers the candidate, too.[1139, 1140]

The latter viewpoint is supported by the fact that the general reasoning of the HLC emphasizes that according to the general principle, unless contrary to labour law regulation, civil law rules constitute the underlying rules of the HLC.[1141] When declaring the protection of personality rights in the employment context (Section 9), the HLC refers to the Civil Code – which states that *every person* is entitled to the protection of the personality rights.[1142] Also, in the employment relationship a hierarchal relation can be found between the parties, the employee is in a position of existential vulnerability.[1143] One of the aims of labour law is to counterweigh this vulnerability; in order to achieve this, labour law contains several provisions for the protection of the employee.[1144] However, this existential vulnerability is not unique to the employee-employer relationship: it is (even more intensely)[1145] present before the conclusion of the employment contract, as – under the not always favourable labour market conditions – the candidate is typically not in the position to balance between concluding a contract and the violation of his/her fundamental rights.[1146]

Based on the above-mentioned arguments, it seems logical that the provisions protecting employees must be adequately applicable to candidates. The phrasing of Section 10 itself also suggests the applicability of these provisions to candidates as it regulates the case of *concluding* the employment contract – for which one needs to be a candidate and not an employee.[1147] With regard to the above, it would be recommended to clarify in Hungarian law – similarly to French law – that the relevant data protection provisions of the HLC are also applicable to job applicants. Such a clarification might include the insertion of a subsection stating that these provisions are to be applied to job applicants as well.[1148]

(b) Applicants' right to data protection in the labour codes

While the FLC explicitly aims recruitment, the HLC does it in a more abstract way, through regulating employee statements and disclosure of personal information in order to conclude an employment relationship. These provisions echo data protection requirements such as purpose limitation, necessity, relevancy and transparency.

Besides the general clause of Article L1121-1 stipulating the protection of individual and collective rights and freedoms, from Article L1221-6 to Article L1221-9 the FLC contains provisions explicitly regulating the recruitment process. In these provisions it expressly

---

[1139] *Arany-Tóth* 2008a. p. 114.; Hajdú – Kun 2014. p. 94.

[1140] According to J*óri et al*., the *material* scope of the act covers the hiring phase, too. Source: Jóri – Hegedűs – Kerekes 2010. p. 278.

[1141] *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről*, 2011. p. 86.

[1142] Similarly, the basic principles of the Privacy Act are applied to every data processing, not only to the processing of personal data relating to employees.

[1143] However, it also has to be seen that this defencelessness does not characterize all employees. Bankó –Szőke 2016. pp. 43–44.

[1144] Gyulavári 2013. p. 19.

[1145] The Commissioner's Recommendation on job advertisements and on the activity of private recruitment agencies

[1146] Hajdú 2005. p. 170.

[1147] Arany-Tóth 2008a. p. 114.

[1148] Such a subsection might be formulated as follows: "*Subsection (6) of Section 10: Subsections (1)–(5) are also adequately applicable to job applicants.*"

refers to the most important data protection principles, leaving no question regarding whether these principles are applied to the recruitment phase or not.

Article L1221-6 asserts the *principle of finality*, which requires that information asked from a job applicant in any form must only be processed for the aim of assessing the applicant's capacities to occupy the given employment or to evaluate his/her professional abilities. Therefore it aims to protect the applicant's extra-professional life through limiting the processing of personal data to the professional capacities of the applicant.[1149] Moreover, it emphasizes the principle of necessity by stipulating that the information obtained must have a direct link and must be necessary for the proposed job or for the evaluation of professional aptitudes. The Article also prescribes that the applicant must reply in good faith to the information requests.

Article L1221-8 requires the employer *to inform* the applicants regarding the methods and techniques used for recruitment, prior to their application. It also declares that the results obtained with such methods and techniques are confidential. These methods and techniques must be relevant in the light of the objectives sought. Article L1221-9 further emphasizes the *principle of transparency* and the employer's obligation to inform applicants prior to the collection of personal data.

The HLC contains provisions relating to *employee statements and disclosure of personal information* – which covers the case of processing the job applicants' personal data through obtaining different kinds of information. The HLC also prescribes the purpose limitation principle; it defines the purpose of such processing, which is the conclusion of the employment relationship,[1150] and in relation to this identifying the best candidate. [1151] It further refers to the principle of necessity and adds that statements and disclosure must be necessary in order to conclude the employment relationship[1152] – imposing limitations on the scope of information that can be processed.[1153] Also, similarly to the FLC, the HLC also contains provisions with respect to *informing* candidates: it requires employers to inform candidates in writing prior to the data processing.[1154] It means that information must be provided to applicants, thereby ensuring the transparency of the processing.

With regard to the grammatical formulation of the labour codes regulating data processing in the recruitment phase, a suggestion might be made. As these provisions were adopted before the vast proliferation of SNSs, their application to these Web 2. 0. services might raise certain concerns, as the grammatical formulation of the relevant provisions of the labour codes does not correspond perfectly with the reality of the information society. The FLC uses the expression "information requested" ("informations demandées") in the first subparagraph of Article L1221-6, while the HLC employs the expression "making a statement or disclosing certain information" ("nyilatkozat megtétele vagy adat közlése") in Subsection 1 of Section 10. Interpreting these provisions from a strict grammatical point of view would result in excluding information obtained by the employer through unilaterally accessing (without requesting) the prospective employee's SNS profile.

[1149] For example, the employer can ask for a school certificate, proof of a degree, driving licence, but cannot ask for academic records or for personal files. Source: Radé 2002. p. 184.

[1150] Subsection (1) of Section 10 of the HLC

[1151] Arany-Tóth 2016– p. 29.

[1152] Subsection (1) of Section 10 of the HLC

[1153] Usually information directly connected to the identity of the applicant is not considered to be essential for the conclusion of the employment contract. Source: Bankó – Berke – Kiss 2017. p. 46.

[1154] Subsection (5) of Section 10 of the HLC

The aim of these provisions is to protect job candidates' rights during recruitment, regardless of the method used. Data protection requirements also apply to every processing during recruitment. So, despite this grammatical lack, the data protection requirements apply; still, it would be desirable to clarify the scope of protection. In order that the grammatical formulation of these provisions better correspond with real-life conditions, it would be desirable to complete the regulation with the expression "collected", reflecting better the reality of the methods of obtaining personal data in the age of the information society.

(B) Practice of the data protection supervisory bodies

Both the CNIL and the NAIH have addressed the question of the job applicant's right to data protection, emphasizing that the employer must respect data protection requirements during the recruitment as well and clarified how exactly employers should comply with these requirements in this context. They examined the proper use of different recruitment tools (e.g. lie detectors, personality tests, etc.) from a data protection point of view, giving substance to the general provisions of the labour codes. In the following, instead of the exhaustive presentation of the CNIL's and NAIH's practice, focus will be put on their conclusions which might be relevant in relation to SNSs.

(a) France: the CNIL

The CNIL issued a *deliberation* in 2002 *on the collection and processing of personal information during recruitment*,[1155] in which it clarified the application of the data protection principles to the recruitment process. It stated that unless justified by the specific nature of the job, or by the legal regulation of a foreign country concerned by the post, generally – amongst others – information such as date of entry to France, information relating to family members (name, nationality, profession), height, weights, housing conditions or community life shall not be processed. The deliberation also states that it is prohibited to process personal data relating to the candidate's racial or ethnic origin, political opinion, religious or philosophical convictions, membership in a trade union, data relating to his/her health or sexual life – without the consent of the applicant. Even in the case of consent, the processing cannot lack a direct and necessary link to the job proposed.[1156, 1157]

The CNIL reiterated this position in several of its documents. In 2013 it provided a list of information which is, as a main rule, not relevant, unless justified by particular circumstances. These items of information include, for example, date of arrival in France, original citizenship, family background, health status or community life[1158] – information which is often shared on SNSs by an average user. In its information sheets relating to employment, the CNIL also dealt with the phase of recruitment, and again it reiterated

[1155] CNIL: *Délibération n°02-017* du 21 mars 2002

[1156] It should not be forgotten that, as demonstrated before, since 2002, the appreciation of the validity of employee consent as a legal ground of processing has considerably changed.

[1157] The deliberation also treated the question of transparency and prior information of the individual, the exercise of the rights of the data subject and the prohibition of automated profiles.

[1158] https://www.cnil.fr/fr/les-operations-de-recrutement (Accessed: 20 June 2019)

the importance of the principle of relevancy and the importance of being informed on the processing of applicants' personal data.[1159]

While previously the employer had to actively look for that information, today it is not uncommon to find this information within reach on SNSs. In addition, drawing conclusions from this information might matter, too. In another *deliberation in 2007*,[1160] the CNIL recognized the lack of relevancy and the very subjective nature of comments contained in files relating to applicants (and former employees).[1161] So the conclusions drawn from the consultation of the profile of the applicant shall also present an objective nature.

(b) Hungary: the Data Protection Commissioner and the NAIH

In 2006 the Hungarian Data Protection Commissioner adopted a recommendation on job advertisements and on the activity of private recruitment agencies[1162] in order to ensure the uniform protection of job applicants' rights. In this recommendation the Commissioner drew attention to the informational vulnerability of job applicants and the increased importance that he/she can follow and control the processing of his/her personal data during the hiring process. It is crucial that the applicant is aware to whom he/she is sending the information and knows where he/she can ask for information regarding the status of the decision. Therefore, job advertisements must contain information about the controller and about the contact information ensuring that the applicants can exercise their rights relating to the processing. In a case[1163] on the questions that can be asked during a job interview, the Commissioner noted that if the employer asks a question violating privacy rights, in order to prevent impairment of rights, the applicant can refuse to answer or can give an untruthful answer.[1164]

The former *Hungarian Data Protection Commissioner* extensively dealt with the issue of tests and data protection. According to him, a difference must be made between two types of the tests: between tests evaluating the professional suitability and readiness, and between tests relating to psychological and personality traits of the individual.[1165] The former case relates to tests aiming to map the professional competences and expertise of employees, and indeed the employer is entitled to obtain that information, before and also during the employment.[1166] In contrast, tests aiming to know the psychological or personality traits can enable the employer to draw conclusions relating to the individual's personal traits that can contribute to organizing work more effectively. Although this is a legitimate interest on the part of the employer, during the enforcement of this interest the employer must respect the employee's personality rights.[1167]

[1159] CNIL: *Le recrutement et la gestion du personnel*. Fiches pratiques. Travail & Données personnelles, 2018

[1160] CNIL: Délibération n°2007-374 du 11 décembre 2007

[1161] These comments included, for example, comments relating to the behaviour of the individual ("catastrophe", "liar and unreliable", "lame", "not great", "hygienic problems (smell) !!!!!", "so annoying"), comments relating to their health status ("disappeared after a depression", "depressive", "problems with alcoholism", "suffers from cancer, cannot work anymore") or comments relating to the personal or family relations ("girlfriend/friend of M. – not reliable", "does not live with her husband anymore", "wife of G.").

[1162] ABI 167/A/2006-3.

[1163] ABI 900/A/2006

[1164] ABI 900/A/2006

[1165] ABI 814/A/2004-8.

[1166] ABI 814/A/2004-8.

[1167] ABI 814/A/2004-8.

Relating to this case, the Commissioner also emphasized that depending on the characteristics of the given job, certain personality traits might have increased relevancy, these tests cannot be used on a general basis to a large group of employees: its use should be carefully planned and selected. Also, the tests should be limited to the examination of the personal traits essential for the employment, with the existence of a legitimate purpose. It was also recommended that an independent third party should analyse the tests.[1168] In the same case, the Commissioner also stated that the psychological test should be based on the informed, voluntary consent of the employee. However, this statement has become outdated since, as the case took place in 2004; later it was concluded that the voluntary nature of the consent is highly questionable and that the legitimate ground of balancing rights and interests might be better adapted to the employment context.[1169] As on SNSs the employer has an unprecedented possibility to assess the personal traits of job applicants (and employees), these requirements will have high importance in the case of pre-employment SNS screenings – as will be presented in Chapter 2.

In another case[1170] the Commissioner dealt with a machine using digital face recognition destined to be applied during interviews. The machine would analyse the features of the applicant and draw consequences regarding his/her personality traits and behaviour. In relation to personality tests, the Commissioner laid down that the employee cannot be subjected to a method which would provide the employer data over which the individual does not have control. First, the result of the test should be transferred to the individual, who can then decide whether he/she consents to transfer it to the employer, providing him/her the possibility to make a decision. The Commissioner also outlines that there is another, more traditional method to effectively assess whether the employee is truly competent and well-suited for the job: probation.

In 2012 president of the NAIH *Attila Péterfalvi [et al.]* summarized what requirements an aptitude test must meet.[1171] First of all, the principle of purpose limitation requires that it must be determined exactly what competences these tests aim to measure and how it is relevant regarding the employment relationship. In addition, the methods chosen must be able to assess these competences: they shall provide relevant data that can in reality contribute to achieving the purpose of the processing. As these tests are able to reveal information that the individual is not even aware of, first the individual should be informed of the result of test and then he/she can decide (and bear the consequences of refusing) whether the result can be transferred to the employer as well. Attention was raised also to the fact that these tests may inadvertently reveal information which has no relation to the purpose of the processing: these data should be erased.

§2: Asking for information from applicants

Special attention will be paid to job interviews, as they provide the employer the possibility to pose a vast amount of questions to the applicant, thus learning a little more about his/her personality. While in practice the employer might even ask questions relating to the

[1168] ABI 814/A/2004-8.
[1169] NAIH-4001-6/2012/V. pp. 2-3.
[1170] ABI 2550/K/2007-3.
[1171] Péterfalvi 2012. pp. 298–299.

personal life of the applicant, *(A)* the previously presented data protection principles, such as purpose limitation or necessity, impose limitations to what kinds of questions can be asked. Following from the general labour law principles such as cooperation, *(B)* the applicant also has certain tools to protect himself/herself against the unlawful questions of the employer.

It was already addressed both in France and in Hungary what questions can be asked during a job interview, thereby determining the boundaries of personal and professional life, and according to my opinion, these observations provide a useful guidance when it comes to the protection of applicants' personal lives on SNSs, as the observations can be adequately applied to identifying this boundary on these online platforms.

(A) Job interviews

Naturally, the employer is interested in knowing all the essential information about an applicant, including his/her personality as well.[1172] During job interviews this information need is manifested in asking questions from the applicant: the employer is entitled and is required as well to pose questions.[1173]

In line with the data protection principles, these questions can relate to the employment relationship or checking the aptitudes necessary for the job.[1174] Therefore – just as it was the case when asking for information from the applicant – the questions must be connected to the professional life of the candidate, personal considerations should be excluded from the decision-making process. However, it is difficult to exhaustively define what the questions belonging to this circle are, as it is difficult to exhaustively define what falls under the notion of "competency" in this context.[1175] In France, a bulletin from 1993 provided certain clarification: the employer can obtain information relating to the applicant's competences, technical knowledge, adaptability, the ability to integrate into a team, etc.[1176]

Even though it is beyond the scope of the present monograph to examine this question in detail, certain similarities still have to be outlined between *discrimination* and privacy/data protection. Information belonging to the personal life of the prospective employee or being beyond the scope of purpose limitation and data minimization often overlaps with what constitutes protected characteristics in anti-discrimination law,[1177] and the more information employers gather, the more they can be exposed to discrimination claims.[1178]

Discrimination might appear in the form of discriminative questions during interviews (e.g. question relating to the potential pregnancy of the applicant), or also through obtaining

---

[1172] Bankó – Berke – Kiss 2017. p. 112.
[1173] Duquesne 2003. p. 58.
[1174] Hajdú 2005. p. 170.; Duquesne 2003. p. 58.
[1175] Arany-Tóth 2008a. p. 117.
[1176] Radé 2002. p. 184.
[1177] See these characteristics in: Article 1 of Directive 2000/78/EC; Section 8 of Act CXXV of 2003 on Equal Treatment and Promotion of Equal Opportunities; Article L1132-1 of the FLC; Article 1of the Act No. 2008-496 of 27 May 2008 on various provisions of adaptation to Community law in the field of the fight against discrimination.
[1178] Lory 2010. p. 38.

such information via SNSs.[1179] On SNSs users typically share information also falling under the scope of protected characteristics, such as religious or political view, relationship status, sexual orientation, etc.

One illustrative example is the case of *Gaskell v. University of Kentucky* from the US. The University of Kentucky created a hiring committee for the position of founding director for the university's astronomical observatory. Mr. Gaskell was the leading candidate, "clearly the most experienced" candidate and had "already done everything [the hiring committee] could possibly want the observatory director to do." However, the committee conducted an Internet search and found Mr. Gaskell's personal website, containing an article entitled *Modern Astronomy, the Bible, and Creation*. This article made the committee decide to hire another candidate, based on concerns relating to the religious views of Mr. Gaskell.[1180]

Discrimination in relation to SNSs is realised not only if the candidate's profile reveals protected characteristics: the *procedure* itself can also be discriminative – and therefore is to be avoided. These cases include when instead of inspecting equally every candidate's profiles, the employer decides to inspect the profiles of candidates pertaining to a certain race or to an age group.[1181] In addition to being discriminative, such a practice might also possibly infringe the data protection principle of fairness.

In Hungary, the *Equal Treatment Advisory Board* ("Egyenlő Bánásmód Tanácsadó Testület") already regulated what kinds of questions cannot be asked during a job interview: in 2007 they issued a resolution on the questions that can be asked during a job interview.[1182] In its resolution, the Equal Treatment Advisory Board emphasized that it is not possible to provide an exhaustive list of the questions that cannot be asked during a job interview because of being considered discriminative. The assessment of such questions must be based on a case-by-case basis, based on the given circumstances. Generally, it is prohibited to ask questions which are not necessary for assessing whether the potential employee is capable of performing the given job. By way of example, these include questions relating to the relationship of the applicant, to family life, to origins, to place of habitation, to sexual habits, to religious or to political views, etc. However, the Equal Treatment Advisory Board also draws attention to the fact that in some certain, exceptional cases the employer might be entitled to ask certain information relating to these matters.

In France the *Defender of Rights* issued a guide on how to recruit with the help of digital tools without discriminating. In the document attention was raised to SNSs, which are deemed to present an increased risk to the right of job applicants, especially when it comes to the inspection of personal SNS profiles – a common practice amongst recruiters. According

---

[1179] See the field experiment conducted by *Matthieu Manant*, *Serge Pajak* and *Nicolas Soulié* at Paris-Sud University, justifying the existence of obtaining information to be the ground of discrimination on SNSs. In their experiment they created two fictitious job candidates and sent their applications (with identical cover letters and résumés) to different companies. They also created profiles for these two candidates and indicated their hometowns and spoken languages, in which the two candidates considerably differed. While the first candidate was born in a French city, the second one was born in Marrakesh and spoke Arabic. This information was only available on Facebook, not in the CV. As a result of the field experiment, they found that the first candidate received 40 % more call-backs than the second one – which they thought is due to the subject's protected characteristic. Source: Manant – Pajak – Soulié 2014

[1180] Carlson 2014. pp. 484–485.

[1181] Byrnside 2008. p. 464.

[1182] Az Egyenlő Bánásmód Tanácsadó Testület 1/2007. TT. sz. állásfoglalása az állásinterjún feltehető munkáltatói kérdésekről

to the Defender of Rights, the employer's access to such sites presents a considerable risk to the applicant's rights and highly enables the employer to make a biased decision.[1183]

To conclude, the employer's questions fall into two groups: questions relating to personal life and to professional life. If the question relates to the personal life of the applicant, the employer must not ask it, apart from certain strict exceptions[1184] – thus ensuring the protection of the personal life of the applicant. However, if the question relates to the professional life, it is lawful to ask it. Although it is difficult to define a strict dividing line between these two spheres, as it was already seen, doctrine, data protection authorities and other institutions already gave numerous examples for these two categories, providing essential guidance.

(B) The "right to lie"

In case the employer does not respect the above limitations, the applicants have certain possibilities resulting from the general requirements set by labour law with the aim of protecting themselves against the unlawful questions of the employer.

The *HLC* contains a provision amongst the general requirements of conduct, declaring the obligation of cooperation.[1185] During the performance of rights and obligations, the parties are obliged to act mutually taking into account the other party's rights and interests.[1186] As a subset of this obligation of cooperation, the HLC also specifies the obligation to inform.[1187] In this regard, it states that the parties must inform each other concerning all facts, information and circumstances, and any changes therein, which are considered essential from the point of view of concluding the employment relationship.[1188] The *FLC* also declares the principle of good faith,[1189] moreover, it specifically states that the job applicant is required to answer truthfully to the employer's information requests.[1190]

In relation to job interviews, these obligations can be interpreted in such a way that the employee is obliged to answer questions that are directly related to the employment relationship –[1191] expressly stated as such by the FLC.[1192] It means that the candidate is expected to give the demanded information regarding his/her qualification, professional experience. The candidate must answer truthfully if the purpose of the question is to assess the aptitudes for the job, but if the question is not related to the employment relationship, he/she can refuse to answer or cannot be sanctioned if he/she has not given a truthful answer to the question violating personality rights.[1193]

[1183] Le Défenseur des droits 2015. p. 14.

[1184] For example: ideologically oriented enterprises or faith-oriented enterprises ("entreprise de tendance").

[1185] Subsection (2) of Section 6 of the HLC

[1186] Cséffán 2019. p. 19.

[1187] Gyulavári 2017. p. 74.

[1188] Subsection (4) of Section 6 of the HLC

[1189] Article L1222-1 of the FLC

[1190] Paragraph 3 of Article L1221-6 of the FLC

[1191] Bankó – Berke – Kiss 2017.

[1192] Paragraph 3 of Article L1221-6 of the FLC

[1193] Berke – Kiss 2014. p. 60.; Bankó – Berke – Kiss 2017. p. 61.; ABI 900/A/2006 and Le Lamy Droit Du Numérique 2014. p. 3. (Page number referring to the online version of the article downloaded from the website of the Cujas Library in Paris.)

It follows from the general requirement of conduct of cooperation and obligation of information, as well as from the applicant's right to privacy and right to data protection, enshrined in the labour codes, that in case the employer asks questions going beyond the lawful scope enounced above, the applicant is not in breach of the obligations imposed on him/her if he/she does not provide a truthful answer to them.[1194] All these rules provide the applicant the legal possibility to protect himself/herself against the unlawful questions asked by the employer during job interviews – recognizing the importance of such protection. However, in the case of SNSs, the scenario is different: instead of asking the question face-to-face from the applicant, thus providing the possibility whether to (truthfully) answer, in the case of SNSs the employer does not ask for the same information face-to-face, but checks it by himself/herself without the involvement of the applicant. Therefore, the applicant is unable to effectively protect his/her rights during SNS background checks.

Chapter 2: Social network sites and arising data protection questions

Part I. already presented the most important data protection requirements, which were laid down in the GDPR. However, obtaining personal data from SNSs raises certain challenges to these existing requirements, putting applicants' right to data protection at risk. Chapter 2 will present the arising data protection issues in relation to SNSs and recruitment and proposes answers to these questions.

Chapter 2 is composed of two parts: *Section 1* will discuss the most important principles of data processing, while *Section 2* will focus on issues relating to access and transparency. Here, a refinement must be made: although in Part I. access and transparency were mentioned among the data protection principles, here they are discussed under separate headings. The reason for this separation is due to the other principles being more relevant regarding the *content* available on SNSs, transparency and access rather relate to the *procedure* of conducting pre-employment SNS background checks.

Before addressing the legal issues specific to data protection, it must be examined whether data protection rules can apply to the phase of recruitment, and especially to (which) SNSs. According to certain public perceptions, once they posted information online, it should not come as a surprise to users of SNSs that this information is used, for example, in the hiring process.[1195] It cannot be emphasized enough that while privacy protection indeed might be affected by the behaviour of the user, data protection rules apply *regardless of* whether it was the user who published himself/herself the information.[1196, 1197]

[1194] Other authors only refer to the applicant's possibility to deny answering an unlawful question. (Gyulavári 2017. p. 134.) The wording chosen by *Mariann Arany-Tóth* also suggests the existence of a mere right to refusal. (Arany-Tóth 2008a. p. 125.) However, in my opinion, providing the possibility to the applicant to merely refuse to answer an unlawful question does not provide effective protection, as then the applicant would instantly have to face the consequences of the refusal, while in the case of being able to provide an untruthful answer, the employer would not even necessarily notice the applicant's act.

[1195] Flaherty – Whitmore 2013. p. 23.; Lory 2010. p. 37.

[1196] Dupuis 2013. p. 44.

[1197] The contrary might be true for questions asked during a job interview. According to an EU study, prepared by *Paul De Hert* and *Hans Lammerant*, the questions that are asked during an interview do not necessarily fall under the *scope of data protection law*, as they are not always processed by automated means or are not

The *material scope of the GDPR* applies to automated means of processing and to manual processing if the processed personal data are contained or are intended to be contained in a filing system,[1198] regardless of the methods used. Therefore, when processing takes place through SNSs, data protection rules apply. The *WP29* explicitly addressed the question of pre-employment and SNSs and stated in its Opinion 2/2017 that just because the personal data are made publicly available by the applicant, it does not mean that requirements, such as the legal ground, necessity, etc. would not apply to this kind of processing.[1199, 1200]

In 2016 the *NAIH* came to the same conclusion as the WP29 in its "Information notice on the basic requirements of data processing at work", emphasizing that data protection requirements – such as prior notification, necessity, respect of the chosen data protection settings – shall apply.[1201] In a case relating to employment background checks, similar conclusions were drawn, supplemented by raising attention to the arising data protection challenges, such as the enforcement of accuracy, lawfulness and the rights of the data subject.[1202] Therefore, SNSs during recruitment are subject to data protection regulations.

Section 1: Questions relating to data processing principles

Using SNSs to assess the suitability of job applicants poses several questions in relation to the enforcement of the data protection principles. These principles were already presented in Part I., which contains their more detailed presentation: here, brief reference will be made to their core attributes, then focus will be put on the SNS-specific questions. Although Title 1 focuses on the phase of recruitment, even at this stage it must be highlighted that the same or very similar data protection questions might arise in other phases of the employment relationship as well. As a consequence, what is going to be discussed in this Chapter might be adequately applicable to other phases.

(§1) Lawfulness and purpose limitation

Before addressing issues relating to the data quality principles, two preliminary questions must be discussed: lawfulness and the purpose limitation principle. As it was already examined in Part I., lawfulness requires the processing to be based on one of the six legal grounds: having a legal ground is an obligatory pre-requirement to any processing. The principle of purpose limitation is one of the most significant data processing principles,[1203] therefore reference to it must also be made.

---

intended to form part of a filing system. Even if that is the case, these questions are clearly related to privacy. De Hert – Lammerant 2013. p. 40.

[1198] Recital (15) of the GDPR; Paragraph 1 of Article 2 of the GDPR

[1199] WP29: *Opinion 2/2017*. p. 11.

[1200] The CoE also expressly refers to the importance of refraining from bypassing a candidate's (and employee's) chosen privacy settings and from collecting data without their knowledge through an intermediary, under another name or using a pseudonym. CoE: *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 2015. 5. 3. and CoE 2015. p. 7.

[1201] NAIH 2016. p. 19.

[1202] NAIH/2016/4386/2/V

[1203] European Union Agency for Fundamental Rights – Council of Europe 2018. p. 122.

(A) Principle of lawfulness

Under the GDPR, every data processing shall have a legal ground. According to *Edit Kajtár,* out of the six legal grounds regulated by the GDPR three might possibly be applied: consent, the necessity of processing in order to enter into the contract and the balancing between the rights of the individual and the data controller's legitimate interest. [(a), (b) and (f) of Article 6 of the GDPR][1204] The possible application of these legal grounds must be assessed.

One might ask the question: can the applicant consent to conducting an SNS background check? The GDPR reinforced the requirements towards *consent*, questioning its applicability in the employment context.[1205] One of the requirements of consent is to be freely given – which is not ensured in cases when there is a clear imbalance between the controller and the data subject.[1206] As a hierarchal relationship is present between job applicants and employers, consent does not seem to be appropriate when it comes to the lawfulness of pre-employment SNS background checks.[1207]

Another possible legal ground is the *performance of a contract*, when processing is necessary in order to take steps at the request of the data subject prior to entering into a contract: when without the processing of personal data the contract between the parties could not be executed, the processing of these data will be considered lawful.[1208] However, according to the WP29, *prior to entering into contract*, conducting a detailed background check following a candidate's application should not be understood as a necessary measure for entering into contract.[1209]

The application of the '*balancing test*' is also dubious, as it is the employer's legitimate interest to identify the best candidate possible, but he/she can achieve this purpose with less intrusive methods.[1210] Still, for the above-mentioned reasons, it seems to be the most appropriate legal ground applicable to the case of pre-employment SNS screenings.

(B) Purpose limitation

The purpose of pre-employment SNS background checks is the same as for the whole recruitment process: to identify the best applicant. Following from the freedom to contract, this purpose will be legitimate. As it was already addressed in Chapter 1, both the FLC and the HLC define the purpose of processing: the employer can only access personal data available on SNSs if it serves the purpose of assessing the professional capacities of the applicant. The applicant's personal life must not be subject to pre-employment SNS background checks. Pre-employment SNS background checks can serve this purpose, as

---

[1204] Kajtár 2015a. p. 100.

[1205] *Zsolt György Balogh [et al.]* are of the same opinion, though according to them consent as a legal ground was generally accepted by Hungarian doctrine. Source: Balogh et al. 2012a. pp. 16–17.

[1206] Recital (43) of the GDPR

[1207] However, according to the (previous) Hungarian literature, the voluntary nature of consent was present prior to concluding the employment relationship – erroneously according to my opinion. Athough these opinions did not address SNS background checks but the recruitment in general, especially the case of presumed consent when the applicant initiated the processing by applying for a position. Source: Balogh et al. 2012a. p. 16.

[1208] Péterfalvi – Révész – Buzás 2018. p. 123.

[1209] WP29: *Opinion 06/2014*. p. 18.

[1210] Kajtár – Mestre 2016. pp. 32–33.; Kajtár 2015b. p. 271.

information available on these sites can contribute to assessing the professional capacities of the applicant.

What have already been stated regarding the employer's legitimate interests during recruitment (identifying the best candidate) apply to SNSs as well, the purpose is unchanged. However, even with the existence of a legitimate purpose, processing can become unlawful if other data quality principles are not met. The following pages will focus on presenting the data quality principles that the employer must respect in addition to purpose limitation.

(§2) Data quality[1211] principle

The reliability of the information is closely connected to the data protection principles, but their enforcement during a pre-employment SNS background check is highly questionable[1212] – as it will be demonstrated in the following paragraphs. As it was referred to in the introduction, the principle of data quality means that "*[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*"[1213]

(A) Principle of data minimization

According to the *principle of data minimization*, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed,[1214] basically requiring that only the minimum necessary personal data shall be processed. The following paragraphs will deal with the two components of this principle: relevancy and necessity.

Relevancy is ensured by both labour codes through limiting recruitment methods to information which is connected to the professional life of the applicant. Although these provisions aim to protect applicants' personal lives by stating that during recruitment only necessary information relating directly to the professional capacities of the candidate can be processed,[1215] the implementation of this principle is quite challenging in the context of SNSs. Even though it is true that several types of personal data might contribute to assessing the applicant's professional aptitudes (e.g. verifying professional experience, communication skills, etc.), SNS profiles might also contain personal data directly relating to the personal life of the applicant – not fulfilling the requirement of relevancy.

The legal issue is that this "legally consultable" data (information relating to the professional life) and data not meeting the requirement of data minimization (information relating to personal life) are inseparable on the profile of the user.[1216] For example, the

---

[1211] "Data quality" is a reference to the OECD's data protection guidelines, and it means that "[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date." (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. Article 8)

[1212] Flaherty – Whitmore 2013. pp. 21–22.

[1213] *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. Article 8

[1214] Item c) of Paragraph 1 of Article 5 of the GDPR

[1215] Article L1221-6 of the FLC and Subsection (1) of Section 10 of the HLC

[1216] Kajtár 2015b. pp. 271–272.

employer might be entitled to access a candidate's profile in order to identify the best candidate, to verify information from the CV[1217] or to look for negative comments regarding the previous employer. However, at the same time he/she could automatically gain access to data which have no connection or relevancy to the legitimate purpose – e.g. relationship status, political opinion, hobbies, family members, etc.

This is a recent issue, as in the pre-SNS era this information usually would not have been available to the employer in the course of a traditional job interview. For example, while race, sex, age are (usually) evident when the employer conducts an interview, other factors (often available on SNSs), such as relationship status, political affiliation, etc. are typically not discovered through an interview (unless shared by the applicant or asked by the employer).[1218]

Any monitoring shall be proportionate and the least intrusive possible[1219] compared to the purpose of the processing. In the context of SNSs, the employer must also consider if he/she can obtain the desired information with less intrusive methods, whether the monitoring is truly needed, or the same result could be achieved through traditional forms of monitoring.[1220] It means that he/she must assess whether having a job interview, conducting a professional aptitude test, asking recommendation from the previous employer, or checking a professional SNS (e.g. LinkedIn) instead of a personal one would be a more privacy-friendly solution, which can still provide the necessary information.

Differentiation must be made between two types of personal data: personal data relating to the professional capacities of the applicant and personal data relating to his/her personal life. Regarding the first category, it must be assessed whether the traditional methods of recruitment (interview, tests, etc.) are capable of providing the employer the information sought. Regarding the second category, it was already established that SNSs might provide a glimpse into the user's personal life to an extent never experienced before.

Although the requirement of relevancy should limit employers to collecting personal data relating only to the professional life of the applicant, however, again, on SNSs it is technologically impossible to only collect this minimum necessary data, as the personal data which – in harmony with data minimization – could be collected and personal data not corresponding to this principle are *inseparable* on these sites.[1221] As a result, even if the employer accesses the applicant's SNS profile to obtain information fulfilling the data protection requirements, he/she might automatically gain access to personal data that he/she is not entitled to process.

An exception might be the use of professional SNSs (e.g. LinkedIn). Professional SNSs operate with the aim of providing the users the possibility to shape their online identities relating to their professional lives. Usually, users on these sites limit themselves to sharing personal data relating to their professional life (e.g. education, work experience, professional connections, etc.) – unlike on Facebook, Instagram and other personal SNSs. The *CNIL* is of the opinion that the use of professional SNS sites is allowed, as on these sites users provide only information regarding their

---

[1217] Kajtár 2015a. p. 101.
[1218] Byrnside 2008. p. 463
[1219] WP29: *Opinion 8/2001*. p. 4., p. 21., p. 25.; WP29: *Opinion 2/2017*. p. 7.
[1220] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 13.
[1221] Kajtár 2015a. p. 101.

professional lives. However, the employer is not entitled to search for the profiles on personal SNSs.[1222]

(B) Principle of accuracy

The principle of *accuracy* requires that personal data shall be accurate and, where necessary, kept up-to-date.[1223] Usually personal data are considered to be inaccurate if they do not correspond with reality and also if they are not complete or are embedded into the wrong context.[1224] These requirements are highly endangered in several regards when it comes to data obtained from SNSs. *First*, it will be examined whether the applicant himself/herself can be correctly identified during pre-employment SNS background checks. *Second*, it will be addressed whether the author of the content can play a role in relation to accuracy. *Third*, questions relating to the possible conclusions drawn from the content itself will be addressed. *Then*, the time factor, up-to-dateness will be examined.

First, the principle of accuracy can be very important regarding the *identification of the job applicant*. Identifying the right applicant is crucial in order to avoid situations where the employer finds the wrong candidate[1225] and the prospective employee is mistakenly associated with the SNS activity of someone else. This scenario can happen for several reasons: especially if the applicant has a very common name (e.g. Kovács Péter or Pierre Martin) and/or there is no other publicly available personal data (e.g. profile picture) which can help to correctly identify him/her.[1226] Associating the online activities with the wrong individual unquestionably infringes the principle of accuracy.

Second, the employee might not have been the *author of the given content* – a profile can be hacked by a third party: for example, *Sherry D. Sanders* describes a hypothetical situation where an applicant's Twitter profile is hacked: the hacker posts racist comments in the name of the applicant – which the applicant does not see, as he has not accessed his Twitter account for months.[1227] Besides hacking, even friends or colleagues can post, as a prank, in the name of the applicant (for example, if he/she leaves his/her device unattended): see, for example, the case of an employee of a security company whose *colleagues* uploaded a video of him to his Facebook page, showing him demonstrating his physical competences on a floor of the European Commission only reserved for commissioners – and was dismissed as a consequence.[1228] In extreme cases even fake profiles can be created: *Ian Byrnside* describes the phenomenon of college students intentionally creating fake profiles of others

---

[1222] https://www.cnil.fr/fr/cnil-direct/question/354 (Accessed: 21 December 2019)
A proposed *German bill* (though rejected in 2013) reached the same conclusion, by making a distinction between personal and professional SNSs, prohibiting the access to the first category, but permitting access to the second one. Kajtár – Mestre 2016. p. 36.

[1223] Item d) of Paragraph 1 of Article 5 of the GDPR

[1224] Rücker – Kugler 2018. p. 68.

[1225] Tenenbaum 2012. p. 13. *Jason Tenenbaum* googled himself and found out that typing "Jason Tenenbaum" into Google returns results for another attorney from a neighbouring town – providing the possibility to easily mistaken the two persons.

[1226] Flynn 2012. pp. 20–21.

[1227] Sanders 2012. p. 243.

[1228] Lambert 2014. p. 230.

who are considered to be competition, containing unflattering information – ruining his/her chances of finding employment.[1229]

Third, processing personal data obtained from SNSs can often lead to the misinterpretation of the personal data. It is highly questionable how/whether the employer can make reliable conclusions from accessing candidates' SNS profiles. *Teresa Coelho Moreira* illustrates how certain information can have dubious interpretation, therefore contradicting the principle of data quality. For example, there are several ways for the employer to interpret the fact that certain candidates are available on these sites, while others are not (do those present on these sites have more developed skills relating to technology or are the others more conscious regarding privacy issues?), or that an applicant likes to travel (is he/she flexible or rather unreliable?).[1230]

Also, often the information originally posted was intended for a different audience,[1231] and although in a legal way it does not exempt the user, it constitutes a problem that users may not be aware of the functioning of SNSs and may be mistaken regarding the public or private nature of the published content,[1232] publishing something presuming that it would be accessible only to a narrow circle of users – e.g. only to friends –, but not to the employer. Personal data available on these sites can be inaccurate, incomplete and easily interpreted out of context, thereby giving a false impression of the user.[1233] As a result, the quality of personal data is not guaranteed.[1234]

Fourth, up-to-dateness: in the context of recruitment, up-to-dateness means that a decision should not be based on outdated information. However, it must be seen that the Internet does not forget – it is also true in the case of SNSs: on SNSs information is often available dating back years. This principle also has a close connection with the *right to be forgotten*.

If personal data are outdated, the requirements of relevancy and accuracy are more easily infringed. A prospective employee might have loved partying wildly at a younger age and might have provided a rich documentation of this activity on Facebook – bearing no relevancy with regard to his/her professional aptitudes years later. People are able to change and to develop, but the unforgettable (and unforgivable) nature of the Internet might stigmatize them and might not let them change and "escape" from their past mistakes or their past selves. For example, a funny photo taken in high school years ago or a compromising content can have an impact on the future carrier options even if it is not relevant anymore.[1235] Five seconds eternalized on the web can define someone's whole Internet presence.[1236]

[1229] Byrnside 2008. p. 471.

[1230] Moreira 2013. p. 77.

[1231] In the age of SNSs, when everyone equipped with a smartphone may feel as a celebrity, online profiles do not reflect the professional capacities of a user. Source: Ghoshray 2013. p. 572.

[1232] See more in: Sprague 2011. p. 15.; Kajtár – Mestre 2016. pp. 24–25.

[1233] Ghoshray 2013. pp. 562–563.

[1234] Szabó 2010. pp. 58–59.

[1235] On the importance of forgetting see Mayer-Schönberger 2011. and Székely, Iván: *Jog ahhoz, hogy elfelejtsenek és töröljenek*. Információs társadalom, 13(3–4), 2013. pp. 7–27.

[1236] In the US, *Lindsey Stone* was fired after her colleague posted a photo to Facebook, showing Ms. Stone engaging in disrespectful behaviour (giving a finger and imitating a scream) in the Arlington National (military) Cemetery – next to a sign asking for silence and respect. According to her, she did not think, it was just part of an inside joke between her and her colleague. However, the firing was not the only negative outcome for Ms Stone: the photo went viral and she became the target of extremely hostile comments from the Internet community. Since then, she started working for a new employer, but said that she was terrified that the new

Since the wide adoption of SNSs, years have passed, leading to the phenomenon that certain (early) users possess a digital footprint on these platforms dating back years. The right to be forgotten aims to ensure that individuals can "escape" from their online past.[1237] It is alarming that especially young users have the tendency to share the most intimate details of their personal lives.[1238] However, following from the very nature of the SNSs' function, the documentation of these "reckless" young years permanently stays on the Internet. Accessing that past information might lead to the consequence that the employer draws present conclusions from the past, which may lead to coming to incorrect conclusions.[1239]

In conclusion, data quality principles are highly at stake when it comes to processing information obtained from applicants' SNS profiles – possibly raising the question of completely banning these searches, as it will be discussed later. It means on the one hand that the applicants' rights can be easily infringed, and on the other hand that the employer can easily base his/her decision on unreliable data. These issues mainly arise on personal SNSs, which contain more information relating to personal life due to their nature.

(§3) Conducting the background checks

In order to find a right balance between the employer's interest of choosing the best applicant and the applicant's rights, it is important that if the employer decides to conduct an SNS background check, he/she follows a systematic approach instead of performing it in an *ad hoc* way. Drafting internal policies, providing trainings and documenting[1240] could be useful means to achieve this objective. On the following pages the scope of the information to be viewed, the procedure in which they should be treated and the question of who should conduct these background checks will be discussed.

It was proposed on several occasions[1241] that the employer should only access professional SNSs, but access to personal SNSs should be prohibited. Through legitimizing the consultation of only professional SNSs – and banning that of personal SNSs –, it could be achieved that the personal life of the applicant is left unaffected by the screening, while the professional profiles can help the employer better judge the professional capacity of the applicant. However, as it will be discussed in §2, prohibition in itself is not considered to be an effective solution, as because of the invisibility of such searches, the technical feasibility of such prohibition is highly questionable.

Time factors must also be taken into consideration: to handle the challenges relating to outdatedness and to the right to be forgotten, – in a joint publication with *József Hajdú*,

---

employer would find out about what had happened in the cemetery. "*Those five seconds of her life is her entire Internet presence[.]*" https://www.theguardian.com/technology/2015/feb/21/internet-shaming-lindsey-stone-jon-ronson (Accessed: 3 May 2018)

[1237] https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (Accessed: 13 August 2019)

[1238] Mayer-Schönberger 2011. p. 3.

[1239] As an illustrative example see the hypothetical scenario in which an individual's whole online presence was determined by a 2-minute-long interview in which he expressed his controversial opinion on a certain topic. Source: Ghoshray 2013. p. 555.

[1240] Brown – Vaughn 2011. pp. 223–224.

[1241] https://www.cnil.fr/fr/cnil-direct/question/354 (Accessed: 21 December 2019) and a proposed German draft bill from 2010: Source: Kajtár – Mestre 2016. p. 36.

Viktória Lechner and *Attila Turi*[1242] – we recommended as a *de lege ferenda* suggestion to introduce a time limitation period for the processing of personal data originating from SNSs. It would mean that in accordance with the general limitation period in labour law,[1243] posts, pictures and other contents published to SNSs before that period should not be processed in the recruitment process.

If the employer decides to conduct pre-employment SNS screening, he/she should do it through a fair and uniform procedure. Case-by-case or discriminatory screenings are to be avoided.[1244] If for a position a screening is required, each applicant should be screened, preferably at the late stage of the selection process in order to minimize the number of applicants screened.[1245] SNS pre-employment screenings should not be conducted on a general basis. Their application should be limited to those cases when they are truly necessary, for example, when the nature of the given job or the type of employer justifies it (e.g. it is more probable that background checks can be justified if the position comes with high responsibility). Prior to the screening, objective criteria should be established in relation to what exactly the employer aims to know about the applicant (For example, are there spelling mistakes on the profile? Is there content promoting hatred? Are there negative comments regarding the previous employer?) – in accordance with the principle of relevancy.

In order to solve the problem of the inseparability of personal and work-related information, it is advisable that a third party – who will not participate in the decision-making – conducts the background check and transmits only the work-related information to the decision-makers.[1246] Thus it can be avoided that the decision-maker would make the decision based on personal data not fulfilling the criteria of data minimization and proportionality.

In this regard, the proposition of *Nathan J. Ebnet* might be relevant to French and Hungarian law, despite being recommended in the first place to US law. He recommends the use of third-party background screening service. He cites the example of Social Intelligence:[1247] a company offering to conduct pre-employment online background checks in accordance with the legal regulations in force.[1248] According to the description on Social Intelligence's website, they primarily search for and flag user-generated content in the field of (a) racist, sexist, or discriminatory behaviour, (b) sexually explicit material, (c) threats or acts of violence and (d) potentially illegal activity. At the end of the process the employer can review the report which contains examples of the negative content found, but none related to protected characteristics or private information with no connection to the job. If no negative information is found, the report will state that "No Pertinent Information"

[1242] Hajdú, József et al.: *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), forthcoming

[1243] In Hungary the general limitation period is 3 years [Subsection (19) of Section 286 of the HLC]. In contrast, French regulation contains several limitation periods: which seems to be the most relevant is 5 years in case of discrimination. (Article L1134-5 of the FLC)

[1244] Brown – Vaughn 2011. p. 223.

[1245] Information Commissioner's Office 2011. p. 23.

[1246] Peebles 2012. pp. 1428–1429.; Sprague 2011. p. 32.

[1247] https://www.socialintel.com/(Accessed: 13 August 2019)

[1248] https://www.washingtonpost.com/lifestyle/style/more-employers-using-firms-that-check-applicants-social-media-history/2011/07/12/gIQAxnJYGI_story.html?noredirect=on&utm_term=.1506923db7c6 (Accessed: 16 August 2018)

was found.[1249] Although *Ebnet* admits that involving a third party in the background check comes with extra expenses to the employer, he believes that the efficiency of these searches would transform this expense into an investment.[1250]

In addition to involving an independent third-party in the recruitment process, he also suggests adopting elements from the already existing US Fair Credit Reporting Act, covering credit reports.[1251] Namely, he recommends to require the prior approval of applicants of such a screening taking place and to notify applicants if an adverse decision is made.[1252] Therefore transparency would be ensured and applicants would have the possibility to explain certain compromising content. He argues that through the adoption of these measures, an adequate balance can be found between the employer's legitimate interests and applicants' rights.

Another type of third-party intermediary was suggested by *Peter Baumhart*. In response to the growing phenomenon of employers asking for applicants' passwords, he suggests the involvement of an information escrow agent in the pre-employment background check. The information escrow agent would act as an intermediary between the parties to whom applicants could disclose their passwords and employers could provide a list of information that needs to be flagged.[1253] The employer would only receive the red flags relevant to the employment and no other irrelevant information. While the intrusion into the applicant's privacy exists, it is present to a lesser extent compared to the situation when the employer asks for the password.[1254]

Although it would be incompatible with French and Hungarian laws to legitimize a system where the applicant should provide his/her login credentials, some elements of these two solutions might be adapted to the legal system. The idea of involving an intermediary into the recruitment process could and should be adequately implemented – although it would be better suited in the form of a third-party background screening service. With the participation of these third parties it could be prevented that the employer accesses data irrelevant to the employment – eliminating the issues in relation to the inseparability of professional and personal life during pre-employment SNS background checks.

Section 2. Access and transparency of processing

As data protection requirements apply even if the information was publicly made available by the applicant and is easily available, the employer still must inform applicants that an SNS background check might take place. It should be indicated prior to the recruitment – for example, in the job advertisement – that an SNS background check will be conducted during the selection process, and it should state precisely which sites will be checked

---

[1249] https://www.socialintel.com/how-it-works/ (Accessed: 16 August 2018)

[1250] Ebnet 2012. p. 327.

[1251] The Fair Credit Reporting Act was adopted in 1970 and aims to regulate the collection and reporting of credit information about consumers, with the purpose of ensuring accuracy of the information collected. Ebnet 2012. pp. 312–314.

[1252] Ebnet 2012. pp. 326–327.

[1253] Baumhart 2015. pp. 524–525.

[1254] Baumhart 2015. pp. 526–527.

and what the lawful information that the employer aims to obtain is.[1255, 1256] However, in practice, this principle is often violated especially due to the *(§1)* invisibility of such searches. Besides transparency, it has also importance *(§2)* how the employer can gain access to the information.

(§1) Access and transparency

According to the *principle of direct collection*, it is desirable that when it is possible, employers collect personal data directly from the individual concerned.[1257] Although even before the expansion of SNSs the employer had different possibilities to obtain personal data *not* directly from the prospective employee (e.g. investigation, asking the previous employer for recommendation), with the advent and expansion of SNSs it has become considerably easier to collect personal data not directly from the data subject.[1258] This fundamentally affects the ways of accessing personal data, giving room on the one hand for *(A)* invisible searches and on the other hand for *(B)* searches bypassing the individual's choice of privacy settings. These new ways of access also have serious implications for the transparency of processing.

(A) Invisible background checks

The principle of transparency is highly at stake, as these SNS background checks often stay invisible for the applicant. What is meant by invisible background check is the employer accessing the publicly available profiles of the applicant – without his/her awareness. Often – depending on the (non) use of privacy settings – gaining access to a job applicants' profile is effortless and provides access to a wide amount of personal data. For example, the employer/recruiter might access the applicant's profile from outside of the SNS (if the privacy settings are set to public), or (if the privacy settings make the content available to other users) he/she can have access to the candidate's profile from his/her or the company's profile. Either way, access is fast, easy to conduct and cost-effective – and the individual is not necessarily aware of the conducted search.

Theoretically, labour law and data protection provisions are able to adequately regulate pre-employment SNS screenings. However, their enforcement in practice is highly problematic, as these screenings stay undetected,[1259] often applicants are not aware that an adverse decision was based on an SNS background check. In practice, they (or DPAs) have limited chance to find out about the existence of such searches: for example, it might be possible that the applicant discovers the existence of a background check during the job

---

[1255] Mikkelson 2010. p. 6.

[1256] NAIH 2016. p. 19.

[1257] This principle is enshrined in the CoE: *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*. 2015. 5. 1.: "*Employers should collect personal data directly from the data subject concerned. When it is necessary and lawful to process data collected from third parties, for example, to obtain professional references, the data subject should be duly informed in advance.*"

[1258] Kajtár 2016. p. 149.

[1259] Pók 2012. p. 13.

interview, for example, if an employer asks questions about an event that he/she learned during an Internet search.[1260] Still, besides these extreme cases, it is quasi impossible for the applicant to prove (or know) that the decision was based on the content found on SNSs.[1261]

As a result, the legal issue is that the job applicant might not even be aware of the fact that a processing takes place – which is contrary to the requirement of *transparency*. Knowing about the existence of a processing is a precondition to exercising the rights of the data subject. In the case of invisible searches, the applicant will not know what data the employer has access to, how he/she will interpret that information: the requirement of prior information and the principle of transparency guaranteed by the data protection regulation will be infringed.

Transparency is closely related to the exercise of the *rights of the data subject*: it follows from the invisible nature of these searches that the job applicant cannot participate in the data processing and cannot exercise his/her rights relating to data processing, as he/she might not even know about the processing. In addition, because of the high unreliability of personal data collected from SNSs, the infringement of rights might be considerable. Due to the challenges relating to the principle of accuracy, it is very easy to misinterpret those data, as they are taken out of context – and the user has no chance to participate in the processing.[1262] The information vulnerability of the job applicant might be considerable, therefore ensuring his/her participation in the processing and guaranteeing the exercise of the above-mentioned rights is crucial. If the true participation of the data subject through informing him/her about the existence of the screening and the exercise of the data subjects' rights are ensured, compliance with data protection regulation is realized, as a consequence of which the hiring decisions could be based on reliable data more effectively, thus serving the purpose of identifying the best candidate.

Providing prior information to applicants is crucial in ensuring the transparency of processing. However, as *Attila Péterfalvi [et al.]* noted, if providing prior information can jeopardize the principle of accuracy, the information should be kept to the necessary extent.[1263] The employer should inform employees that an SNS background check will be conducted during the selection process, state precisely which sites will be checked and what the lawful information that the employer aims to obtain is.[1264] Also, a contact should be provided to applicants, where they could turn in case they wanted to exercise their rights

---

[1260] https://blogs.harvard.edu/infolaw/2006/11/15/finnish-employers-cannot-google-applicants/ (Accessed: 2 July 2018) Although the article did not detail it, in my opinion revealing the existence of a background check might be possible through accidentally seeing documentation, or by the interviewer asking questions that without a background check would not have been asked.

[1261] Kajtár 2015b. p. 278.

[1262] See, for example, the case of *Nathalie Blanchard*, who was diagnosed with major depression and went on sick-leave. However, all of a sudden, her insurance company cut her benefits because they saw photos of her on Facebook, in which she went to the beach, had fun with her friends, and went to bars. Therefore, the company judged that she is not sick anymore. However, what was not known to them was that Ms. Blanchard performed these activities on her doctor's orders, as part of her healing process. Source: http://www.cbc.ca/news/canada/montreal/depressed-woman-loses-benefits-over-facebook-photos-1.861843 (Accessed: 3 May 2018)

[1263] Péterfalvi 2012. p. 299. However, such statement might raise the question whether in relation to SNSs employees can alter the result of the background checks by taking certain steps (e.g. applying privacy settings) and hindering access to the profile.

[1264] Mikkelson 2010. p. 6.

of data subject. Applicants should be given the possibility to consult and if necessary, to rectify the personal data processed.

(B) Other ways of access

Invisible searches are not the only way to access data on SNSs although they constitute the most evident way of access. Other, more intrusive practices exist which can provide the employer access to a candidate's profile. Among these "other ways of access" differentiation is made between two groups: obtaining access to content available to other users and obtaining access to content available to the user himself/herself.[1265]

The employer might obtain access to content available to other users. Under this category it is supposed that the applicant has used privacy settings and made steps towards concealing information from certain categories of users and the employer would like to bypass those settings and gain access to more information than by default he/she is allowed to. He/she can do so by friending the applicant, asking the applicant to change the privacy settings or ask a friend of the applicant who is employed at the workplace to provide access through his/her own profile. The employer might also obtain access to content available to the user himself/herself. In this case the interference in the applicant's private life is more serious, as through these means the employer can access an extremely wide circle of information – even those only available to the data subject. In the most serious case *hacking* might also be imaginable.[1266] During a job interview the employer might ask the applicant *to log in* to his/her profile and "show the employer around" or can ask for the applicant's *password*.

Asking for applicants' *password* is not an uncommon phenomenon,[1267] especially in the US, where the States enacted several password protection acts in order to ensure the protection of applicants' rights.[1268] As an illustrative example, see the hiring policy of the city of Bozeman in the US, resulting in a public outcry. In 2009 the Bozeman Daily Chronicle aired an article describing the excessive online pre-employment background checks conducted by the city. For years, the city systematically asked prospective employees to provide their login credentials (username and passwords) to SNSs they were present on as part of their general recruiting practice.[1269] In these cases, the applicant's right to respect for private life is infringed as the employer gains access to information that the applicant intended to conceal from him/her or even not to publicly share with anyone (e.g. chat

[1265] The ways of accessing that are grouped into these two categories are from: Engler – Tanoury 2007. pp. 65–66.; Park 2014. p. 790.

[1266] That was the case of a Finnish employer, where two managers intercepted an employee's private communication on Facebook and were accused of hacking and were finally sentenced. Lambert 2014. pp. 307–308.

[1267] Reacting to this emerging issue, even Facebook published an announcement in which it encouraged applicants/employees not to provide their passwords to the employer and called upon employers not to ask for passwords. https://newsroom.fb.com/news/2012/03/protecting-your-passwords-and-your-privacy/ (Accessed: 13 August 2019)

[1268] This was especially a concern in the US. Against these phenomena various password protection acts were enacted. See more in: Sprague, Robert: No Surfing Allowed: A Review & Analysis of Legislation Prohibiting Employers from Demanding Access to Employees' & Job Applicants' Social Media Accounts. *Albany Law Journal of Science and Technology*, 24(3), 2014. pp. 481–513. and Del Riego – Sánchez Abril – Levin 2012. pp. 1., 18–26.

[1269] https://www.bozemandailychronicle.com/news/city-requires-facebook-passwords-from-job-applicants/article_a9458e22-498a-5b71-b07d-6628b487f797.html (Accessed: 3 May 2018)

messages). Also, by using the privacy settings and customizing access to the content, the applicant exercises his/her right to informational self-determination – which is bypassed by the employer.

From a *data protection* viewpoint, bypassing the privacy settings is not compatible with EU or national legislation either. The CoE, the WP29 and the NAIH all stated that only the publicly available personal data can be used in the recruitment process,[1270] while the CNIL completely excluded personal SNSs from the process:[1271] therefore no corresponding legal ground can be found in these regulations. In addition, it constitutes a problem that when the applicant is requested to act (accept friend request, change the privacy settings, log into or provide password), the *hierarchal* relation between the parties poses a challenge. If the applicant complies with the request, the voluntary nature of this act is highly questionable. When instead of the applicant, a common friend, an employee is asked to provide access through his/her own profile,[1272] the drawbacks of the hierarchal relation are manifested between the employee and the employer. In the latter case *transparency* issues might also arise, as the applicant is not necessarily aware that an employee provided access to his/her profile.

(C) Regulating instead of prohibiting

Title 1 is based on the assumption that instead of prohibiting the conduct of pre-employment SNS background checks, they should rather be regulated. Certain steps were made towards prohibiting SNS background checks: in *France* an agreement was signed between different professional associations, aiming to achieve that employers do not use search engines and SNSs for recruitment.[1273] Others differentiated between personal and professional SNSs: the *CNIL* also expressed that personal SNSs should not be consulted in the recruitment process as they reveal a multitude of information pertaining to the private life of the applicant.[1274] A *German* draft bill from 2010 adopted the same position and prohibited access to personal SNS profiles, while allowing to use information from professional SNSs.[1275] In *Finland*, due to the principle of direct collection, it is forbidden to google applicants[1276] or to perform an SNS background check.[1277]

[1270] CoE: *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 2015. 5. 3. and CoE 2015. p. 7.; NAIH 2016. p. 19.

[1271] https://www.cnil.fr/fr/cnil-direct/question/354 (Accessed: 21 December 2019)

[1272] In a Belgian case in 2011 the employer gained access to an employee's account by asking another employee to communicate him a certain content. Lambert 2014. p. 230.

[1273] https://www.michaelpage.fr/sites/michaelpage.fr/files/Charte_rxseaux_sociaux_internet_vie_privxe_et_recrutement.pdf (Accessed: 13 August 2019)

[1274] https://www.cnil.fr/fr/cnil-direct/question/354 (Accessed: 21 December 2019)
This standpoint is further nuanced by doctrine: *Caroline Fel* and *Emmanuel Sordet* argue that if the applicant's SNS profile is accessible to the public, his/her right to privacy is not infringed if the employer accesses the profile. Fel – Sordet 2010. p. 22.

[1275] Finally, for reasons of lack of consensus, the proposed bill was rejected in 2013. Source: Kajtár – Mestre 2016. p. 36.

[1276] https://blogs.harvard.edu/infolaw/2006/11/15/finnish-employers-cannot-google-applicants/ (Accessed: 2 July 2018)

[1277] https://www.lexology.com/library/detail.aspx?g=b03caa90-2830-4194-a967-6cceaa561e7e (Accessed: 17 July 2018)

In contrast to the opinions arguing that SNS background checks should be prohibited, other solutions welcomed the *regulation* of SNS background checks, instead of prohibiting them. It was already discussed that the *WP29* expressed how the data protection requirements shall apply to SNS screenings,[1278] indirectly implying that these searches are not prohibited. In the UK, the *Information Commissioner's Office's* (hereinafter referred to as: ICO) Employment Practices Code, instead of banning these searches, laid down the requirements towards pre-employment vetting, such as notifying applicants.[1279] In 2016 the *NAIH* in its "Information notice on the basic requirements of data processing at work" argued that it would not be reasonable to prohibit the use of SNSs in the recruitment process.[1280] The NAIH also noted that it is permissible to make conclusions from the profiles but further processing operations such as making copies of the profile, storing or transferring it are prohibited.[1281]

Even though banning pre-employment SNS screenings would indeed constitute a straightforward solution and in theory would eliminate all the data protection challenges discussed throughout Title 1, in practice this solution seems unreasonable because of the invisibility of such searches and because of its benefits.[1282] Due to the ease and the invisibility of these searches, in practice it seems to be more effective to allow conducting them while providing guidance on how to comply with the data protection requirements than completely prohibiting such screenings – also corresponding better with the reality of social media. Regulated SNS pre-employment background checks could contribute to ensuring accessibility, accuracy, relevancy and other principles,[1283] thus respecting individuals' rights to a greater extent – in contrast to "clandestine" searches. However, as even in the case of regulation these searches stay invisible and evade enforcement, one might ask why regulation would be a better solution when prohibition is judged to be ineffective.

Employers as well are interested in conducting background checks in accordance with data protection requirements. It would be necessary and welcomed that employers realize that it is also in their own interest to comply with the data protection regulation for two reasons. *On the one hand*, in the case of non-compliance with the data protection requirements, they can face various consequences in which the GDPR has become more severe: they can face administrative fines up to 20 million euros, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover.[1284] However, because of the invisibility of these searches, this scenario has little practical relevance.

On the other hand, the issues relating to the data protection principles highly question the relevancy, necessity, reliability, up-to-dateness and accuracy of the obtained data. If no safeguards are applied during the screenings, this practice could be counterproductive in choosing the best candidate possible. This means that not only prospective employees' rights might be infringed but the employer would base his/her decision on unreliable data. Because of invisibility, it is of key importance that employers realize that – in addition to respecting applicants' rights – it also serves their own interests to comply with the data protection regulation and avoid screening in an inefficient or illegal way. If the employer

[1278] WP29: *Opinion 2/2017*. p. 11.
[1279] Information Commissioner's Office 2011. p. 23.
[1280] NAIH 2016. p. 19.
[1281] NAIH 2016. p. 19.
[1282] Kajtár – Mestre 2016. p. 38.
[1283] Ebnet 2012. p. 326.
[1284] Article 83 of the GDPR

is aware of these potential risks and proceeds accordingly, these risks can be eliminated.[1285] Ensuring the participation of the applicant and considering that too much information does not necessarily help making the decision can be the means to achieve that.[1286]

(§2) Role of the applicant

Although it is the employer who is in a more dominant position as he/she defines the methods used during the recruitment, leaving no decision-making position for the employee, and conducts the background check himself/herself, it is important to realize that applicants can also take steps towards ensuring the protection of their rights in the 21st century. Although data protection applies irrespective of whether the applicant is oversharing or posting once in a lifetime, applicants can also take further steps in order to actively practice their right to informational self-determination and they can highly contribute to preventing the occurrence of negative consequences in the hiring process: both in the field of preventing the rise of these issues and also in detecting them after they have occurred.

(A) Increased consciousness during the use of SNSs

Through the adoption of a more conscious behaviour while using and posting to SNSs – in accordance with the right to informational self-determination requiring data subjects to be an active part in the processing –, applicants can increasingly contribute to the protection of their rights – while still enjoying the possibilities provided by SNSs. With such conduct, the major part of problems might even be *prevented*.

Concerning *the appropriate audiences*, the use of privacy settings is a crucial point. The CNIL emphasizes the importance of actively managing the privacy settings in order to control which audiences can have access to the content on their profiles.[1287] For example, Facebook gives users the possibility to use differentiated privacy settings – in theory it is possible that every friend of the user has access to a different content on the profile.[1288] By effectively using the privacy settings, it would be possible to shape the online identity into an "employer-friendly" version, where the employer (or users with whom the employee is not friends) can only have access to one part of the profile – for example, to a part only containing professional information, while access is reserved to the closest friends of the user.

Even though 100 % safe protection does not exist, and a very determined employer can somehow bypass privacy settings, most employers encountering the barriers imposed by data protection settings would not start to hack the profile in order to gain access to it. Even with such minimal precaution a considerable part of the problems – except for the extreme cases – could be successfully prevented.

[1285] Byrnside 2008. p. 471.

[1286] Byrnside 2008. p. 474.

[1287] https://www.cnil.fr/fr/maitriser-les-informations-publiees-sur-les-reseaux-sociaux (Accessed: 26 February 2017) and Cornesse 2011. pp. 52–53.

[1288] To stay with the example of Facebook, before sharing something, the applicant should think over what the right form for the given content is: would he/she want to share – for example, holiday pictures – in an album accessible to all Facebook users, or "only" to all of his/her friends, to his/her closest friends or in a private group destined for communication with the closest friends, or in a private message, etc.?

Besides applying at least basic privacy settings, it is crucial that the applicant should be aware of what kind of information he/she shares and with which audience. Regarding *the content shared*, at the 30th International Conference of Data Protection and Privacy Commissioners it was advised that SNS users carefully consider what kind of personal data they publish on these sites and whether they publish any personal data to these sites. They should not forget that they might be later confronted with that information in a different context, for example, in a hiring process.[1289] Also, privacy is a collective matter: what a user does might affect another user.[1290] In the age of Web 2.0 individuals do not owe a perfect control over their online presence.[1291] Even if someone is conscious regarding his/her e-reputation, other users can publish information relating to third parties. It is important that users should refrain from publishing personal data relating to other users without their consent (e.g. pictures and tagging).[1292]

Although the use of privacy settings can provide certain protection, it is safer if users do not rely heavily on them and, in addition, carefully think over whether to post or not to post.[1293] There exists a so-called Grandmother rule, which can help users to judge the appropriateness of material published on SNSs: according to this rule, users should only share information on SNSs that they would feel comfortable to share with their grandmother.[1294]

(B) E-reputation and awareness

Managing e-reputation[1295] does not consist simply of the single act of abstaining from posting certain content: it should be continuously monitored. Even if the individual himself/herself does not use SNSs, it is recommended to monitor possible online presence in order to be able to detect any possibly compromising information and take the necessary steps. In order to promote such behaviour, raising awareness is crucial, so that individuals can have knowledge of the possible risks and adopt a more conscious behaviour.

The user should also control his/her digital identity by monitoring what information is available regarding him/her on the Internet – for example, typing his/her name into a search engine in order to monitor whether third persons have posted information relating to him/her.[1296] Such content could have been posted by the individual or by other parties (see, for instance, the example of creating fake profiles for competition), or can simply give results of individuals sharing the same name. Not only information published by third parties should be monitored: regularly reviewing the content previously published by the user himself/herself (e.g. pictures from years before) and removing what is not relevant any more can also play an important role.

[1289] 30th International Conference of Data Protection and Privacy Commissioners 2008. p. 2.
[1290] http://www.danah.org/papers/talks/2011/PDF2011.html (Accessed: 28 February 2017)
[1291] Szabó 2010. p. 58.
[1292] 30th International Conference of Data Protection and Privacy Commissioners 2008. p. 2.
[1293] Pók 2012. p. 13.
[1294] Byrnside 2008. p. 474.
[1295] According to the CNIL, e-reputation is the online image of the individual, composed of every piece of information relating to the individual available online, e.g. blog, videos, photos either published by the individual or by others. https://www.cnil.fr/fr/le-reputation-en-questions-0 (Accessed: 4 April 2017)
[1296] https://www.cnil.fr/fr/le-reputation-en-questions-0 (Accessed: 4 April 2017)

If the applicant is aware of the content which the employer might have access to, he/she can make the necessary steps to remove that content.[1297] Either he/she can ask the third party to remove the content, or can report it, or can even use online reputation management services. These online reputation management services help users track, verify online information or shape online personas.[1298]

In order to ensure the active and effective participation of individuals, it is crucial that *individuals are aware* of the basic functioning of these sites, the issues in relation to their right to data protection and the possible consequences of the use of SNSs. As an example, in France, the CNIL takes very forward-thinking steps in informing users on what behaviour they should adopt in order to take steps to protect their own privacy. They actively engage in social media and promote their activity. They publish information notices, informing users in a plain, concise language on their rights or on how to protect them. Two documents relate directly to the subject of the present Chapter: an article entitled "Job applicants: protect your own reputation on the web!"[1299] and a poster entitled "10 pieces of advice to stay clean on the web."[1300, 1301] The first document aims directly job applicants and includes pieces of advice, such as think before posting, manage e-reputation, highlight content that puts the user in a favourable light, pay attention to tags and to privacy settings. The second document is more general and provides practical advice to users of the Internet, such as the use of privacy settings, respecting the privacy of others, managing e-reputation, using several e-mail addresses and pseudonyms, choosing passwords, etc.

In contrast to this active, awareness raising activity of the CNIL, in *Hungary*, the NAIH has room for improvement. Even though on the website of the NAIH rich documentation is available including the annual reports, cases and information notices, these are official documents, lacking a plain language. To date the NAIH is not present in social media. Although different information notices and other materials were published in the field of children's online data protection,[1302] their awareness raising activity is not as comprehensive as the CNIL's.

[1297] Byrnside 2008. p. 474.

[1298] Kennedy – Macko 2007. p. 11. (Page number referring to the online version of the article.)

[1299] https://www.cnil.fr/fr/candidats-lemploi-protegez-votre-reputation-sur-le-web (Accessed: 19 August 2018)

[1300] https://www.cnil.fr/fr/10-conseils-pour-rester-net-sur-le-web (Accessed: 19 August 2018)

[1301] Other, more general articles advise users on how to adopt a more privacy and data protection conscious use on the Internet and on SNS, e.g. how to secure their accounts through adopting appropriate passwords, what precautions to adopt when using a public WIFI, how to use privacy settings etc. See these articles at: https://www.cnil.fr/fr/configurer (Accessed: 5 November 2018)

[1302] They were published in the frame of the project entitled "Key to the World of the Net!" and aimed to ensure the protection of children in the online world. A study was published together with different videos, quizzes and advice. The materials are available at the following site: https://www.naih.hu/adatvedelemr-l-fiataloknak--kulcs-a-net-vilagahoz--projekt.html (Accessed: 19 August 2018)

Title 2: The use of social network sites at the expense of working hours

SNSs can have an important effect on working hours. The main issue that they represent is that a huge number of employees spend their working hours surfing on SNSs instead of working – seriously compromising the interests of the employer, who lawfully expects the employee to work during working hours. It was already demonstrated that one of the employee's main obligation is to perform work: this obligation can be violated by the personal use of SNSs during working hours.

An employment relationship necessarily comes with the limitation of certain rights and the autonomy of the employees,[1303] meaning, for example, that the employee is not free to spend working time as he/she wishes. It is the very nature of employment that the employee must perform work under the subordination of the employer.[1304] 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.[1305]

In Title 2, emphasis will be put on the examination of using SNSs at the expense of working hours, with the main focus on the traditional (typical) employment contract.[1306] Therefore, the assessment of the content of SNS posts is not as relevant as in the case of examining the employees' exercise of freedom of expression or behaviour outside working hours: what is important is that the employee *used* SNSs during working hours. Although it is possible to publish excessive criticism, libel or harm the employer's legitimate interest in other ways during the working hours as well, these issues will be further discussed under Title 3.

The starting point is that the employer has the right to regulate the personal use of the devices provided by him/her and has the right to monitor whether the employee complies with his/her instructions.[1307] One of the employees' main obligations is *the obligation to perform work* during working hours, while the employer is entitled to monitor whether employees comply with that obligation.

In French law, the notion of employment contract itself refers to employees' obligation to work.[1308] The employee is obliged to perform the work for which he/she has been hired,[1309] and arising from the *intuitu personae* nature of the employment relationship, he/she has to do it in person.[1310] In addition, he/she is subject to a requirement of availability: he/she is obliged to be at the employer's disposal and follow his/her orders without being able to freely carry on his/her personal affairs.[1311] The employee also has to respect working

---

[1303] Kardkovács 2012. p. 40.

[1304] Cour de cassation, 22 juillet 1954 (Bull. civ. IV, no 576) referred to in: Le Lamy social 2019

[1305] Hendrickx 2002. p. 97.

[1306] Although the case of the bring your own device phenomenon will be addressed as well.

[1307] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 24.

[1308] As an employment contract is "*a convention according to which a person engages in performing work for another person under its subordination for remuneration*." Source: Cour de cassation, 22 juillet 1954 (Bull. civ. IV, no 576) referred to in: Le Lamy social 2019

[1309] Ouaissi 2017. p. 141.

[1310] Favennec-Héry – Verkindt 2016. p. 421.

[1311] Article L3121-1 of the FLC

hours and follow the instructions of the employer.[1312] From the employer's perspective, it is a confirmed principle in jurisprudence that the employer has the right to control and monitor the activity of employees during working hours.[1313]

Similarly, in *Hungarian law*, the very definition of employment contract refers to the employees' obligation to perform work,[1314] and the employees' other obligations give further guidance on the substance of this obligation.[1315] The employees' two most important obligations are to perform work and to be at the disposal of the employer during working hours.[1316] The employee should not just show up at the workplace, he/she has to spend his/her whole worktime performing work of high quality and quantity. If the employee is present at the workplace but spends his/her time, for example, reading or sending instant messages instead of performing work, the employer is entitled to terminate his/her relationship.[1317] On the other side, the employer is entitled to give instructions regarding the organization of work[1318] and has the right and obligation to control employees' work and maintain work discipline: as a consequence, he/she may apply detrimental legal consequences in the case of the employee's breach of obligation.[1319] Therefore he/she can monitor – respecting the requirements set by Sections 9–11/A of the HLC – whether employees respect their obligations and spend their working time performing work.

Although today it is a well-established principle that "*[w]orkers do not abandon their right to privacy and data protection every morning at the doors of the workplace[,]*"[1320] drawing the exact lines of these rights can pose questions. Because of the subordinate relationship between the employees and the employer, these rights have to be balanced against the employer's legitimate economic interests. Regulating and monitoring the use of SNSs can concern the employee's right to privacy, while the monitoring necessarily comes with the processing of personal data and falls under the scope of the data protection legislation, meaning that the data protection requirements aiming to ensure the employees' right to personal data protection shall be respected during such monitoring. Title 2 will examine whether and to what extent can the employer interfere with employees' personal lives through *regulating* the personal use of social media during working hours and how is it possible to *monitor* compliance?

[1312] Ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social 2015. p. 90.

[1313] Cass. soc., 14 mars 2000, N° 98-42090; Cass. soc., 4 juillet 2012, N° 11-30266; Cass. soc., 18 mars 2008, N° 06-45093

[1314] Subsection (2) of Section 42 of the HLC: "*Under an employment contract:*
a) the employee is required to work as instructed by the employer;
b) the employer is required to provide work for the employee and to pay wages."

[1315] Subsection (1) of Section 52 of the HLC: *"Employees shall:*
a) appear at the place and time specified by the employer, in a condition fit for work;
b) be at the employer's disposal in a condition fit for work during their working time for the purpose of performing work;
c) perform work in person, with the level of professional expertise and workmanship that can be reasonably expected, in accordance with the relevant regulations, requirements, instructions and customs[.]"

[1316] Gyulavári 2013. p. 254.

[1317] Gyulavári 2013. p. 257.

[1318] While the employee must also perform work according to the employer's instructions. Source: 7001/2005. (MK 170.) FMM-PM együttes irányelv

[1319] Gyulavári 2013. p. 249.

[1320] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 4.

Title 2 will examine the assumption 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. Neither of the two labour codes or the data protection acts regulate specifically employee monitoring jointly with SNSs. Therefore SNSs must be assessed in the light of the rules laid down in the labour codes relating to employee monitoring in general.[1321] Also, the practice of the courts and the data protection supervisory authorities elaborated the detailed conditions of certain types of monitoring – amongst them the monitoring of Internet and e-mail.

As social media and SNSs are Internet based platforms which enable to post certain content and to communicate with other users, the rules relating to Internet and e-mail monitoring are adequately applicable to employees' use of social media during working hours. However, SNSs have certain characteristics that make it necessary to enumerate the special issues raised by them, in order to be able to judge whether already established rules need adjustments and if yes, in what regards. A great difference compared to e-mail monitoring is that while sending e-mails usually necessarily comes with the job (meaning that the employee might use the same platform for work and personal purposes), as a main rule, messaging on SNSs is usually not part of a job at all and is purely personal. Therefore, while the access of an e-mail account can be associated with working as well, accessing an SNS (regardless of whether it is for surfing or communicating) supposes personal activity. A double approach is adopted, as it must be taken into consideration that when an employee surfs SNSs (e.g. the Facebook or Instagram newsfeed), this activity is like surfing the *Internet*; whereas when using the instant chat messaging services incorporated into these platforms (e.g. Facebook Messenger, Instagram Direct), more emphatic similarities with the regulation of the use and monitoring of *e-mail* can be observed.

As the use of SNSs is based on the use of the Internet, the already elaborated rules of monitoring employees' personal use of the Internet are applicable to the personal use of SNSs as well. The already presented general rules of monitoring are adequately applicable to Internet monitoring as well. Both French and Hungarian legal systems have already addressed the question of monitoring employees' use of the Internet and e-mail.

In *French law*, the CNIL's standpoint is that the employer is entitled to regulate the use of the Internet and e-mail by imposing limitations on its personal use for the purpose of guaranteeing the security of the network and preventing abusive personal use. However, certain personal use is usually tolerated if it is reasonable and does not affect security or productivity.[1322] At the core of the regulation a presumption is found: e-mails are presumed to be of professional nature, unless the employee obviously indicates the personal character of the messages – imposing limitations on the employer's right to monitor them, giving room for the employee's right to respect for private life.[1323] The employer cannot have access to those messages even if the personal use was forbidden, unless authorized to do so by a judge.[1324] However, the employer can freely access professional e-mails:[1325] he/she

---

[1321] Article L1121-1, and Articles L1222-2 to L1222-4 of the FLC and Sections 9–11/A of the HLC

[1322] CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018

[1323] Cass. soc., 30 mai 2007, N° 05-43102. "*However, the correspondences sent or received by the employee at the workplace are presumed to have a professional character, so the employer may open them without the presence of the concerned employee, except if they are identified as personal.*" Source: Cass. soc., 11 juillet 2012 n° 11-22.972

[1324] La Rédaction D.O. 2013. p. 3.

[1325] CNIL: *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010. p. 19.

can have access to them even without the employee's presence.[1326, 1327] In contrast, in the case of Internet connections, no such exception exists: Internet connections and the sites visited are presumed to be professional so the employer can have access to them.[1328, 1329]

In Hungary, the legal situation is slightly different as, due to the amendment of the HLC in 2019, a provision was added regulating explicitly the use of electronic equipment provided by the employer.[1330] The HLC now stipulates that unless the parties agreed otherwise, the employee can use the equipment provided by the employer exclusively for professional purposes. It also adds that during the monitoring of such use, the employer can only process data in relation to the employment relationship. The amendment corresponds with the prevailing view in doctrine related to the legislation prior to this amendment, arguing that the employer is free to decide whether he/she allows the personal use of the Internet, and if yes, to what extent.[1331] Then, the extent of the monitoring will be highly dependent on whether the employer has allowed personal use or not: in Hungarian law as well, more extensive protection is afforded to personal communication/use of the Internet.

The case of SNS use during working hours will be examined by taking a double, privacy-data protection/regulation-monitoring approach: attaching privacy to the regulation of SNS use, and data protection to the monitoring of compliance with the regulation. *First*, in Chapter 1 it will be addressed to what extent employees' right to private life is extended to the workplace, namely: do they have the "right" to use social media during working hours and how can the employer regulate or prohibit their use? *Then*, in Chapter 2 it will be discussed what data protection requirements must be enforced during the monitoring of whether employees comply with the employer's regulation. Therefore, regulation and monitoring will be treated separately.

Chapter 1: Possible prohibition of personal use of SNSs during working hours

The regulation of the personal use of SNSs (and within this subject the question of possibly prohibiting its use) will be treated from a privacy angle. When regulating such a use, the employee's right to privacy can be affected, as since the *Niemietz case* it is established that "*[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings[,]*"[1332] which are very often established at

---

[1326] CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018

[1327] However, certain limits are imposed on the employer's access in line with the general principle of proportionality: it is forbidden to automatically receive a copy of each message or to use a key logger program. CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018

[1328] "*[…] the connections made by an employee on websites during working hours from an IT tool provided by the employer for the performance of work are presumed to have a professional nature so the employer can look into them for the purpose of identifying them, without the presence of the employee.*" Cass. soc., 9 juillet 2008, N° 06-45800; Cass. soc., 9 février 2010, N° 08-45253

[1329] Again, this access is not limitless: the use of key logger programs or storing information related to the sites visited for a period longer than 6 months is prohibited. Griguer 2013. p. 75.

[1330] Subsections (2) and (3) of Section 11/A of the HLC

[1331] Arany-Tóth 2016. p. 107.; Berke – Kiss 2014. p. 62.; Németh 2013a. pp. 37–38.; Kun 2013. p. 13., Szőke et al. 2012. p. 34.

[1332] ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.

the workplace.[1333] The personal use of the employer's electronic devices can constitute a way to establish relationship with others. It is undisputable that as a main rule, the employer is entitled to decide whether he/she allows the personal use of the Internet, e-mail (and SNS). However, the question that needs to be considered is whether the use of SNSs – one of today's main platforms of communicating and establishing relation with others – can be completely prohibited during working hours?

The starting point of Chapter 1 will be the already elaborated set of rules in the field of regulating/prohibiting the personal use of the Internet and e-mail – addressed in *Section 1*. Then, *Section 2* will examine what kind of new challenges SNSs raise compared to the existing regulation, and in the light of these challenges, how their personal uses should be regulated.

Section 1. Employees' right to personal life within the workplace: regulating personal use of the Internet and e-mail during working hours

The examination of the already established regulation in the field of Internet and e-mail monitoring can constitute the basis for the further examination of the main subject. This is because of the similarities between the Internet/e-mail and SNSs: as SNSs are Internet based platforms, they allow the user to "surf" on them (like on the Internet); and they also allow the employee to communicate with other users (like in the case of e-mail). Regulating the personal use of the Internet and e-mail was already addressed by regulations: detailed rules were elaborated both at *(§1)* the international level (amongst which focus will be put on the European regime) and at *(§2)* the national level.

§1. Outlook to European law

Under European law, attention should be paid especially to documents issued by the EU's WP29, and by the CoE's ECtHR. The WP29's documents provide useful and detailed guidance to Member States, while the ECtHR recently addressed the question of employee monitoring, putting this already existing phenomenon into a new perspective. Besides, contracting parties, such as France or Hungary are also obliged to take into consideration the ECtHR's decisions both during legislation and the application of law.[1334] Therefore the documents of the WP29 and the ECtHR's decisions are of high importance in relation to the national regulation (and monitoring discussed in detail in Chapter 2) of SNS use at the expense of working hours.

(A) EU perspective: the WP29's documents

The WP29 expressed in the *Working document on the surveillance of electronic communications in the workplace*, already presented in Part I, that it is up to the employer

[1333] ECtHR: *Niemietz v. Germany*, application no. 13710/88, 1992. par. 29.
[1334] Rózsavölgyi 2018. p. 47.

to decide whether he/she allows the personal use of the Internet and if yes, to what extent.[1335] However, the working document does not address the question whether a *complete* ban is possible, it only adds, without providing legal arguments, that a blanket ban seems to be impractical and unrealistic, as the Internet has gained a huge importance even during work.[1336]

Although the WP29 mostly deals with monitoring and the extent of prohibition/regulation, in its *Opinion 2/2017 on data processing at work* the WP29 explicitly refers to employees' "*legitimate right to use work facilities for some private usage*".[1337] When stating that, the WP29 referred to the ECtHR's Halford case[1338] and Bărbulescu case.[1339] However, according to my opinion, these references do not truly show the existence or the content of employees' right to use the employer's equipment for personal use, as the formulation of their reasoning rather suggests that it is only ensured that the use of such devices by employees for personal purposes might be covered by Article 8 of the ECHR.

The WP29's latter conclusion might be more crystallized through *Paul De Hert*'s and *Hans Lammerant*'s study relating to European workplace privacy/data protection, which referred to the ECtHR case law:[1340] therefore this study might help more to better understand employees' "right to private usage". In the study they pointed out that employees' have their rights even within the workplace, meaning that although the existence of the employer's right to decide how his/her equipment can be used (and to monitor compliance) is not questioned, it is limited not only by the employees' right to privacy (including the protection of communication), but also by their right to communication. This results in the fact that the employer cannot prohibit *all* private communication. Although he/she can prohibit the privative use of certain telecommunication means, this should not mean that employees can be left without any alternative to communicate.[1341]

(B) CoE: the ECtHR's case law

The ECtHR's case law in the field of monitoring employees' use of the employer's equipment (such as telephone, the Internet, e-mail)[1342] has not addressed the extent to which personal use can be prohibited (whether the employer has the possibility to ban it completely), it rather focused on the existence of the right to privacy, which is a separate issue and will be discussed in relation to monitoring.[1343] However, cases such as the Bărbulescu v. Romania

---

[1335] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 24.

[1336] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 24.

[1337] WP29: *Opinion 2/2017*. p. 14.

[1338] "*telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8 paragraph 1*" ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 44.

[1339] Although in a reference to the 2016 judgement and not to the 2017 Grand Chamber judgement. They referred to the ECtHR stating that the employer can only monitor the use to a limited and proportionate extent.

[1340] Notably to the case of Halford and Copland.

[1341] De Hert – Lammerant 2013. p. 53.

[1342] E.g. Halford v. the United Kingdom, Copland v. the United Kingdom

[1343] Although in the Copland case the ECtHR remarked in par. 42. that "*[t]he applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone*", implying that unless given prior notification, the employee can reasonably think that the equipment can be used for personal purposes as well. (Rózsavölgyi 2018. p. 43.)

(2017) directly address the question, and the Libert v. France case (2018) also contains some important observations.

(a) Case of Bărbulescu v. Romania

The *Bărbulescu v. Romania (2017)* case can serve as an important starting point when it comes to both regulating and monitoring the personal use of SNSs. The applicant, Mr. Bărbulescu was dismissed for using the Internet and a Yahoo account for private purposes against the prohibition of the employer – also, the account was created at the initiative of the employer. The employer found this out by monitoring the use of the equipment. Although Mr. Bărbulescu was informed that the personal use if IT equipment was prohibited, he was not informed as concerns the details of the implementation of the monitoring which, as it turned out, registered all content of his communication for a certain period.

Besides elaborating the rules relating to monitoring,[1344] the decision is also significant for what it stated on *social private life*. In this case the ECtHR acknowledged the existence of "social private life" and ruled that "*[…] an employer's instructions cannot reduce private social life in the workplace to zero.*"[1345] In this context private social life means the possibility for the individual to develop his/her social identity,[1346] and the ECtHR noted that instant messaging services constitute one form of leading a private social life.[1347] The ECtHR also stated that restrictions on an individual's professional life may fall within Article 8 in the case that they have "*repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others.*"[1348] Even in the workplace, respect for private life and for the privacy of correspondence continues to exist, although it may be restricted to a necessary extent.[1349] Thus, the complete ban of personal communication seems to restrict the private social life of employees to an unreasonable extent.

(b) Case of Libert v. France

Even though it mainly relates to the storage of personal files on the employer's computer, the *Libert v. France (2018)* case[1350] contains some important observations. The case related to the opening of personal files stored on a work computer. The applicant, employee of the French national railway company (SNCF), was dismissed after the seizure of his work computer revealed that he stored a considerable number of pornographic files and forged documents. The applicant argued that the employer violated Article 8, by accessing those files in his absence.

In its judgement the ECtHR recalled that the employer has the right to ensure that employees use the equipment provided by him/her for executing their work in compliance with their contractual obligations and applicable regulation.[1351] The employee's files identified

---

[1344] Costes 2017. p. 35.
[1345] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 80.
[1346] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 70.
[1347] Colonna – Renaux-Personnic 2017. p. 2. (Page number referring to the online version of the articledownloaded from: https://www.gazette-du-palais.fr)
[1348] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 71.
[1349] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 80.
[1350] ECtHR: *Libert v. France*, application no. 588/13, 2018
[1351] ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 46.

as personal receive more protection, as according to French law they can only be opened if there is a risk or a particular event and in the presence of the employee or if he/she has been properly notified of it – contrary to files presumed to be of professional nature.[1352] The ECtHR confirmed the principle that the employee is entitled to the right to respect for private life even within the workplace, and that files obviously identified as personal, stored on the computer provided by the employer for work purposes, might pertain to the private life of the employee.[1353] Although the decision does not mention a right to use the employer's equipment for personal purposes, through providing protection to the personal files stored on work computers, certain tolerance is manifested, suggesting that a complete ban of personal use would not be feasible.[1354]

§2. Regulation at the national level: France and Hungary

Besides the regional level, detailed rules were elaborated at the national level as well, including French and Hungarian law. When assessing the legitimacy of a complete ban of personal use in the French and the Hungarian system, first *(A)* the fundaments of protecting employees' personal lives will be discussed mostly through presenting the labour codes and scholars' opinion on the subject. Then *(B)* the DPA's position will be examined. Finally, *(C)* relevant case law will be examined, with the aim of tracing the line between abusive personal use, and personal use that should be tolerated by the employer[1355] – thereby determining the possibility to apply legal consequences against employees who use the Internet/e-mail/SNSs for personal purposes during working hours.

(A) Private/personal life at work

The FLC contains no direct provision aiming to regulate the use of the employer's equipment and its monitoring. However, an important principle, namely the respect of the employee's right to respect for private life within the workplace (during the use of the company's equipment) was established by the jurisprudence, which serves as a basis for the further analysis of the relevant rules. *In France*, the Court of Cassation's landmark[1356] *Nikon decision*[1357] must be first mentioned.[1358] The case related to an employee of the Nikon France Society, who was dismissed for serious misconduct particularly for using the company's equipment for personal purposes – which was provided for him for professional purposes.

[1352] Cass. soc., 17 mai 2005, N° 03-40017

[1353] ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 25.

[1354] On the Libert case see more in: Sipka – Zaccaria 2018.; Marchadier 2018.; Nasom-Tissandier 2018.

[1355] *Márton Leó Zaccaria* observed the employees' increasing possibilities due to technological development: today employees often feel limited in their rights when the employer wants to restrict or prohibit such personal use, while even before the proliferation of ICT and SNSs it was not an established practice that employees spend their working hours writing letters to their friends. Source: Zaccaria 2016. p. 16.

[1356] Dupuis 2001. p. 5. (Page number referring to the online version of the article downloaded from: https://lamyline-lamy-fr)

[1357] Cass. soc., 2 octobre 2001, n° 99-42.942

[1358] Although it relates to case law, due to the high importance of the Nikon case, it will be discussed in part (A) instead of part (C).

The Court of Cassation – which granted employees an extremely (even too) favourable position[1359] – affirmed that the employee has the right to respect for private life, especially to the secrecy of correspondence, even during working hours, at the workplace.[1360]

The Court of Cassation held that that "*the employee is entitled, even during work hours and at his/her workplace, to have the intimacy of his/her private life respected; that this implies in particular the secrecy of correspondence; that the employer may not therefore, without violating this fundamental freedom, examine personal e-mails sent and received by an employee through a computer provided as a work tool, and this applies even if the employer has forbidden the non-professional use of the computer[.]*" Therefore, the Court of Cassation admitted the existence of an autonomous sphere reserved for the intimacies of private life, which must be respected even if the employer has prohibited personal use. However, through referring to Article L. 1121-1 of the FLC,[1361] the decision maintains the possibility of limiting these rights, within the borders set by legislation.[1362] The essence of the decision is based on the protection of the employee's private life within the workplace.[1363] However, recognizing such protection does not mean that the employer cannot ban or sanction abusive personal use.[1364]

Thus, the Court of Cassation questioned the strict separation of professional and personal life, through acknowledging the respect of private life within the workplace.[1365] The decision had a great impact: while it was recognized that it made a huge step in recognizing employees' right to respect to private life within the workplace,[1366] it was also pointed out that potential abuses on the part of the employees might also take place.[1367] The decision might seem paradoxical insomuch as it put employers in a difficult position as, although they could order employees not to use equipment for private purposes, they were not allowed to lawfully open private letters, even if they violated the employer's orders.[1368] Later on, this principle became more nuanced through the adoption and application of the previously mentioned presumption of professional character of communication.[1369] Even though the Nikon decision did not address whether employees' have the right to use the employer's equipment for personal purposes, it afforded protection to personal use, even if it took place contrary to the employer's internal regulation.

As regards the regulation of the personal use of the Internet and e-mails, the starting point is that as Internet connection and e-mails are perceived as a work tool necessary for the execution of work, the employer can regulate and control their use.[1370] However, according to the majority opinion, the total prohibition of the personal use of the Internet and

---

[1359] Gautier 2001. p. 3150.

[1360] Kocher 2013. p. 129.

[1361] Back then Article L. 120-2 of the FLC.

[1362] Kocher 2013. p. 132.

[1363] Gautier 2001. p. 3149. Its reasoning can be reduced to the following syllogism: everyone has the right to respect for private life, and more precisely to the secrecy of correspondence; private life can take place within the workplace; as a result, opening a communication addressed to the employee violates the employee's rights.

[1364] *Rapport de la Cour de Cassation 2001*: A. Contrat de travail 1. Exécution.

[1365] Lyon-Caen 2001. p. 10.

[1366] According to *Jean Hauser*, if private life flows into the workplace, it also raises the question of whether the work can flow into the private life of the employee. Hauser 2002. p. 72.

[1367] Kocher 2013. p. 130.

[1368] Vigneau 2002. p. 357.

[1369] This question will be further addressed in Section 2.

[1370] Féral-Schuhl 2018. p. 394.

e-mail would be considered illegitimate, as such a prohibition would be inconsistent with the principle of proportionality laid down in Article L1121-1 of the FLC.[1371, 1372] Personal use to a reasonable extent, for legitimate purposes such as urgent personal communication should be tolerated.[1373]

Jean-Emmanuel Ray expresses that even though in theory the employer is entitled to completely ban the personal use, in reality the situation is more nuanced, as in practice the enforcement of such a ban is not feasible. As in the 21st century ICT are part of everyday life, it would be disproportionate to sanction an employee for conducting simple, everyday activities such as for calling a family member in an urgent situation, or for buying plane tickets for his/her holiday during the work pause – if the activity did not constitute abuse.[1374] Today, these simple everyday activities are often conducted through different SNSs. *Jean Louis Denier* expressed a similar opinion in 2003, arguing that although no legal constraint of providing "private" use of company equipment weighs on the employer, other factors, especially the blurred boundaries of professional and personal life make it more realistic to tolerate a certain personal use.[1375] Then, the next step is to define the limits of tolerable personal use – which will be mostly curved out by the jurisprudence of French courts.

In Hungary, when assessing whether the employee committed misconduct, the starting point is that employers have the discretional right to decide whether they allow the personal use of the Internet or not.[1376] This standpoint was further nuanced by the amendment of the HLC in 2019, explicitly determining at the statutory level that unless agreed otherwise, the employee should use the work equipment exclusively for professional purposes.[1377] Prior to the amendment, the HLC stated that the employee's private life cannot be subject to monitoring: instead of such a declaration (especially with regard to the fact that other acts ensure the protection of the private life of the individual) emphasis is put on the employee being able to use work equipment solely for professional purposes.[1378]

Such a formulation suggests that a complete ban of personal use is possible. As regards SNSs, according to the Commentary of the HLC, the employer can prohibit employees using SNSs during working hours.[1379] Such a complete ban seems feasible, even accessing sites from the employees' own device can be prohibited.[1380] This position was already supported prior to the amendment by a number of scholars – although they usually added that despite the possibility of a complete ban, the employer should consider tolerating a certain use. They usually started their analysis by differentiating between whether the employer has authorized personal use or not, implying that it is his/her right to decide whether personal use is allowed. According to *Janka Németh*, the employer can choose from among three

---

[1371] Grangé – Froger 2003. p. 216.

[1372] However, the contrary was expressed by *Paul-Henri Antonmattei*, who was of the opinion that the complete ban of non-professional use seems legally justified, as the employee has the right to respect to his/her personal life at the workplace, and not the right to personal life. Antonmattei 2002. p. 39.

[1373] Grynbaum – Le Goffic – Morlet-Haïdara 2014. pp. 111–112.

[1374] Ray 2001a. pp. 95–97.

[1375] Denier 2003. p. 32.

[1376] Berke – Kiss 2014. p. 62.

[1377] Subsection (2) of Section 11/A of the HLC

[1378] *T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról*, 2019. p. 102.

[1379] Berke – Kiss 2014. p. 62.

[1380] Kun 2013. p. 13.

scenarios: banning the use of the Internet completely,[1381] only banning the personal use of the Internet or not placing restrictions on the employees' use of the Internet.[1382, 1383] Then, the scale of monitoring is influenced by which scenario was chosen by the employer.[1384] It is also important to consider the period when the banned activity takes place: during periods when the employee is not busy, or at the direct expense of his/her obligations (e.g. a salesperson ignoring customers and surfing on Facebook).[1385]

Gábor Kártyás, *Rita Répáczki* and *Gábor Takács* add further nuances to this position and note that the employer is entitled to completely prohibit the personal use during working hours: it is up to him/her to decide whether personal use is allowed and to what extent. However, they also note that in most of the jobs – jobs which do not require constant physical and mental presence – it is not counterproductive if the employee consults these sites for short periods from time to time. On the contrary, a complete ban might be counterproductive in these cases.[1386] They also argue that with regard to the principle of mutual cooperation, in situations of major importance (e.g. the employee's wife is about to give birth, etc.), the employer should try to make an exception from the ban.[1387] In relation to communication, *Edit Kajtár* argued that even though the employer can decide what policy to adopt, the reasonable personal use of the professional e-mail account is usually tolerated.[1388, 1389] In my opinion, these intermediate standpoints adequately take into consideration the realities of SNSs through allowing a certain tolerance relating to their personal use.

(B) Position of the DPAs

The *CNIL* expressed on several occasions that although the employer can decide how to regulate the personal use of his/her equipment, it is recommended that a reasonable personal use is tolerated rather than applying a complete ban. In relation to the *Internet*, they stated that completely prohibiting the use of the Internet for non-professional reasons does not seem realistic in the information society and seems disproportionate in regards to the applicable legal provisions. They also add that a reasonable use, which is not likely to undermine the conditions of professional network access, does not question productivity

---

[1381] Although she questions the efficacity of such a measure, as the Internet can be used for work as well.

[1382] Németh 2013a. pp. 38–39.

[1383] Or, as *Edit Kajtár* phrased it, the employer can choose between banning, restricting and regulating the use of the Internet. Kajtár, 2016. p. 119.

[1384] If the employer decided to allow the personal use of these sites, the employee cannot be sanctioned for using them in compliance with the rules, while the non-conform use can lead to legal consequences, especially if the banned use takes places during working hours and the content visited is compromising. Kártyás – Kozma-Fecske 2016. p. 17.

[1385] Kun 2013. p. 13.

[1386] Kártyás – Répáczki – Takács 2016. pp. 77–78.

[1387] Kártyás – Répáczki – Takács 2016. pp. 78–79.

[1388] Kajtár 2016. p. 122.

[1389] Although she did not address the question explicitly, *Mariann Arany-Tóth* states that the complete ban of the personal use of the Internet realises interference with the right to freely develop one's personality. (Arany-Tóth 2011– p. 144.) As such interference must meet certain – already presented – requirements, the legitimacy of a complete ban might be questioned.

and is usually socially accepted by most companies and administrations.[1390] In relation to the personal use of the *professional e-mail account*, the CNIL stated that receiving and sending personal messages in reasonable[1391] proportions is generally and socially accepted.[1392] However, despite certain tolerance, the employer has several possibilities to regulate and impose limits on personal use, such as filtering unauthorized websites or forbidding the access to certain sites (e.g. pornographic sites) or the downloading of files or videos, or the access to chat or personal e-mail accounts.[1393]

Neither the former Data Protection Commissioner, nor the NAIH has explicitly addressed the question of whether the complete prohibition of the personal use of the Internet and e-mail is possible. The cases of the *Data Protection Commissioner* mainly dealt with the scope of monitoring,[1394] and differentiated between the cases when the employer allowed personal use and when the use was only permitted for work purposes.[1395] However, instead of addressing the extent of the regulation, these cases were focused on monitoring. One case[1396] took a stand on whether a complete ban is *advisable* or not: it is advisable that the employer limits the use of the Internet to those websites which are necessary for the work, as due to the principle of data minimization, compliance can be better enforced with such a limitation during monitoring.

The *NAIH* published two comprehensive documents in the field of employee monitoring: the already presented *Recommendation on the basic requirements of electronic monitoring at the workplace* (2013) and *Information notice on the basic requirements on data processing at work* (2016). However, the Recommendation governs electronic monitoring (and focuses mainly on CCTV surveillance) and it does not address the employer's power to completely forbid personal use: it only refers to the employee's obligation to work and to be at the employer's disposal.[1397] The Information notice states in relation to Internet and e-mail monitoring that, before implementing the monitoring, it is recommended that the employer adopts an internal policy in which he/she informs employees regarding the access to which sites is blocked/whether the employees can use their professional e-mail for personal purposes – without further investigating the legitimacy of a complete ban.[1398] Neither of the documents refers explicitly to the use of SNSs during working hours.

[1390] Bouchet 2004. p. 23.; CNIL: *Guide pratique pour les employeurs*. Les guides de la CNIL, 2005. p. 11.; CNIL: *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010. p. 18.; CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018

[1391] The CNIL provides examples of draft clauses for internal regulations relating to the personal use by stating that "*only websites with a direct and necessary link to the professional activity are intended to be visited provided that connection time does not exceed a reasonable time and has utility in terms of the functions or mission to carry out. One-time consultations within reasonable limits for personal use regarding Internet pages that are not contrary to the public order and morality and do not incriminate the interests and the reputation of the organisation is tolerated.*" Cited in: Duez-Ruff 2012. p. 6. (Page number referring to the online version of the article downloaded from: http://www.lexbase.fr)

[1392] Bouchet 2004. p. 25.

[1393] Féral-Schuhl 2018. p. 395.

[1394] On the summary of the Data Protection Commissioner's and the NAIH's activity see more in: Arany-Tóth 2016.; Szőke et al. 2012.

[1395] ABI 570/A/2001, ABI 790/A/2001, ABI 866/A/2006-3., ABI 40/K/2006, ABI 1767/K/2006-3., ABI 531/A/2004

[1396] ABI 800/K/2008-3.

[1397] NAIH-4001-6/2012/V. p. 2.

[1398] NAIH 2016. p. 25, p. 30.

(C) Case law: abusive personal use and "Facebook firings"

Case law has an important role in defining where the boundaries between abusive and reasonable personal use are. In France, courts have provided rich case law in this field. In contrast, Hungarian case law is minimal in the subject,[1399] making it difficult to systematically compare the two jurisprudences, as it is difficult to find common grounds and criteria for comparison. As such, the analysis of the jurisprudence will be mainly based on French case law. French courts reflect the position of scholars and the CNIL, as courts usually tolerate the reasonable personal use of the employer's equipment, but validate dismissals if the employee manifested an abuse while using these devices.[1400] Their case law can contribute to defining what use is considered to be abusive or reasonable. This question is important because employees can face various consequences if they use SNSs despite the ban, or contrary to the employer's regulation: in serious cases they can even be dismissed from the workplace.

The *Court of Cassation and regular courts* have already ruled on the personal use of the Internet/e-mail on several occasions. The following paragraphs will examine the French courts' position on defining the limits of an abusive personal use. The length/number of connections were the criteria the most often referred to (time spent on these sites, number of pages visited, and amount of downloaded material), as using the employer's equipment for personal purposes on a regular basis is not an acceptable behaviour.[1401] However, the exact limits of such a use must be defined more precisely. Other, secondary criteria, such as the nature of the sites visited or making professional mistakes can also be of importance.

The *length/number of connections* often played an important role in these cases: the *Court of Appeal of Bordeaux* ruled that using the Internet for personal purposes for one hour during a week is not abusive. In this case, the employee used the Internet connection – despite the ban set in the internal regulation – for personal purposes, for 6.5 hours over a period of more than six weeks. The court ruled that this use cannot be considered excessive and in itself cannot serve as a basis of dismissal, considering that otherwise her behaviour was irreproachable, and the pages visited posed no threat to the employer.[1402] In another case, between a hospital and a doctor, the *Court of Appeal of Paris* found that the dismissal reasoned by the permanent problem of ensuring the respect and the security of patients was not well-founded, as the doctor who accessed pornographic sites (without any paedophilic character) did it without any frequency – not daily, not weekly and not even monthly –, and for not a long time.[1403] The length of connection is also significant as pointed out by the *Court of Appeal of Paris*, which stated that the presentation of a list of websites consulted by the employee is not sufficient to qualify as professional failure, as the proof of the time spent by the employee out of the professional field is missing.[1404]

[1399] According to *Máté Dániel Szabó* and *Iván Székely*, those who were victims of privacy infringements usually do not turn to courts, but rather to the data protection authority. Therefore, the practice of the former Commissioner became case law supplementing the courts' application of law. Szabó – Székely 2005. p. 116. and p. 119. A 2012 report also stated the lack of case law in the field of employee monitoring. Source: Szőke et al. 2012.

[1400] Grynbaum – Le Goffic – Morlet-Haïdara 2014. p. 888.

[1401] Cass. soc., 14 mars 2000, n° 98-42.090

[1402] CA Bordeaux, Chambre sociale, section A, Arrêt du 15 janvier 2013

[1403] CA Paris, Pôle 6, 3ème ch., 15 novembre 2011, n° 09/09 398

[1404] CA Paris, Pôle 6, 6ème ch., 6 février 2013, n° 11/03 458

Dismissal was not well-founded in a case where a web manager was dismissed for publishing 1,336 non-professional tweets during working hours (over a 16-month-long period), as the *Court of Appeal of Chambéry* found that supposing that the writing and the publication of one tweet takes one minute, the time spent with this activity does not exceed 5 minutes per day. In addition, the employee was not subject to any working hours and his job required him to be constantly connected to the Internet.[1405] The *Court of Appeal of Lyon* held in a case where an employee used his work computer for personal purposes on six occasions (4 times during May and 2 times during June) – contrary to the explicit ban laid down in the internal policy – that although this conduct constitutes a violation of his obligations arising from the employment contract, the dismissal was disproportionate compared to the violation committed.[1406] The *Court of Appeal of Basse-Terre* found that contrary to the employer's allegations – according to which the employee used her work computer for very personal purposes abusively and without authorization,– the employee's conduct of creating nine personal files over a period of one year could not serve as a basis for dismissal. (Moreover, the internal regulation allowed personal use to a moderate extent, with the respect of the employee's obligation of loyalty.)[1407] The dismissal of an employee was without an actual and serious basis in a case at the Court of Cassation, in which an employee was dismissed for "illegal and repetitive downloading", but in reality he visited a downloading site for two and a half minutes.[1408, 1409]

In contrast to these decisions, the *Court of Cassation* found the use abusive, and as such the dismissal justified for serious misconduct of the employee in a case when the employee spent 41 hours during the period of one month by surfing the Internet for personal purposes.[1410] The Court of Cassation came to the same conclusion in a case in which an employee connected to not work-related sites – and among them to social media – more than 10,000 times during a period of 18 days.[1411] The Court of Cassation held that an employee who violated his contractual obligations and the internal regulation's ban on the personal use of the Internet by sending one of his colleagues 178 e-mails accompanied by videos having sexual, humorous, political and sporty character from his work computer committed a breach of obligations, and his dismissal was therefore well-founded.[1412]

The *Court of Appeal of Nîmes* stated the abusive nature of surfing on the web for 8.5 hours over a period of less than 2 months – in this case the 8.5 hours was the minimal time spent surfing the web. It also found that the dismissal of the employee was justified, but in contrast to the previously cited case,[1413] the employee made professional mistakes, which, in addition, could be related to the excessive personal use of the Internet.[1414] The *Court of Appeal of Pau* stated that regular access to SNSs (e.g. Facebook), to a personal e-mail

[1405] CA Chambéry, 25 févr. 2016, RG n°15/01264

[1406] CA Lyon,18 novembre 2011, n° 11/01261

[1407] CA Basse-Terre, chambre sociale, 13 octobre 2014, N° de RG: 13/01046

[1408] Cass. soc., 29 octobre 2014, N° 13-18173

[1409] Although it should be added that besides the downloading the sites, the employee visited webpages for personal purposes on numerous occasions. However, as the reasoning of the dismissal only mentioned downloading, activity other than downloading from downloading sites fell beyond the scope of the case.

[1410] Cass. soc., 18 mars 2009, N° 07-44247

[1411] Cass. soc., 26 février 2013, N° 11-27372

[1412] Cass. soc., 18 décembre 2013, nº 12-17.832

[1413] CA Bordeaux, chambre sociale, section A, Arrêt du 15 janvier 2013, where the court took into consideration that the employee's behaviour was otherwise irreprochable, except for the personal use.

[1414] CA Nîmes, 2 avril 2013, n° 12/02146

account (Hotmail), to dating sites and to a lingerie site (where the employee exercised commercial activity) during working hours resulted in her not being able to perform her work, therefore, the court confirmed the dismissal.[1415] The *Court of Appeal of Rennes* also found that personal use during 20% of working time is abusive.[1416] The C*ourt of Appeal of Paris* found the dismissal of an employee justified, who despite the ban laid down in the company's internal regulation and a previous warning, used the Internet for personal purposes. The court affirmed that the digital consumption of 97 MB and 195 MB over the period of two days, exceeding the amount used by all other employees together, was abusive.[1417] The *Court of Appeal of Aix en Provence* confirmed the dismissal of an employee who spent one hour per day surfing on the Internet for personal purposes, despite the ban of the internal regulation. On numerous occasions, the employee deliberately and repeatedly violated the internal regulation and connected to the Internet during working hours, at the expense of working time – as a result, the dismissal for gross misconduct was found valid.[1418]

The *nature of the content* visited/sent might also be of importance: if the employee visits sites with rough content, it can serve as a criterion for assessing the abusive nature. The *Court of Cassation* held that unlawful conduct, such as the sending of anti-Semitic messages can constitute a basis of dismissal.[1419] In the already presented case of the *Court of Appeal of Paris*[1420] between a hospital and a doctor, the court took into consideration that the pornographic sites that were visited did not have any paedophilic character – even though as a main rule, the *Court of Cassation* found that consultation and animation of pornographic sites on work equipment is not covered by the notion of private life.[1421] In the case before the *Court of Appeal of Pau*,[1422] the court also remarked that besides accessing SNSs and personal e-mail accounts, the employee also accessed a lingerie site, where, in addition, she exercised commercial activity.[1423] Besides assessing the length of personal use, the *Court of Appeal of Bordeaux*[1424] also took into consideration that the pages visited posed no threat to the employer.

Professional mistakes as a result of being distracted due to the personal use can also have importance. When judging the use to be abusive, the *Court of Appeal of Nîmes*[1425] considered that the employee made professional mistakes due to the excessive personal use of the Internet. In another case at the *Court of Appeal of Bordeaux*,[1426] the absence of mistakes served as a ground for not establishing the abusive nature of personal use.

The *conclusion* that can be drawn from these cases in relation to SNSs is that several factors can have a determining effect when judging the excessive nature of the use. Usually the *length* of the period spent on these sites is extremely important: if the employee spends a

---

[1415] CA Pau, chambre sociale, Arrêt du 13 juin 2013

[1416] CA Rennes, 7e chambre prud'homale, 20 novembre 2013, n° 12/03567

[1417] CA Paris, Pôle 6, 5ème ch., 19 janvier 2012, n˚ 10/04 071

[1418] CA d'Aix en Provence, 17eme chambre, arrêt au fond du 13 janvier 2015

[1419] Cass. soc., 2 juin 2004, 03-45.269 and Castets-Renard 2011. p. 34.

[1420] CA Paris, Pôle 6, 3ème ch., 15 novembre 2011, n˚ 09/09 398

[1421] Cour de cassation, chambre criminelle, 19 mai 2004, N° 03-83953 However, it must be noted that in the given case the employee had a very extensive use connected to the consultation of pornographic sites, storing files and sending messages as well.

[1422] CA Pau, chambre sociale, Arrêt du 13 juin 2013

[1423] CA Pau, chambre sociale, Arrêt du 13 juin 2013

[1424] CA Bordeaux, chambre sociale, section A, Arrêt du 15 janvier 2013

[1425] CA Nîmes, 02 avril 2013, n° 12/02146

[1426] CA Bordeaux, chambre sociale, section A, Arrêt du 15 janvier 2013

significant part of his/her working hours on Facebook, the abusive use might be established. Also, the *frequency* of the connections might be a decisive factor: if the employee uses SNSs for personal reasons on a regular basis, it will also be taken into account when assessing an abusive use. However, if he/she occasionally accesses these sites, or accesses them for short periods, the use is unlikely to be considered excessive. However, these observations are only valid if the employee's performance is not affected in a negative way by the personal use: if the employee becomes distracted and commits professional mistakes, or as a direct consequence neglects or violates his/her other obligations (e.g. a bus driver checking Facebook while driving, or a cashier ignoring customers because of Facebook), the abusive nature might be more easily established. Also, the *content* accessed might be taken into consideration: for example, visiting Facebook pages containing questionable material (e.g. accessing homophobic, racist, paedophilic content, etc.) might affect the decision. These criteria can be useful when it comes to assessing whether the employee used SNSs to an abusive extent in the light of the given circumstances of a case.

As it was already stated, in *Hungary* limited case law is available compared to France. Notably, one case[1427] relating to the personal use of the Internet shall be mentioned, in which the Hungarian Supreme Court examined whether the personal use of the Internet and e-mail can constitute a basis for extraordinary termination. In this case the employee used his and also his colleague's computer for personal purposes, mainly to visit pornographic sites. According to the court, it is the employee's obligation to perform his/her work in a way that does not lead to the incorrect judgement of the employer or other persons – described in the HLC as well.[1428] The employee, who had an important and confidential position, violated this essential obligation to a significant degree. The Hungarian Supreme Court ruled that infringing the employer's restrictions and using another employee's computer for this purpose constituted a serious breach of obligation, and the activity constituted legal ground for termination of employment.

Another decision relating to being late for work can be mentioned, which can be indirectly relevant to the use of SNSs during working hours, as being late for work is also contrary to the employee's obligation of appearing at work on time. Theoretically, being only a few minutes late constitutes a breach of obligation – although the consequences of this breach will depend on the length of being late.[1429] The consequences of being late might also depend on the given job:[1430] for example, being a few minutes late might come with different implications for an airplane pilot or for a maid. Although arriving at work relatively little late but regularly for longer periods of time might constitute the reason for the termination of employment as it constitutes a breach of obligation,[1431] the Supreme Court of Hungary ruled that the motivation of the termination shall not be considered reasonable if a long-term employee is dismissed because he/she arrived late at the workplace once.[1432, 1433]

[1427] BH 2006.64

[1428] From such reasoning, *Éva Pete* drew the conclusion that the employer can legitimately impose the general prohibition on the personal use of the Internet. Pete 2018. p. 782.

[1429] https://ado.hu/munkaugyek/a-keses-ot-szankcioja/ (Accessed: 7 January 2020)

[1430] https://ado.hu/munkaugyek/a-csak-meg-ot-perc-munkajogi-kovetkezmenyei/ (Accessed: 7 January 2020)

[1431] Halmos – Petrovics 2014. p. 121.

[1432] Gyulavári 2013. p. 200.

[1433] However, being late constituted a legitimate reason for termination of the employment contract in a case when the employee was away from the workplace for hours without permission – exceeding by hours the negotiated period for being away, as a result leaving co-workers with an increased amount of work and jeopardizing

By analogy, this provision should adequately be applied to the case of using SNSs, and the exact circumstances of the case should be taken into consideration. Unless the employer allowed personal use, consulting SNSs on a regular basis even for short periods constitute a breach of the employee's obligations and might serve as a reason for dismissal. However, it might be different if the employee infringes the employer's instructions and checks Facebook one time, for 5 minutes. Also, there might be a difference if a newly hired employee does that on his/her first week or an employee who has worked there for years. Therefore, the exact consequence depends on the given context.

In conclusion, in France a certain tolerance towards the personal use of the Internet can be observed, as a complete ban seems to be incompatible with the principle of proportionality. On the other hand, in Hungary, the employer's right to regulate and even prohibit personal use seems to be more prevailing, as the legality of a complete ban was not questioned especially due to the amendment of the HLC, but it was not questioned either by the majority of the doctrine, by the Data Protection Commissioner or the NAIH. As SNSs are Internet based platforms, these provisions should concern them as well. A common characteristic between the two countries is that according to the case law (much more abundant in France), the gravity of the employee's breach of obligation is linked to the circumstances of the case. In such cases, even if the employee uses SNSs for personal reasons despite the ban of the employer, a dismissal or some other sanction might easily be considered disproportionate if the conduct lacks the abusive character.

As a result, the key question to be answered is: when will the use be considered abusive or excessive? No universal solution can be provided to this question; however, it was determined what the circumstances that are usually taken into consideration are. The most decisive factor was the number of connections (Has the employee accessed SNSs once? Occasionally? Monthly? Weekly? Daily?) and the length of time spent on these sites (1 hour per day? 1 hour per week? 5 hours per day?). Then, as secondary criteria, courts also took into consideration other circumstances which could influence the decision: the content accessed (Does it pose a threat to the security of the network? Is it compromising?), or the eventual effects on the work of the employee (Was the employee distracted and committed mistakes as result of the social media use?). Then, if in consideration of the above criteria the use is not regarded to be excessive, the dismissal is not founded – even in cases when the internal regulation completely forbids the personal use.

However, one important observation must be made in the light of the employees' possibility to use work equipment for private purposes to a non-abusive extent, even if the employer had prohibited such use: in relation to social media, these observations do not lead to the existence of an explicit right to use social media during working hours. Although certain authors came to the conclusion that employees have the right to use social media during working hours,[1434] it is more appropriate to interpret these provisions as aiming to ensure *certain* kind of personal communication (and not being completely cut off from the outside world and being able, for example, to make an urgent personal call or e-mail), but

---

the safety of the service provided. (18/2018. számú munkaügyi elvi határozat) In this case, the Curia took into consideration that the employee was hours late, without giving reason for his absence, misinformed his superior, and it also considered the consequences of the behaviour.

[1434] For example, *Blandine Allix* interpreted the relevant provision of the FLC, the observations of the CNIL and the Nikon decision as giving the right to the employee to consult his/her Facebook account during working hours even if the employer prohibited such a use. Allix 2014.

not necessarily communication through social media.[1435] In this context, employees' right to privacy means that even at the workplace they do not cease to be human beings, and they can establish relationships with others. Therefore, the employer can decide to completely ban the use of SNS during working hours as long as other alternatives of communication (e.g. telephone, e-mail) are provided.

Section 2. New challenges brought by social network sites

The analysis so far was based on the regulation of Internet and e-mail use. However, SNSs present certain characteristics that are specific to them, compared to the traditional monitoring of e-mail and the Internet – which must be addressed in order to assess whether existing rules adequately regulate the matter or adjustments are needed. Besides the most traditional situation addressed in Section 1 (employees connecting to SNSs from the employer's equipment, during working hours), SNSs add certain other criteria to the discussion that must be examined. *§1* will analyse these characteristics, while *§2* will enumerate that in the light of these challenges, how SNS use during working hours should be regulated.

§1. Issues specific to SNSs

In contrast to regulating the "default situation" – covering scenarios when the employee accesses SNSs from the work computer provided by the employer, during working hours, with the employer's power to restrict SNS use – SNSs have certain characteristics that must be examined. Notably, SNSs are not only accessed from work computers, but due to the proliferation of mobile devices (such as smartphones, tablets or smart watches), employees can consult these sites from their *own* devices. So, *first*, it must be addressed whether it constitutes a substantial difference if the employee does not use the employer's equipment, but his/her device to access SNSs? *Second*, it will be examined whether the time of consulting SNSs has importance: namely, the case of employees accessing these sites during *work pauses* will be addressed. *Then*, it will be highlighted how SNSs can become a means to reveal conducts breaching the employee's obligation to work.

(A) Using the employee's device

It is necessary to examine whether there is a difference if the employer aims to ban the use of SNSs during working hours from the *employees' own device*? A challenge brought by technological development is that SNSs can be used not only on computers, but also on mobile devices such as smartphones, tablets or even smartwatches. These days more and more people have their own smartphones and other devices, which they take with themselves everywhere – to the workplace, too. It is also not uncommon that individuals have their own mobile Internet subscription, so the blocking of SNSs (e.g. through not providing Wi-Fi or blocking the access to SNSs) by the employer is not an option in these cases, as employees can access these sites from their own devices. Although the employer

[1435] Baugard 2015. pp. 77–78.

has the right to regulate and monitor the use of SNSs on *his/her* computer, it is necessary to examine whether the scenario will be different when the device constitutes the property of the employee.

First, in the case of BYOD, employees bring their own devices with the purpose of carrying out their jobs.[1436] In the case of BYOD, the employer and the employee jointly agree that instead of the employer providing the necessary working conditions as required by labour law, the employee's own device will be used for it. In such a case, it is obvious that personal use cannot be completely prohibited, and also during the monitoring the employer must pay increased attention to the employee's right to privacy and right to data protection.[1437]

From the phenomenon of BYOD it must be differentiated when the employee uses his/her personal device for personal reasons – still with possible professional consequences. It was already established that in the case of the employer providing the device, he/she has the right to ban personal use and to monitor compliance with the regulation – the detailed rules relating to monitoring will be examined in Chapter 2. However, if the employee uses his/her own device to access SNSs during working hours, these rules will be slightly different, especially in the field of monitoring compliance.

Despite the employee being the owner of the device, the employer can still ban the personal use, as irrespective of who owns the device,[1438] surfing on SNSs during working hours breaches the employee's obligation to work and to be at the disposal of the employer.[1439] Therefore, as such personal use still comes at the expense of working hours, it can be sanctioned.[1440] However, their monitoring will be possible to a lesser extent compared to the use of the employer's devices.

(B) Work pauses

The possible personal use during work pauses also has a close connection with the ownership of the device. When being the owner of the equipment, the employer is entitled to define the rules relating to the use of such devices and is even entitled to prohibit the employee to access SNSs from this equipment. As in this scenario the employer is the owner, this prohibition can be extended to work pauses as well.

However, the situation might be different when the employee intends to access SNSs from his/her own equipment during work pauses. In Hungary, working pauses are not considered to be working time:[1441] during these periods employees are free from performing work or be at the disposal of the employer, making personal use (on their own devices) possible.[1442] In France, as a main rule, working pauses should not be considered as effective

---

[1436] WP29: *Opinion 2/2017*. p. 16.

[1437] The HLC explicitly regulates this issue and states in Subsection (5) of Section 11/A that if the parties agreed that the employee is going to use his/her own equipment for work, the employer can only inspect information relating to the employment relationship.

[1438] Kun 2013. p. 13.

[1439] Proskauer Rose LLP 2014. pp. 7–8.

[1440] Ray 2018. p. 324.

[1441] Subsection (3) of Section 86 of the HLC

[1442] Kártyás – Répáczki – Takács 2016. p. 78.

working time,[1443] meaning that the employee is free to decide how to spend them. Also, when calculating time spent with personal activity, the already presented (French) cases relating to the personal use of the Internet did not take into consideration lunch breaks, implying that personal use during this period is not considered as a breach of obligation and that the employee is free to decide how to spend these pauses.[1444] This means that theoretically, during work pauses the employee should be free to access and use social media from his/her device.

However, *Attila Kun* provided a more nuanced picture of pauses and personal use of one's own equipment. He pointed out that even if the use does not directly violate the employee's obligation to work (e.g. checking Facebook during a pause), the use of social media can have an indirect effect on work, by impairing employees' attention. It is one of the employees' obligation to "appear at the place and time specified by the employer, *in a condition fit for work.*"[1445] The employee is fit for work if he/she is well-rested, is not under the effect of alcohol or drugs and can concentrate on working with all his/her senses, in the right physical and mental condition.[1446] This condition traditionally concerned the consumption of drugs and alcohol and their possible effects on working – but in the 21st century the overuse of SNSs or being overexposed to screens constitute more recent cases. The mass of ever-changing information on social media might result in the fact that the employee receives more information than he/she can process, causing fatigue and reducing concentration, having a direct effect on work.[1447, 1448]

As concerns the break time and the use of social media, it also has to be taken into consideration that the employer has the *obligation to ensure safe working environment*, and the employer has to monitor whether workplace safety rules are respected.[1449] Different regulations[1450] aim to ensure the protection of employees in the case of work with display screen equipment, requiring the employees to make pauses from staring at a screen. Therefore, if an employee works with a computer and spends his/her break looking at the screen of his/her smartphone surfing SNSs, the workplace safety regulations are infringed, as the employer has to ensure breaks for the employee from staring at a screen.[1451] If the employee works on a computer and then uses his/her pause to access social media from his/her smartphone, no pause will be ensured, resulting in the breach of labour law regulations.

In conclusion, in addition to being able to regulate the personal use of the equipment provided by the employer, in theory the employer also has the possibility to prohibit such use from the employees' own devices during working hours (and even during work pauses). The reason for this is that regardless of the ownership of the device, the employee must

---

[1443] Unless during these periods the employee stays at the employer's disposal and complies with his/her guidelines, without being able to freely attend to his/her personal affairs. Article L3121-2 and Article L3121-1 of the FLC

[1444] See, for example: CA Nîmes, 2 avril 2013, n° 12/02146

[1445] Emphasis added by the author. Source: item a) of Subsection (1) of Section 52 of the HLC

[1446] https://jogaszvilag.hu/cegvilag/mit-jelent-munkara-kepes-allapotban-lenni/ (Accessed: 7 January 2020)

[1447] Kun 2013. p. 13.

[1448] See the already presented case, in which the Court of Appeal of Nîmes established the connection between professional mistakes made by the employee and the excessive personal use of the Internet. Source: CA Nîmes, 2 avril 2013, n° 12/02146

[1449] Subsection (4) of Section 51 of the HLC and Article L4121-1 of the FLC

[1450] Article R4542-4 of the FLC and 50/1999. (XI. 3) decree of the Ministry of Health on the minimum health and safety requirements for work with display screen

[1451] Németh 2013a. p. 40.

respect working hours, and must stay in a condition fit for work, along with respecting workplace safety regulations – which might be influenced by the use of SNSs. However, in practice, if the (reasonable) personal use does not come at the expense of the employee's ability to work or does not lead to an extensive use of technology, the employer might consider allowing personal use on the employee's device given the realities of being an employee in the 21st century. According to my opinion, even if the employer decides to adopt a strict, prohibitive policy, in most cases, it should not exclude the possibility for the employee to have a glance at social media from his/her own device.

(C) SNSs as proof of unauthorized absences

Besides surfing on SNSs during working hours, SNSs might also contribute to revealing other types of activities at the expense of working time: in several cases employees on sick leave are caught on social media being a picture of perfect health. However, this activity is not directly connected to our main subject, but rather to the subject of social fraud; as in such a case the use of SNSs itself does not breach any employee obligation but rather reveals those breaches inadvertently. Still, due to the possible proliferation of such discoveries, this subject must be at least briefly addressed.

In those cases the employee's conduct comes at the expense of working hours – similarly to the already discussed scenario, at the workplace during working hours, when the employee surfs on Facebook instead of working – but outside the workplace. Such cases include employees reporting being sick, but in reality being in perfect health, or making false excuses in order to be able to skip work (e.g. funeral of a relative, etc.). Such behaviour existed before SNSs as well, however, due to these platforms, their discoverability have considerably changed, as SNSs sometimes can expose these conducts.

Even before SNSs, it was possible to reveal that the employee was on vacation in spite of claiming to be on sick leave; SNS made it much easier to publish and to access such information. However, early examples of self-exposure from the pre-SNS era also exist: see, for example, the case of a French employee who – while being on sick leave – went abroad for vacation and sent a postcard to his employer from Yugoslavia. As a result of his act, he was dismissed, but the Court of Cassation stated that the dismissal was not justified, as the employee was in a period of suspension of his employment contract, thus the charges against him did not constitute a breach of the obligations under the employment contract as the employee had not committed an act of disloyalty.[1452]

However, SNSs made a change in this field, and can highly contribute to revealing conducts breaching working hours, which is demonstrated by the growing number of cases arising. For example, see the case of a *French employee* who posted to an SNS when returning from sick leave: "after two weeks and three days of holiday it's going to be very hard…", suggesting that instead of being sick, he went on a holiday. However, the court found that as the employee could provide medical documentation for the concerned period, the absence was medically justified, therefore his act could not constitute a misconduct.[1453, 1454]

[1452] Cour de cassation du 16 juin 1998, n° 96-41558

[1453] CA Amiens, 21 mai 2013, n° 12/01638

[1454] Such cases are not only rising in France or in Hungary: see, for example, the *case of Kevin Colvin*, who was an intern at Anglo Irish Bank' s North American arm and told his manager that he had to be absent from work

Except for very special cases,[1455] it is not the use of SNS itself that breaches the employees' obligation in such a case; instead, social media serves as a *tool* revealing the breach of obligation. In such a scenario, the employee violates his/her obligation to work and to be at disposal, as exemption from these obligations is only possible under determined circumstances. Therefore, deceiving the employer through such conduct can even constitute the basis for dismissal.[1456] However, when using such posts for decision-making, attention should be paid to the enforcement of the data quality principles[1457] because information obtained from social media is often not reliable,[1458] as it was already presented in relation to hiring.

§2. Additional factors to be considered

It was seen that from a legal point of view, the employer is entitled to decide how to regulate the personal use of SNSs: it is up to him/her to decide whether personal use is allowed or not and if yes, to what extent. However, in addition to this legal background, additional, non-legal arguments should also be considered when deciding whether to adopt a permissive or a more prohibitive regulation.

First of all, when deciding in relation to personal use, what should be taken into consideration is the exact job that the employee performs, as depending on the exact work tasks, the possibility of a permissive regulation might be automatically excluded. In jobs where constant attention is required (for example, a doctor performing an operation, a worker at a production line or a bus driver, etc.) using SNSs during work is not optional. The employer has the freedom of deciding what regulation to adopt mostly in the cases of employees performing clerical work.

As it was demonstrated by the examined case law, employees can be creative when abusing their "rights" and can spend a considerable amount of *time* on these platforms. This is contrary to the employer's legitimate interests, as he/she is lawfully entitled to expect employees to spend their working hours working. Checking SNSs during working hours is realised at the expense of working hours. Also, it can contribute to decreasing productivity, through fragmenting the attention of the employee, who might as a result

because of a family emergency. However, photos of him posted to Facebook revealed to his supervisors that instead of a family emergency, he attended a Halloween party, dressed as a fairy. He was dismissed due to his action. (Funk 2011. p. 176.) In the case *Gill v SAS Ground Services UK Limited* Mrs. Gill worked as a customer services representative for SAS Ground Services, while in her free time she acted and modelled, and in relation to these activities possessed a Facebook account. She went on sick leave for reasons related to her health, but her Facebook entries and YouTube videos revealed that during this period she attended the London fashion week, where she auditioned 300 models and choreographed a fashion show. She was dismissed for gross misconduct. The tribunal held that this evidence was sufficient to state the misconduct. https://www.xperthr.co.uk/law-reports/in-the-employment-tribunals-august-2010/104153/#gill (Accessed: 20 September 2018)

[1455] See, for example, the case of a Swiss woman who said to her employer that she was sick, complaining to have migraine and that she needed to rest in a dark room without using any computer: then her colleagues reported her seen active on Facebook and changing her status. http://arsboni.hu/kozossegi-media-es-munkajog-kereszttuzeben/ (Accessed: 27 February 2018)

[1456] Horváth – Gelányi 2011. p. 61.

[1457] NAIH/2016/4386/2/V.

[1458] For example, it is possible that the employee on sick leave uploads a holiday picture to Facebook – but taken months before.

commit professional mistakes. Also, as it was referred to, excessive use of such devices can have consequences on the health of the employees, which can result in them leaving on sick leave. Such use can also endanger network security, entails the risk of receiving viruses and also contributes to the deterioration of the device.

The negative effects associated with the extensive use of technology are acknowledged by a growing number of individuals and organizations, encouraging initiatives such as organizing digital detoxes at workplaces. Instead of simply prohibiting SNS use, the employer can actively encourage employees to spend time away from screens by organizing a digital detox, which might turn out to be beneficial for both parties.[1459]

In spite of being free to decide whether employees can use social media at the workplace or not, it should be taken into account that in today's information society it might be *unrealistic* to completely ban its personal use. Today – whether we accept it or not – it has become a reality that individuals, especially younger generations,[1460] spend a considerable amount of time on the Internet and on SNSs and they would not like to be completely cut off from these sites during working hours. It has even become an expectation from employees not to be completely cut off from these platforms while being at work – and a strict prohibitive regulation can even deter young employees.[1461] Checking these profiles occasionally for 5–10 minutes would not necessarily harm the employer, instead, it can even contribute to productivity.[1462] Also, a more permissive regulation can promote trust between the parties, and therefore contribute to a better work environment

Besides employees' expectation, it might also be taken into consideration that the *boundaries between work and private life are more and more blurred*. As employees can receive a work-related e-mail during the weekend or can finish a task (from their own computer) at home in the evening, they might also wish to check their social media profiles during working hours, or just see on the newsfeed what happened to their contacts.[1463] Employees might even consider these "Internet pauses" as a reward in exchange for the stress that they are subject to or in exchange for the overtime, when work invaded their personal lives.[1464] Today it seems unreasonable to completely cut off employees from social media during working hours.

The *technical feasibility* of a ban might also pose certain issues. Since a myriad of these platforms exists, the employer would probably be able to block only the most widely used ones (e.g. Facebook or Instagram), but not all of them – giving employees the possibility to bypass the ban and access sites that were not blocked. Also, a strict regulation might only urge employees to use their own devices to check SNSs – making it more difficult for the employer to monitor it.[1465]

[1459] Such measures might include tech-free meetings, communicating to employees the importance of regular breaks, organizing screen-free activities (e.g. yoga class) setting up of a buddy system, etc. https://hrdailyadvisor.blr.com/2018/07/24/6-ways-introduce-digital-detox-employees-boost-productivity/ (Accessed: 8 January 2020)

[1460] As *Jean-Emmanuel Ray* put it neatly, for young people born with the Internet, "Not being able to be connected is like working in an office without a window." Ray 2009. p. 23.

[1461] Sanders 2013. p. 170.

[1462] https://www.adweek.com/digital/how-social-media-actually-boosts-efficiency-in-an-office-environment/ (Accessed: 27 July 2019).; https://hbr.org/2018/05/employees-who-use-social-media-for-work-are-more-engaged-but-also-more-likely-to-leave-their-jobs (Accessed: 27 July 2019).

[1463] Kajtár 2015b. p. 269.

[1464] Denier 2003. p. 32.

[1465] http://www.pordesresidential.com/wp-content/uploads/2010/11/1-19-2011-miami-herald-biz.pdf (Accessed: 10 March 2017).

To conclude, it can be stated that primary expectation towards the employee is to work at the workplace, and employers both in Hungary and in France have extensive powers to define the extent of the personal use of the employer's equipment. However, completely banning the personal use of the equipment might raise questions related to privacy as the right to privacy comprises the right to establish relationships with others – which is often done through different tools of ICT, such as SNSs.

In France, regulation seems to be more permissive, as the majority of scholars state that a complete ban would be disproportionate: the right to privacy requires that the employee has certain ways of establishing relationships with others, completely forbidding every possibility for personal communication is not allowed. Meanwhile in Hungary, according to the major opinion, legally it seems possible that the employer completely bans the personal use of the employer's equipment, even though several scholars have expressed their opinion – according to my view, correctly – according to which a complete ban would be unrealistic. It is also worth noting that even in cases when the employee uses the Internet/e-mails/SNSs for personal purposes despite the explicit ban imposed by the employer, the use is tolerated by courts if it stays reasonable and is not abusive. What is considered to be reasonable use depends on the exact circumstances: (French) courts usually took into consideration the time spent on these sites, the frequency of visiting them, their nature, whether they adversely affected the employee's work performance.

In addition to the legal considerations, a complete ban faces technical difficulties due to the high number of SNSs and to the growing number of employees owning portable electronic devices. It would also be unrealistic in the 21st century. For all the above reasons, it might be more expedient for the employer to tolerate and allow personal use to a reasonable extent, under specific conditions set by him/her, tailored to the characteristics of the workplace. It is crucial that the employer clearly informs employees about the regulation that he/she chooses to apply and about the exact limits of what is considered to be reasonable personal use by him/her.

The employer has the right to decide whether to allow personal use (and to what extent) or whether it is prohibited. When making and implementing this decision, first, the employer should decide how he/she would like to regulate the personal use of SNSs. In the light of the above, (in most cases) it is recommended that the employer opts for a more permissive regulation, but strictly lays down its condition in order to avoid abuses. If personal use is allowed, it is crucial that employees are aware of the exact rules of such regulation. Regularly informing and educating employees through meetings or trainings might be a good way to inform them about the employer's expectations,[1466] or the employer can lay down the rules in an internal regulation or in a social media policy.[1467] Rules relating to personal use must be clearly established, so that employees can comply with them. Therefore, stating that a reasonable use is allowed is not enough, it is highly recommended that the employer sets the *exact* limits and time periods (e.g. 20 minutes daily, or only during pauses, etc.).

[1466] http://www.pordesresidential.com/wp-content/uploads/2010/11/1-19-2011-miami-herald-biz.pdf (Accessed: 10 March 2017)

[1467] See more on them in Chapter 2.

Chapter 2: Employees' right to data protection: monitoring employee use of SNSs during working hours

The second aspect of the subject is that after imposing the rules on the personal use of SNSs, how can the employer *monitor* whether employees comply with the regulation? As information relating to the use of the Internet/e-mail is considered to be personal data, data protection requirements shall apply to the monitoring of the personal use of the Internet/SNSs.[1468] When it comes to the monitoring of communication (e-mail or instant messaging services), an additional aspect has to be considered, namely that it is not solely the employee's right to privacy/right to data protection which is affected by monitoring, but also the sender's or recipient's rights.[1469]

While regulating the use of work facilities for personal purposes raised more privacy-related issues, a data protection approach is more emphatic in the case of monitoring compliance with the regulation. After determining that the employee's right to privacy does not cease to exist within the workplace – even in the case of the prohibition of the personal use of work facilities –, the determination of the extent of monitoring can be better assessed through a data protection approach. The limits and conditions of such monitoring can be identified through the application of data protection principles, such as transparency, purpose limitation, necessity and proportionality.

Chapter 2 will follow a similar *structure* as Chapter 1: *first*, the already elaborated rules on Internet and e-mail monitoring will be discussed, and *then* the specific characteristics of SNSs will be taken into consideration in relation to the existing legal framework.

Section 1. Starting point: monitoring of the Internet and e-mail

The right to monitor is inherent to the employment contract: its existence is unquestionable, though determining its lawful extent might pose certain questions.[1470] Although the employee is entitled to the right to respect for private life even within the workplace, it does not override the employer's right to access work computers.[1471] Again, similarly to what was already discussed in Chapter 1, *(§1)* first, the European framework will be examined, *(§2)* followed by the national regulations.

§1. Outlook to European law

When addressing the question of the monitoring of the use of the Internet/e-mails, observations are made as regards the extent and the exact rules relating to such monitoring,

---

[1468] WP29: *Opinion 8/2001*. p. 13.; Szőke et al. 2012. p. 28., p. 34.; CNIL: *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010. p. 2.

[1469] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 21.; Szőke et al. 2012. p. 28.; Hegedűs 2005. p. 186.

[1470] Vigneau 2002. p. 355.

[1471] Contamine 2013. p. 157.

determining how data protection requirements should be respected. First, *(a)* the WP29's documents and then the *(b)*ECtHR's case law will be addressed in detail.

(A) EU perspective: the WP29's documents

Although the principles laid down in *Opinion 8/2001* are valid in the case of e-mail and Internet monitoring, it was the *2002 Working document* in which the WP29 has addressed in detail the question of monitoring of e-mail and Internet use at the workplace. The Working document also points out the importance of the general data protection requirements, and then addresses the question of e-mail and Internet monitoring. In its *Opinion 2/2017*, the WP29 enumerates the most common data protection problems specific to the employment context[1472] and takes into account the technological development that occurred since the adoption of its previous documents, while stating that the conclusions laid down in the Working Document still remain valid.[1473] Under the item "*Processing operations resulting from monitoring ICT usage at the workplace*", Opinion 2/2017 expressively deals with e-mail and Internet monitoring at the workplace.

The WP29 emphasizes the importance of proportionality, transparency (e.g. by adopting policies).[1474] The WP29's general standpoint is that instead of monitoring and detection, the emphasis should be placed on *preventing the misuse* of the employer's equipment.[1475] This could be achieved by using programs that remind the employee of the misuse (e.g. warning windows, which pop up and alert the employee).[1476] This can suffice to prevent the misuse and the employee's visit to the website can be avoided. It follows from the requirement of subsidiarity that monitoring might not even be necessary, as the blocking of certain websites – for example, SNSs – can prevent employees from personal use.[1477]

According to the principle of *proportionality* and *data minimization*, the least intrusion possible must be made, so it is advisable that the employer avoid automatic and constant monitoring, unless it is necessary to ensure the security of the system.[1478] When monitoring becomes necessary, due to the principle of proportionality, it should be first limited to the monitoring of traffic (number of mails sent, types of attachments, etc.), instead of monitoring the content of the sites visited or the content of the messages sent.[1479] Often, accessing the name of the sites visited is enough to detect the misuse of the computer, it is not necessary to know exactly what content the employee looked for there or, in several cases, a misuse can be detected by accessing traffic data (such as the participants and time of the communication) without accessing the content.[1480]

[1472] European Union Agency for Fundamental Rights – Council of Europe 2018. p. 332.
[1473] WP29: *Opinion 2/2017*. p. 12.
[1474] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 14.
[1475] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 4.; WP29: *Opinion 2/2017*. p. 15.
[1476] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 5.
[1477] WP29: *Opinion 2/2017*. p. 15.
[1478] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 17.
[1479] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. pp. 4–5., pp. 17–18.
[1480] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. pp. 17–18.

As concerns the *monitoring of communication*, it poses an additional challenge that two persons' personal data are processed: the recipient's and the sender's. The privacy of both parties must be respected: in this regard, the respect of the rights of individuals outside the workplace might present a challenge.[1481] However, in cases when the employee is given an e-mail account for purely personal use or is allowed access to a web-mail account, stricter rules apply: the monitoring of the content of messages is not legitimate (except for very limited cases – e.g. in relation to criminal activities), as the secrecy of correspondence outweighs the employer's legitimate interests in monitoring.[1482]

Often, the distinction between professional and personal communication is difficult (e.g. in the case when the employee uses his/her professional e-mail for personal purposes). However, compared to e-mail monitoring, a significant difference can be observed when it comes to SNS use: usually SNSs are used for personal purposes and only in exceptional cases for work. Therefore, as a main rule, communication taking place on SNSs is personal – and the conditions of monitoring should be more severe.

The principle of *transparency* requires employees to be informed regarding workplace monitoring.[1483] The WP29 also suggests that the employee is informed as soon as misuse of the equipment is detected, in order to prevent future misunderstandings.[1484]

(B) CoE: the ECtHR's case law

Before addressing the more recent case law of the ECtHR, the Halford and Copland cases must briefly be mentioned, as both of them relate to the monitoring of employees. In the *Halford v. the UK* (1997) case the ECtHR ruled that phone calls made from business premises are covered by Article 8 of the ECHR and their interception constitutes an interference with Ms. Halford's right to privacy.[1485] The ECtHR emphasized the importance of transparency in relation to the contracting states providing clear information in their legal order on the terms and conditions of such a (secret) monitoring.[1486] In the Halford case it was held that no adequate provision in domestic law existed, resulting in the violation of Article 8.[1487]

In the *Copland v. the UK case*[1488] Ms. Copland's telephone, e-mail and Internet usage was subjected to monitoring, without informing the applicant about it. Again, the ECtHR held that such communications are covered by Article 8 of the ECHR and that such monitoring is not in accordance with the law, with regard to the lack of notification.[1489] Transparency

---

[1481] In the cases of these individuals the employer should make reasonable efforts to inform them of the monitoring taking place if they can be affected by it. A solution to achieving this might be to insert warning notices to the outbound messages. WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. pp. 17–18.

[1482] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 21.

[1483] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. pp. 14–15.

[1484] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 15.

[1485] ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 44., par. 48.

[1486] ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 49.

[1487] ECtHR: *Halford v. the United Kingdom*, application no. 20605/92, 1997. par. 51.

[1488] ECtHR: *Copland v. the United Kingdom*, application no. 62617/00, 2007

[1489] European Union Agency for Fundamental Rights – Council of Europe 2018. p. 332.

is crucial, but Ms. Copland has received no warning that her communication would be subject to monitoring,[1490] resulting in the violation of Article 8.[1491]

(a) Case of Bărbulescu v. Romania

The Bărbulescu case defined the conditions that must be respected during employee monitoring.[1492] Although the ECtHR's Grand Chamber ruled that national authorities did not strike a faire balance between the interests at stake and violated Article 8, not ensuring adequate protection of the applicant's right to respect for his private life and correspondence,[1493] the existence of the employer's right to monitor remains uncontested. States have a broad margin of appreciation in determining the conditions of employee monitoring. However, such a monitoring cannot be limitless, proportionality and other safeguards are essential in order to make the monitoring lawful.[1494]

One of the significances of the decision is that the ECtHR provided an evaluation grid[1495] and, in paragraph 121 of the judgement, elaborated 6 criteria that should be taken into account when assessing whether employee monitoring was lawful or not. These are:

- *prior information*: whether the employee has been notified of the possibility of monitoring correspondence and other communications, and of how this monitoring is implemented. The information should be provided prior to the processing and should be clear,
- *extent of monitoring*: what is the extent of the monitoring and the degree of intrusion into the employee's privacy? Distinction should be made between monitoring the content of communication or the flow of information. Also, it shall be assessed whether the monitoring's scope was limited in time and space, the number of people having access to the results, and whether all communications were subject to monitoring or only a part of them,
- *employer's legitimate interests*: whether the employer has legitimate reasons to justify the monitoring and the access to their content,
- l*ess intrusiveness*: whether the use of less intrusive methods would have been possible instead of accessing the content of communication,
- *consequences for the employee*: the consequences of the monitoring and how the result of the monitoring will be used by the employer,
- *safeguards*: whether the employee was provided adequate safeguards.

The case and the decision attracted considerable attention of the media,[1496] and it is an important milestone regarding employee monitoring. As the decisions of the ECtHR are binding for the contracting states, this decision has crucial importance. Especially two conclusions can be drawn: *first*, it was reinforced that the employee is entitled to the right to privacy: even in cases when he/she violates the ban on personal use, monitoring

---

[1490] ECtHR: *Copland v. the United Kingdom*, application no. 62617/00, 2007. par. 42.
[1491] ECtHR: *Copland v. the United Kingdom*, application no. 62617/00, 2007. par.44
[1492] Costes 2017. p. 35.
[1493] ECtHR: *Bărbulescu v. Romania*, application no. 61496/08, 2017. par. 141.
[1494] Gheorghe 2017. p. 64.
[1495] Peyronnet 2017.
[1496] In Hungary, especially after the decision of 2016, news portals were publishing articles entitled "*From now on your employer can read your e-mails*" etc. Kártyás – Kozma-Fecske 2016. p. 16.

should be subject to strict conditions; and *second*, the ECtHR provided important criteria regarding what aspect shall be particularly assessed when it comes to the legitimacy of such monitoring. By this, the ECtHR struck a fair balance between employees' rights and the employer's legitimate interests.[1497] Although the adaptation of French law to this decision should not pose problems, as in the case law of the Court of Cassation the balance between these two sides is already ensured in its decisions,[1498] as well as in Hungarian law – [1499] providing the criteria for the monitoring represents a significant guidance for both countries.

(b) Case of Libert v. France

In the *Libert v. France (2018)* case[1500] the ECtHR confirmed the French regulation by judging that the authorities struck a fair balance between the employee's rights and the employer's interest.[1501] The ECtHR ruled that there was no violation of Article 8, as the authorities acted within the margin of appreciation provided to them. The ECtHR noted that a balance had to be found between the employee's right to respect for private life and the employer's right to ensure that employees use the equipment provided by him/her for executing their work in compliance with their contractual obligations and applicable regulation.[1502]

The French courts applied the already elaborated rules in national jurisprudence, according to which employees' files stored on equipment provided by the employer are presumed to be of professional nature, allowing the employer to access them – unless the employee explicitly marks them as personal.[1503] The opening of personal files was only permitted in the case of a risk or a particular event, in the presence of the employee or if he/she has been properly notified of it.[1504]

As soon as a computer is likely to be used for personal purposes, the monitoring of files potentially relating to the private life of the employee constitutes an interference in his/her private life, therefore, it must comply with the requirements making such an interference legitimate.[1505] The ECtHR held that as French law described precisely in which circumstances and in which conditions such a measure was permissible, it complied with the requirements of Article 8, as it was in accordance with the law, pursued a legitimate aim in a democratic society.[1506] The ECtHR was of the opinion that such a measure aimed to guarantee the rights of a third party, the employer, recognizing his/her legitimate interest in ensuring that employees use computer equipment that the employer provided them for work

---

[1497] Andriantsimbazovina 2017. p. 23.

[1498] Andriantsimbazovina 2017. p. 23.; Ray 2018.
However, according to *Joël Colonna* and *Virginie Renaux-Personnic*, while in the case of personal messages, French law is indeed compatible with the decision, it is not necessarily the case when it comes to the monitoring of professional mail. Colonna – Renaux-Personnic 2017. p. 45.

[1499] Rózsavölgyi 2018. p. 48.

[1500] ECtHR: *Libert v. France*, application no. 588/13, 2018

[1501] Loiseau 2018. p. 11. (Page number referring to the online version of the article downloaded from: https://www.lexis360.fr)

[1502] ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 46.

[1503] ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 44.

[1504] ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 44.

[1505] Marchadier 2018. p. 7. (Page number referring to the online version of the article downloaded from: https://www.lexis360.fr)

[1506] Nasom-Tissandier 2018. p. 13.

to execute their tasks, in accordance with their contractual obligations and with applicable regulation.[1507] These measures were accompanied by adequate safeguards guaranteeing the respect of employees' rights, as the opening of personal files was only permitted in limited circumstances – both prescribed by regulation and through the application of the courts.[1508] Therefore, the way in which courts addressed the case was in accordance with Article 8.[1509]

The *conclusion* that can be drawn from the ECtHR's relevant case law is that the employer is indeed entitled to monitor employees. However, such a monitoring cannot be limitless; it must respect employees' rights.[1510] It must meet the criteria such as being necessary, set by legal regulations, and the procedure must be transparent. With regard to SNSs, it means that the employer is entitled to monitor their use, however, only to a necessary extent, in order to achieve a legitimate purpose and only through giving detailed information to the employee. The scope of these criteria is further examined in national regulations.

§2. Regulation at the national level: France and Hungary

After examining what the "European norms" relating to monitoring are, it will be examined how France and Hungary regulate the question of monitoring SNS use at the workplace during working hours. The above-mentioned WP29 documents regulate the most important rules regarding the monitoring of employees' Internet use, while the relevant ECtHR case law provided the most important principles. However, these general requirements and principles must be assessed in a more detailed way – which was achieved at the national level.

First, it will be presented how France and Hungary decided to guarantee employees' right to data protection, and then, how the data protection principles are enforced. As the general protection of employees' rights has already been presented (principle of necessity, proportionality, transparency, etc.), here, focus will be put explicitly on the enforcement of these principles in the case of Internet and e-mail monitoring.

(A) The outlines of regulation

The *FLC* contains no direct provision in relation to the electronic monitoring of employees or their communication or Internet use. As it was already addressed, in France, the Nikon decision laid down the principle that the employee has the right to respect for private life even while being at the workplace.[1511] This protection was aimed at communication marked as personal,[1512] resulting in a distinction between personal and professional communication.[1513] However, this right is not without limits, the employer, as the person responsible for the

[1507] ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 46.
[1508] Sipka – Zaccaria 2018. p. 46.
[1509] ECtHR: *Libert v. France*, application no. 588/13, 2018. par. 53. Also see: Loiseau 2018. pp. 30–37.
[1510] Sipka – Zaccaria 2018. p. 47.
[1511] Cass. soc.,2 octobre 2001, n° 99-42.942
[1512] Ray – Bouchet 2010. p. 47.
[1513] Kocher 2013. p. 131.

functioning of the workplace, has the right to monitor employees.[1514] In the workplace the employee is expected to work for his/her employer: therefore, the employer can access communication conducted at work, unless it is explicitly marked as personal.[1515] In order to determine the nature of the communication, a presumption was established, according to which unless explicitly marked as personal, the communication is presumed to have a professional nature.[1516] Then courts provided more guidance in relation to the application of this presumption.

According to *jurisprudence in France*, employers are entitled to monitor employees' activities during working hours, only their secret monitoring is prohibited.[1517] Following from the rights and obligations of the parties, the employee's activity performed on the employer's equipment is presumed to have a professional character,[1518] both e-mails[1519] and Internet[1520] connections. E-mails can be opened without the presence of the employee, and Internet connections can be consulted. The exception is when the *e-mail message* is clearly marked as personal.[1521] The employee can identify e-mail as personal, for example, by placing a "warning" into the subject of the message or by creating a separate, personal folder within the account. Correctly identifying personal mails is crucial for the employee, as stricter rules apply to them: the Court of Cassation stated that "*[…] unless there is a risk or a particular event, the employer may only open messages stored on the hard drive of the computer identified as personal by the employee in the presence of the employee or if he/she has been properly notified of it[.]*"[1522] This requirement applies in the case of accessing the employee's SNS account as well: according to different courts,[1523] the employer can get to know the content of the employee's Facebook account only in the presence of the employee – otherwise this proof will be considered unfair.

Internet connections from the work computer during working hours are presumed to be of professional nature – without the possibility to identify them as personal –, so the employer can look into them for the purpose of identifying them, without the presence of the employee.[1524] Therefore the employee does not have the opportunity to mark the connection to Facebook as personal – it will automatically be presumed professional.

The *CNIL* also emphasized that employers are indeed entitled to limit and regulate how employees can use work devices and are entitled to monitor such a use,[1525] through, for example, detecting viruses, filtering unauthorized sites, prohibiting downloading, monitoring the size of messages sent/received, etc.[1526] It also confirmed that by default employees'

[1514] Michel 2018. p. 1. (Page number referring to the online version of the article downloaded from: https://www-lextenso-fr)

[1515] Ray 2007. p. 957.

[1516] Kocher 2013. p. 131.

[1517] Cass. soc.,14 mars 2000, n° 98-42.090

[1518] Cass. soc., 26 févr. 2013, n° 11-27372

[1519] Cour de cassation, civile, chambre sociale, 16 mai 2013, n° 12-11.866

[1520] Cour de cassation, civile, chambre sociale, 9 février 2010, n° 08-45.253

[1521] Cass. soc.,11 juillet 2012, n˚ 11-22.972; Cass. soc., 15 décembre 2010, N° 08-42486; Cass. soc., 16 mai 2013, N° 12-11866

[1522] Cass. soc., 17 juin 2009, n° 08-40.274

[1523] CA Rouen, Chambre sociale, 10 février 2015, n° 14/03335; CA Caen, 1re chambre sociale, 27 janvier 2017, n° 15/04417; CA Caen, 1re chambre sociale, 27 janvier 2017, n° 15/04402

[1524] Cass. soc., 9 juillet 2008, N° 06-45800; Cass. soc., 9 février 2010, N° 08-45253

[1525] CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018

[1526] CNIL: *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010. p. 18,; Bouchet 2004. p. 23.

activities conducted on the employer's equipment are presumed to be professional activity.[1527] If messages are marked as personal (for example, in the subject of the message or registering the message in a specific folder), they are going to be protected by the secrecy of correspondence.[1528] However, Internet connections and visited pages do not receive this protection, even if marked as favourites or added to certain bookmarks.[1529] The CNIL also expressed more detailed recommendation in relation to the enforcement of the different data protection principles, such as transparency or necessity – which is going to be addressed in part (B).

The amendment of the *HLC* in 2019 made a significant change in the electronic monitoring of employees. While prior to the amendment none of the provisions aimed explicitly at electronic monitoring, now Section 11/A contains direct provisions on the monitoring of work equipment. Besides declaring that unless agreed otherwise, work equipment can only be used for professional purposes,[1530] it adds that during monitoring, the employer can only consult data connected to the employment relationship.[1531] The HLC specifies what is considered to be data connected to the employment relationship: data which is necessary to monitor in compliance with the established rules relating to the use of work equipment.[1532] Therefore, the extent of monitoring will be influenced by whether the employer has authorized personal use: if personal use is allowed, the employer can only monitor whether the conditions of personal use are respected; and if personal use is prohibited, the employer can only consult data to an extent allowing him/her to assess whether the data relates to the personal life of the employee or to the professional life.[1533]

Prior to the amendment, the extent of monitoring was also determined according to whether the employer has authorized the personal use or not.[1534] In contrast to French regulation, protection is afforded not only to personal e-mails, but also to the authorised personal use of the *Internet*: if personal use was allowed, than it is not possible to monitor the use of the Internet.[1535] I share the view of *Mariann Arany-Tóth*, who adds that despite the authorization of personal use, monitoring should be allowed to control whether employees comply with the rules imposed on personal use.[1536]

Concerning *e-mail monitoring*, a distinction is made between personal and professional messages, and outgoing and incoming messages. However, as there is no established presumption created in order to establish whether the communication was professional or personal, the examination of the messages is conducted on a case-by-case basis. Also, in Hungarian regulation more attention is paid to the fact that individuals outside the organisation might be concerned by the monitoring, therefore their rights have to be respected

---

[1527] CNIL: *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010. p. 19.
[1528] Bouchet 2004. p. 25.
[1529] CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018
[1530] Subsection (2) of Section 11/A of the HLC
[1531] Subsection (3) of Section 11/A of the HLC
[1532] Subsection (4) of Section 11/A of the HLC
[1533] *T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról*, 2019. p. 102.
[1534] Kártyás – Répáczki – Takács 2016. p. 17.
[1535] Bankó – Szőke 2016. p. 65.; Pete 2018. p. 782. See also: ABI 570/A/2001; ABI 790/A/2001
[1536] Arany-Tóth 2016. pp. 111–112.

as well: the extent of monitoring can be wider in the case of professional messages and outgoing messages.[1537]

It was already referred to that in Hungary in the field of employee monitoring, the practice of the Hungarian data protection supervisory authority bears special significance, acting as veritable case law.[1538] As it was already mentioned, the *NAIH* issued two crucial documents in the field of employee monitoring: *Recommendation on the basic requirements of electronic monitoring at the workplace* (2013) and *Information notice on the basic requirements on data processing at work* (2016), among which the second contains detailed rules relating to the monitoring of Internet and e-mail use.

In the information notice, first, the NAIH refined this position and stated that the employer is entitled to monitor whether employees comply with the internal regulation regarding the use of the equipment.[1539] Then, it recommended certain best practices and drew attention to the data protection requirements that must be respected during such a monitoring (e.g. legal ground, necessity, transparency), and provided guidance in relation to how exactly the employer can comply with them. These requirements and the possible solutions given to them will be further addressed in part (B).

(B) Data protection principles

IP addresses, e-mail addresses, the websites visited all constitute personal data. As a consequence, their monitoring must comply with labour law legislation and data protection regulation as well. Both the French and the Hungarian data protection supervisory authorities already refined what data protection requirements must be respected during the monitoring and provided recommendations to comply with such requirements. Notably, the principle of transparency and the principle of proportionality/necessity must be examined in detail.

(a) Principle of transparency

The general principle of transparency is also applicable when it comes to the monitoring of Internet/e-mail/SNS use at work. Regarding this principle, there are no differences compared to what was already presented: the principle of transparency requires that employees are aware of the processing prior to its start, and it is enshrined both at the international level and in French and Hungarian law. The covert surveillance of employees' activity on SNSs during working hours is not permitted.[1540]

In accordance with the principle of transparency, the *CNIL* emphasized the importance of informing employees about monitoring on several occasions.[1541] The CNIL also drew attention to the growing practice of adopting internal regulations, which can indeed be a good way of informing employees, raising awareness, reminding them what kind of

---

[1537] Bankó – Szőke 2016. p. 58.

[1538] Balogh et al. 2012a. pp. 12–13.

[1539] NAIH 2016. p. 30.

[1540] See, for example, the cases ABI 1012/K/2005-3, ABI 1723/P/2008, ABI 800/K/2008, ABI 235/K/2008 relating to the use of spyware, where the commissioner stated that the use of such a program is not compatible with the principle of proportionality and necessity.

[1541] CNIL: *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010. p. 18.

behaviour can represent a risk for the workplace.[1542] The NAIH also encourages the adoption of such regulations, as they can constitute an effective way of informing employees of their obligations and of the expectations of the employer relating to the personal use of workplace equipment, as well as the rules relating to monitoring.[1543]

As regards informing employees, it is also said that *prevention* is more favourable than detection. Prior information on the use of SNSs at the workplace has key importance, as it would allow employees to be aware of the existing regulation in the workplace and to comply with it – which might make it possible to prevent monitoring[1544] or misuses.[1545] In the case of using social media for long periods, pop-up windows, or even applications analysing the time spent on the Internet can help employees to realize that they approached or passed the time limit allowed by the employer. Regularly sending out reminders to employees regarding the rules on personal use can also be a recommended method.[1546]

(b) Principle of proportionality

Although the employer has the right to monitor, it should not be limitless: it is especially the proportionality principle that limits his/her rights during monitoring. In *France*, Article L1121-1 of the FLC aims to ensure that employee monitoring is proportionate to the aim sought and is not a means to discipline employees without any other purpose.[1547] As *Christiane Féral-Schuhl* remarks, in accordance with the principle of proportionality, employers should only monitor employees if the employee is suspected of abusive use, for example, because of abnormally long connections or an unusually huge amount of downloaded files.[1548] According to the CNIL, first, monitoring should be conducted retrospectively, at a global level (e.g. at the level of the whole workplace or a service), therefore the examination of individual connections of a certain employee could be avoided.[1549] Also, the use of key logger programs, or receiving an automatic copy of all messages is to be avoided.[1550]

In *Hungary*, the NAIH recommended the adoption of a staggered control system, where first looking at the subject and the sender can help to contribute to deciding whether the communication was of a professional or a personal nature – without having access to the content.[1551] It is important that the employer cannot have access to the content of personal communication, or the pages visited – even if the employee violated the policies relating to personal use.[1552, 1553] Having access to such content is allowed only if without that access

---

[1542] Bouchet 2004. p. 11.
[1543] NAIH 2016. pp. 25–26.
[1544] NAIH 2016. p. 25.
[1545] Kártyás – Répáczki – Takács 2016. p. 67.
[1546] NAIH 2016. p. 26.
[1547] Grynbaum – Le Goffic – Morlet-Haïdara 2014. p. 896.
[1548] Féral-Schuhl 2018. p. 415.
[1549] CNIL: *Guide pratique pour les employeurs*. Les guides de la CNIL, 2005. p. 11.
[1550] CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018
[1551] NAIH 2016. p. 26.
[1552] NAIH 2016. p. 27.
[1553] By stating that, the NAIH refined the previous practice, according to which the content of such a communication was accessible to the employer if he/she obtained the consent of both the sender and the recipient. (Szőke et al. 2012. p. 30.) As Szőke [et. al.] noted, inconsistencies could be found in the practice of the Data Protection Commissioner, mostly due to the uncertainties relating to the legal ground of processing. (Szőke et al. 2012.

it is not possible to establish whether the employee has breached the regulation related to personal use.[1554, 1555]

After narrowing down the search to professional messages, the employer can process more detailed information; but even in this case proportionality shall be respected and – depending on the exact circumstances – searches should be limited (e.g. in time, only to messages with an attachment, etc.). The employer should only have access after narrowing down the search as much as possible.[1556] As there is no presumption in Hungarian regulation, as a main rule, the presence of the employee is requested in order to avoid the possible confusion of professional and personal messages; the employee can then indicate if the message is personal, thus avoiding having access to the content of personal messages.[1557] However, even though the content of communication is protected, in such a case the employee would still have to face the legal consequences of personal use.[1558]

In relation to SNSs, this means that as a main rule, SNSs suppose personal use (in contrast to other Internet connections), employers should not access the content of these pages, as in most cases the purpose sought can be achieved by collecting data on the name/address of the sites visited (e.g. www.facebook.com), when they were accessed and for how long.[1559]

Section 2. New factors to be considered – highlighted by SNSs

Section 1 focused on the already existing regulation which is applicable to the monitoring of Internet and e-mail use. Although what was said is adequately applicable to SNSs as well, SNSs possess certain characteristics that distinguish them from the Internet and e-mail. First, these *(§1)* characteristics will be examined, then *(§2)* it will be addressed how exactly employers should monitor employees' SNS use in the light of the above-presented legal regulations, considering the specificities of SNSs. The question that Section 2 aims to answer is that in consideration of the challenges brought by SNSs, how the employers should monitor the use of SNSs during working hours.

§1. Specific issues raised by SNSs

Despite their similarities to the Internet and e-mail, SNSs also have several specific characteristics, which raise new questions in relation to the application of the already established regulation. When discussing specific issues raised by SNSs, a difference must

p. 28., p. 30.) However, since the establishment of the NAIH and the change of the legal environment in 2011–2012, one of the greatest changes in workplace data protection was the application of the legal ground of balancing interests – instead of the previously used consent. (Bankó – Szőke 2016. p. 53.)

[1554] Kártyás – Répáczki – Takács 2016. p. 67.

[1555] Recently, it has also appeared in the practice of the NAIH that according to the principle of fairness, the presence of the employee (or a person appointed by the employee) should be ensured, unless the matter is urgent or the employee does not work at the employer anymore. However, even in these cases, the (former) employee should be informed of the measures taken. Source: NAIH/2019/51/11., p. 19.

[1556] NAIH 2016. p. 27.

[1557] NAIH 2016. p. 27.

[1558] Hegedűs 2006. p. 49.

[1559] NAIH 2016. p. 31.

be made between two scenarios: SNS use constituting part of the employee's job description and not. For the purposes of the monograph it will be presumed that, as a main rule, SNS use is *not* part of the employee's job, and the case when it is will be treated separately.

When it comes to the monitoring of the personal use of SNSs, the main difference that can be observed compared to the monitoring of the personal use of the Internet and e-mail is the lack of the possible confusion of personal and professional use. In the case of Internet and e-mail monitoring, the main privacy/data protection issue lies in the fact that both the Internet and e-mail can be used for professional and for personal purposes as well, therefore, the confusion between professional and personal use is possible.[1560] In contrast, in the case of SNSs, this confusion is not present, as SNSs are usually not used as a tool for work, but uniquely for personal purposes.

It means that in the case of *surfing SNSs*, no special challenges arise, as the principle according to which every Internet connection is presumed to have a professional nature is clearly laid down *in French law*. Although these connections do not receive more intense protection – as they are presumed to be of professional nature, in contrast to their clearly personal nature –, through the effective application of the proportionality principle (e.g. consulting the name of the site, instead of the exact content) the employee's right can be protected. *In Hungary* as well, the application of the proportionality principle ensures protection, despite the lack of such presumption.

However, the *use of SNSs as messaging services* might seem to be more problematic at first sight, especially in French law. *In France*, protection is afforded to personal correspondence when the employee marks the communication as personal. However, on instant chat messaging services on SNSs, users do not have appropriate means to identify the message as personal (as the field "subject" is missing) – which is a key criterion in order to trigger the protection afforded by the secrecy of correspondence.[1561] In accordance with the existing legal framework, in the lack of identifying as such, the communication on SNSs is not presumed to be personal, despite the fact that SNSs are not even used for work.

However, contrary to this established presumption of professional nature, in 2017 the Court of Cassation – in the light of the presumption of professional nature – rejected the employer's arguments according to which accessing an employee's Facebook account by obtaining access to the professional cellphone of another employee was acceptable.[1562] Instead, it ruled that regardless of the device used (even if it is the employer's), SNSs are included in the right to respect for the employee's private life – excluding the application of the presumption in the case of SNSs. Although I welcome such a solution as it grants protection to communication conducted on SNSs, it is unfortunate that no further details were provided regarding the background of adopting this solution.[1563]

All this means that in reality, corresponding through SNSs is more similar to the case of using a personal e-mail account. Naturally, as even personal e-mails received/sent through professional accounts are protected by the secrecy of correspondence, e-mails received/

[1560] Féral-Schuhl 2018. p. 420.; Grynbaum – Le Goffic – Morlet-Haïdara 2014. p. 902.; NAIH 2016. p. 25.

[1561] In the case of e-mails, it is recommended to identify the message as personal either by storing them in a directory entitled "personal" or "private", or by indicating in the subject field "personal" or "private". (Source: CNIL: *Les outils informatiques au travail*. Fiches pratiques: Travail & données personnelles, 2018) However, that is usually not an option when it comes to SNSs. A solution can be to place identification at the beginning of the message in order to appear in the preview of the message.

[1562] Cass. soc., 20 décembre 2017, N° 16-19609

[1563] Mayoux 2018. p. 25. See more on the case in Title 3.

sent through a *personal account* should receive increased protection.[1564] Employers cannot monitor e-mails from employees' personal accounts, they are covered by the secrecy of correspondence – and they cannot be used during litigation either.[1565, 1566] This restriction applies even if the employee accesses the personal account from the work computer,[1567] however, if e-mails transferred from a personal e-mail account are stored on the hard drive of the work computer, they are not presumed to have a personal character.[1568]

In Hungary, as there is no presumption, the employer should examine on a case-by-case basis whether the correspondence was professional or personal. As SNSs *a priori* suppose personal use, establishing that they have a personal nature should not constitute a specific problem, as due to the lack of presumption they are not presumed to be professional.

Although most job descriptions do not include *the use of SNSs as part of the job*, in certain cases it is conceivable that employees might use those for work purposes. One obvious example is the operation of the company's official social media account. In such cases accessing SNSs can be of professional nature: giving rise to possibly blurring personal and professional use.

In French law, in such cases, the confusion of personal and professional use becomes possible so – just like in the case of "traditional" Internet and e-mail monitoring – the rules elaborated to these monitorings shall be applied, which allow the employer to consult the sites visited as they are presumed to be of professional nature. A challenge involved in the use of the messaging functions of SNSs services is that, due to the lack of the field "subject", it is not possible to indicate in the subject field that personal communication takes place. In this regard, the situation is similar to that of SMS messages, which are presumed to have a professional character, unless identified as personal:[1569] however, technically it is not feasible to indicate the personal character of these messages, the employer has to access the content of the message to be able to know its personal nature.[1570] Although this solution was proposed for SMSs, chat messages on SNSs have similar characteristics, making it possible to apply this method to them: the personal character can be signalled by placing identification at the beginning of the message (e.g. "!!!personal message!!!") in order to appear in the preview of the message.[1571]

In Hungarian law, it is also a problem that messages sent within SNSs cannot be easily identified as personal. Therefore, distinguishing professional and personal use can be challenging. However, those said in relation to French law can successfully be applied to Hungarian law as well: indicating in the preview of the message that it is personal can constitute an effective way of separating professional messages from private ones. Also, the name of the corresponding party can be revealing[1572] and can contribute to excluding

---

[1564] Lhernould 2016. p. 11.

[1565] Cour de cassation, 26 janvier 2016, n° 14-15.360

[1566] Unless exceptional circumstances are present, and safeguards are guaranteed – e.g. involvement of a bailiff, research limited to the messages in relation to the litigation. (Cour de cassation, 1ère chambre civile, 20 septembre 2017, n° 16-13082) The employer has to demonstrate to the judge the existence of a legitimate aim, and that a violation was already committed. Griguer 2010. p. 63.

[1567] Cass. soc., 7 avril 2016, n° 14-27949

[1568] Cass. soc., 19 juin 2013, N° 12-12138

[1569] Cour de cassation, chambre commerciale, financière et économique, 10 février 2015, n° 13-14.779

[1570] Lhernould 2015. p. 10.

[1571] Adam 2015. p. 193.

[1572] For example, Facebook allows giving nicknames to parties – which can constitute a way of showing the personal character of a message.

certain messages. Besides, by ensuring the presence of the employee it can be achieved that the employer successfully distinguishes between personal and professional messages and does not access personal communication.

It was already established that the employer is entitled to monitor the use of work equipment. However, it was already presented that the proliferation of mobile devices in everyday life raises specific questions when *employees use their own devices* to access SNSs during working hours. Although regulating their use seemed to be possible, their monitoring can pose specific questions.[1573] In cases when the device is the employee's property, the employer is limited in monitoring their use; he/she cannot have access to the content/pages visited on these devices.[1574] However, even if the employee succeeds in escaping from the prying eyes of the employer through accessing SNSs from his/her own device, an excessive use of these sites would come at the expense of the performance of work tasks,[1575] allowing the employer to eventually detect the abuse and take the necessary steps.

Without the possibility to monitor personal devices, the activity of employees checking their Facebook can easily remain invisible. However, in certain exceptional cases the employer can still find out about such a use. One exception can be when the employee posts or likes something during working hours – despite the ban of social media use – and the time of the post or like reveals to the employer that the employee has infringed the limitation. Another exception can be manifested in the consequences of (abusive) personal use: if personal use has negative effects on working (e.g. committing mistakes, missing deadlines, etc.), the employer can sanction such behaviour in accordance with the relevant labour law regulations.[1576]

§2. Monitoring employees' SNS use

It was already established on several occasions that the employer is entitled to monitor employees. Such a monitoring can include the monitoring of the use of the work equipment as well as the employee's respect of working hours. In Section 1 it was found that the employer is free to decide whether the personal use of work equipment is authorized or not and is entitled to monitor compliance with the established regulation. The following paragraphs contain recommendations regarding how employers should monitor whether employees respect the rules set up and what they should take into consideration when establishing monitoring. First, *(A)* it will be discussed what rules should be established, then *(B)* how they should be communicated to employees.

[1573] Kun 2013. p. 13.

[1574] Proskauer Rose LLP 2014. p. 3.; Kun 2013. p. 13., Ray 2018. p. 324.

[1575] Ray 2018. p. 324.

[1576] For example, an employee in Wales was dismissed in 2013 for accessing social network sites during working hours from his own device. Unfortunately, it was not documented how the employer became aware of such use. https://www.mirror.co.uk/news/uk-news/dvla-worker-fired-using-facebook-1903697 (Accessed: 25 July 2019)

(A) Rules of employee monitoring

As regards enforcing that employees comply with the rules of personal SNS use set by the employer, it is recommended that emphasis is put on *prevention*. If employees are aware of the rules (either it is a complete ban or a more permissive regulation), the emergence of several issues can be prevented. This can be achieved by informing them: raising their awareness through regularly reminding them of the rules or organizing trainings can be effective ways to achieve this goal.

Another way of prevention is to make it impossible for employees to engage in the prohibited behaviour. The most obvious means is to ban the access to SNSs. However, when opting for such a solution, employers should take the weak points into consideration: that it is not possible to prohibit access to all social media and SNS platforms, only to the most popular ones (e.g. Facebook, Instagram, YouTube, Twitter). Also, such a ban can only be put on the employer's equipment. Employees would still have the possibility to access these sites from their own devices.

If the employee tries to access a prohibited site despite the restrictions imposed on such a use, he/she should be reminded of the rules. For example, alerts and pop-up windows should be employed, which can remind the employee that he/she wants to access a prohibited page, or in the case of a more permissive regulation that he/she is approaching/exceeded the authorized time limit.[1577] Such a measure can also contribute to enhancing compliance with the regulation and also to preventing misuse through raising employee awareness.

As a main rule, the employer should not gain access to the exact content visited or communication held in either countries with regard to the fact that SNSs are used for personal purposes, both in the case of surfing on them or using them as a means of communication. In accordance with the data protection principles, instead of accessing the content, the employer should settle for having access to the different indicators of the use (e.g. time spent on SNSs, or data traffic), as through that information he/she is perfectly capable of ascertaining whether personal use has taken place or not, or whether it has exceeded the allowed amount.[1578]

In cases when the employer is in need of determining whether the use was personal or professional, it can be recommended to encourage employees who use SNSs as part of their jobs to indicate at the beginning of the message if it is personal in order to avoid confusion (e.g. "PERSONAL MESSAGE").[1579] The presence of the employee can also contribute to the protection of private life and data protection rights.[1580]

(B) Social media policies

It is not uncommon for employers to regulate the question of SNS use at the workplace in internal social media policies and it is a recommended practice by different organizations.[1581]

[1577] WP29: *Working document on the surveillance of electronic communications in the workplace*, 2002. p. 5.
[1578] Buttarelli 2009
[1579] Information Commissioner's Office 2011. p. 70.
[1580] French law even requires it: Cour de cassation, civile, chambre sociale, 17 juin 2009, 08-40.274
[1581] See, for example, the survey conducted by Proskauer on social media in the workplace or the ICO's code of practice. Source: Proskauer Rose LLP 2014. p. 23.; Information Commissioner's Office 2011. p. 66.

Usually, these policies aim to regulate behaviour both within and outside the workplace, and also the possible disciplinary sanctions that can be given in case of breach of the policy.[1582] According to *Teresa Coelho Moreira*, the adoption of "rules of good conduct" or a "charter of informatics" is the most appropriate way to enhance the principle of transparency and to comply with legal obligations.[1583] In a recommendation in 2013, the NAIH also held that the employer should adopt detailed internal policies relating to monitoring, guaranteeing the enforcement of the requirements set in the HDPA and the HLC.[1584] The CNIL also pleaded in favour of adopting such documents.[1585]

In France two types of these documents exist: these guidelines can either serve as a guidance regarding what conduct employees should adopt when it comes to the personal use of SNSs during working hours, or they can be part of the employer's internal regulation.[1586] In the first case, these documents have informative roles, while in the second case they are considered supplements to the internal regulation and are binding both for the employee and for the employer.[1587] However, it is important to note that it is not the existence of such a charter that qualifies the employees' actions as violation: even when there exists no such document, the breach of duty of the employee is established (e.g. obligation of work and being at the disposal of the employer).[1588]

According to the HLC, the employer can draft internal policies,[1589] allowing the employer to unilaterally define obligations to be respected by employees.[1590] Such a policy can relate to the use of SNSs.[1591] However, the wide adoption of social media policies is not (yet?) a common phenomenon in Hungary.[1592] However, certain exceptions can be mentioned, such as the social media policy of the Hungarian National Health Service[1593] or the Hungarian National Savings Bank's policy.[1594]

The employer has extensive powers in setting the limits on personal use. A research project entitled "*Data protection challenges arising during the use of social network sites in the context of employment*"[1595] conducted by *József Hajdú*, *Adrienn Lukács*, *Viktória Lechner* and *Attila Turi* – amongst other matters – examined the possibilities lying in internal social media guidelines in relation to social media. Although the research primarily

---

[1582] Thornthwaite 2016. p. 334.

[1583] Moreira 2016. p. 23.

[1584] NAIH-4001-6/2012/V. p. 3.; NAIH/2019/51/11. p. 16.

[1585] Bouchet 2004. p. 11.

[1586] Niel 2007. pp. 37–38.

[1587] Kocher 2013. p. 133.

[1588] Nivelles 2014. p. 11.

[1589] Section 17 of the HLC

[1590] Section 15 of the HLC
Although it should be noted that according to Subsection (1) of Section 264 of the HLC "*[e]mployers shall consult the works council prior to passing a decision in respect of any plans for actions and adopting regulations affecting a large number of employees[.]*" raising the question of the possible role of social partners in the process. In France the social and economic council of the workplace must be consulted for its opinion if the policy is adopted as part of the employer's internal regulation.

[1591] Rácz 2015. p. 295.

[1592] Kártyás – Répászki – Takács 2016. p. 67.

[1593] http://arsboni.hu/kozossegi-media-es-munkajog-kereszttuzeben/ (Accessed: 27 February 2018)

[1594] https://ado.hu/munkaugyek/facebook-szabalyzat-beleszolhat-a-munkaltato/ (Accessed: 15 November 2018)

[1595] "*A közösségi oldalak használata során felmerülő adatvédelmi jogi problémák a munkajog kontextusában.*" The research was carried out among the programs of the Ministry of Justice aimed at raising the standard of legal education. The next paragraphs are highly based on the results of the research.

focused on off-duty conducts on SNSs,[1596] certain factors have relevancy when it comes to SNS use during working hours as well. It is crucial to emphasize that there exists no one-size-fits-all solution: the suggestions to be presented serve as a point of reference, which need to be tailored to the particularities of the specific work environment.

First, *fundamental provisions* should be laid down. In order to avoid misunderstandings, the *definition* of social media should be clarified. As the exhaustive enumeration of every SNS is not possible, it is recommended that the employer indicates a general definition of social media/SNSs and then by way of example specifies the most frequently used sites, known to most employees. The *personal scope* of the regulation is also crucial: the employer should clearly indicate to whom the regulation is applicable (e.g. a group of employees, all employees).

Then, *general rules of conduct* should be laid down. Employees should be reminded of their obligations – notably the obligation to work – and that even though a reasonable personal use is tolerated, equipment should primarily be used for professional purposes, and working hours should be spent working and not surfing on SNSs.

Rules relating to the personal use of SNSs should clearly detail what kind of activity is permissible – the employer has extensive powers to regulate this matter. He/she can impose limitations regarding the sites visited, the time spent on them and the period when they can be used. He/she can define what SNSs can or cannot be accessed during working hours and can even block access to sites. If personal use is permitted, time limitations can still be imposed on their use – e.g. 20 minutes of use is permitted daily. It might also be useful if the employer defines the period during which these sites can be accessed (e.g. as a sort of a "warming up" in the morning after arriving at the workplace). It is important to emphasize that even if personal use is tolerated to a certain extent, it should not in any case come at the expense of executing a task (e.g. when an employee should deal with customers).

Internal regulations can play an important role in *French law* when it comes to the presumption of professional nature of correspondence. The internal regulation can contain refinements as regards how exactly messages should be identified as personal: in such cases if the employee does not identify them as personal as required by the regulation, the employer can open them.[1597] In the exceptional cases when employees might also use SNSs for professional purposes, therefore personal and professional use can mingle, the internal regulation can contain provisions regarding how employees should indicate that the communication on SNSs is private. Although compared to e-mails, in the case of SNSs it is considerably more difficult to identify the message as personal, it was demonstrated that certain measures might still be conceivable. The internal regulation can also restrict the employer's right to access the content of these messages[1598] (e.g. only in the presence of the employee).[1599]

Such policies should also contain information on how exactly *monitoring* will be conducted in order to verify whether the employee complies with the rules made regarding personal use. As presented before, emphasis should be put on prevention, and the monitoring of traffic data should be preferred to the monitoring of the actual content/communication,

[1596] It will be presented later in Title 3.
[1597] Cass. soc., 4 juillet 2012, N° 11-12502
[1598] Cass. soc., 26 juin 2012, n° 11-15310
[1599] Kocher 2013. pp. 129–140. p. 133.

while accessing the content of personal communication is not possible. If the policy is adopted as part of the internal regulation, breaching its provisions can result in applying *disciplinary sanctions* against the employee.[1600] Therefore, these policies should remind employees that in the case of violating them and breaching obligations, sanctions can be applied.

[1600] Niel 2007. p. 40.

Title 3: Employees' engaging in social network sites with special regard to off-duty conduct

During working hours, it follows from the employee's obligation to work that he/she can be limited in the use of SNSs. However, beyond working hours there is no such obligation to work, and as a result, it must be examined what other obligations the employee has that can justify the limitations in the use of SNSs during that period. Just as personal life flows into professional life, professional life flows into the personal life of the employee. As employees do not leave their rights at the doorsteps of the workplace every morning, they do not cease to be employees when they leave the workplace: they are still subject to certain obligations originating from the employment relationship.[1601] On the one hand, employees are subject notably to the duty of loyalty, which can restrict the employee's freedom of action and interfere with his/her *personal life* by restricting employees' off-duty conduct to a certain extent. On the other hand, questions regarding the *right to data protection* also arise, in relation to employers who decide to monitor and/or to process employees' personal data obtained from SNSs.

Criticising or complaining about the employer, making disparaging comments about the workplace or colleagues, or making "pranks" at the workplace have always existed. However, while earlier these statements did rarely leave the employees' close environment (e.g. gossiping around the coffee machine or criticizing the employer in a pub on Friday night or at a friends'/family gathering during the weekend), the advent of social media brought certain changes. Nowadays – as various examples will illustrate throughout Title 3 – it is not uncommon that employees let off steam on SNSs, which can even result in the termination of their employment. Compared to the "traditional" way of expressing negative opinion, SNSs pose new challenges. Notably, social media and SNSs brought a change of paradigm regarding especially the publicity of the statements or content. Depending on the chosen privacy settings, such communication might take place in front of a considerably bigger, often public audience, giving increased importance to the protection of employer's rights.

As a response, employers restrict more and more often what an employee can post or cannot post in social media (in internal social media policies, for example) or sanction employees for their conduct on SNSs in order to protect their business. It is increasingly common that employees' behaviour on SNSs exceeding the limits of freedom of expression results in the termination of employment.[1602] This growing number of news[1603] and cases[1604] relating to "Facebook firings" manifests that employees are often not aware that their

---

[1601] Apart from the freedom of thought, all freedoms of the employee can bear some limitations in relation to the employment relationship. Waquet 2002. p. 4. (Page number referring to the online version of the article downloaded from: https://lamyline-lamy-fr)

[1602] Kun 2018. p. 133.

[1603] A simple Google search (e.g. "fired for Facebook", "Facebook-os felmondás", "licenciement Facebook") reveals a myriad of cases as regards employees whose employment relationship was terminated due to their use of Facebook. Or see, for example, the blog entitled "The Facebook Fired" where a compilation of Facebook firings is present. https://thefacebookfired.wordpress.com/(Accessed: 7 August 2019)

[1604] See, for example: CA Reims, chambre sociale, 9 juin 2010, n° 09/03205; CA Besançon, chambre sociale, 15 novembre 2011, n° 10/02642; CA Reims, chambre sociale, 15 Novembre 2017, n° 16/02786; CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343; Cass. soc., 20 déc. 2017, n°16-19609; Cass. soc., 12 sept. 2018, n°16-11.690; Taylor v Somerfield Stores Ltd. Case no: S/107487/07 Held at Aberdeen on 24 July 2007; Konop v. Hawaian Airlines (United States Court of Appeals for the Ninth Circuit, 236 F.3d

activity can result in dismissal and do not realize that even though the activity takes place within their personal lives, they could still suffer legal consequences.

The starting point of Title 3 is that the examined conducts usually (although not always) take place outside the workplace, beyond working hours, by using the employees' own equipment, therefore in the course of employees' personal life, where employees are free to act as they wish. However, ensuing from the labour law regulation, this freedom is not limitless: employees are subject to certain obligations, which results in professional life flowing into personal life through imposing certain limitations on the employees' freedom of action. In *French labour law*, the case law relating to the termination of employment established exceptions to the main rule, namely that the dismissal cannot be based on the employee's personal life, unless certain conditions are met.[1605] Through these exceptions, the boundaries of personal and professional life are outlined. In contrast, in *Hungarian labour law*, the HLC contains provisions[1606] which explicitly address employees' off-duty conduct, imposing certain limitation on them. The overarching question is how the existing regulation/case law should be applied to SNSs.

Title 3 intends to examine the boundaries between personal and public activities in relation to employees' off-duty conduct on SNSs. In the light of the obligations incumbent on employees, first it should be determined whether using these platforms falls under private or personal life, or whether they rather constitute a public forum. Then it should be determined where exactly the boundaries of employees' freedom to act lie: this raises the question to what extent employers can restrict and sanction employees' conduct that took place outside their professional life – not in the workplace, during non-working hours, and with the help of the employee's device.

Chapter 1 will address the boundaries of employees' personal life and off-duty conduct by examining in what regard employees can be restricted while using SNSs and expressing themselves on these platforms. Employees' activity on SNSs can jeopardize the employer's rights in several ways – among which the form of the activity and the subject of the activity were chosen in the monograph as main assessment criteria. The *form* of the activity can take different shapes. Either it can be an expression of opinion (typically manifested in posts or comments), or it can take other forms (e.g. video, photo) not containing explicit statements. Regarding the *subject* of the activity, it can either be connected directly to the workplace (e.g. criticizing the employer), or it can relate to a matter that has no direct connection to the workplace (e.g. publishing anti-Semitic comments under an article). *Chapter 2* will deal with enforcing these restrictions and will examine the possibilities that employers have for the enforcement of their rights, and the conditions (notably data protection) that they must respect when controlling employees' off-duty conduct on SNSs.

1035.); District of New Jersey: *Pietrylo v. Hillstone Restaurant Group*, No. 06-05754, 2009; LAG Hamm Urteil (vom 10. Oktober 2012 Az. 3 Sa 644/12), etc.

[1605] Different for disciplinary and for non-disciplinary dismissal, as it will be presented in detail.

[1606] See Section 8 and notably Subsection (2) of Section 8 of the HLC.

Theoretically, the employee's professional life and personal life are meant to be separated: into professional life, connected to the workplace; and into personal life, independent of the workplace, where the employee is free to act as he/she wishes. However, it was already demonstrated that due to the technological development, the boundaries of work and personal life are more and more blurred – which is increasingly true in the case of social media.[1607] This is the reason why it is important to determine the boundaries between these two spheres in relation to SNSs and off-duty conduct, namely: to what extent can limitations be imposed on the employee's personal life? National regulations already addressed the question: in French law through the rules and jurisprudence relating to dismissal, while in Hungarian labour law, Section 8 of the HLC contains specific provisions on the employee's conduct outside working hours. Prior to addressing the specific questions raised by SNSs, the general rules in relation to dismissals will be presented.

In *French labour law* the protection of employees' personal life appears through the rules relating to dismissal, as personal life must be respected during the decision-making. Differentiation is made between dismissal on personal and on economic grounds[1608] – among which the former is relevant regarding the subject of the monograph. In the case of dismissal based on personal grounds, the reason for the dismissal is based on the person of the employee: the reason can either be disciplinary (supposing the sanctioning of the employee for his/her misconduct – "faute", e.g. breaching an obligation arising from the employment relationship) or non-disciplinary (e.g., professional incompetence, disagreement between the employee and the employer, etc.).[1609]

Although in the case of dismissal on personal grounds the reason for dismissal lies in the person of the employee, as a main rule, when dismissing an employee, the employer must respect the employee's personal (and private) life. According to the main principle set by French courts, the personal life of the employee is protected; dismissal cannot be based on the personal life.[1610] However, it does not mean that the employee is completely free to do anything outside the workplace without eventual consequences, as there are exceptions when the employer may pronounce a disciplinary and a non-disciplinary dismissal – based on the personal life of the employee.

While in French law the starting point is that the dismissal should not be based on the personal life of the employee, and then the jurisprudence establishes certain exceptions, in *Hungarian labour law*, limitations are *a priori* imposed on employees' off-duty conduct and courts examine whether employees acted in respect with these provisions. Sections 6–8 of the HLC contain provisions relating to common rules of conduct, determining how the parties should behave. Among these provisions Subsection (2) of Section 8 imposes limitation on employees' conduct during and *outside* working hours, while Subsection (3) regulates specifically the question of employees' freedom of expression. These provisions aim to determine the legitimate extent to which employees can be bound to respect certain limitations imposed on their personal lives. In addition, Subsection (1) contains provisions

[1607] Ellickson – Atkinson 2013. p. 261.
[1608] Title 3 of Book II of Part I of the FLC
[1609] Grandguillot 2016. p. 67.
[1610] Cass. soc., 20 nov. 1991, n° 89-44.605; Cass. soc., 14 mai 1997, N° 94-45473

on the protection of the employer's legitimate economic interests, while Subsection (4) on the protection of the employer's business secrets.

In *French labour law*, the termination of the employment relationship based on the personal life of the employee can be either disciplinary or non-disciplinary. When it comes to *disciplinary dismissals*, in which case the dismissal is grounded on the misconduct of the employee, an element pertaining to the personal life can only justify a dismissal if it constitutes a *breach of duty or obligations* resulting from the employment contract.[1611, 1612] Through this statement, the Court of Cassation adopted a position similar to the one of the State Council's, which also expressed that an act of the employee realized outside the execution of the employment contract cannot be a reason for dismissal for misconduct, unless it constitutes an infringement of an obligation arising from the employment contract.[1613] Although it is not perfectly clear the breach of which obligations can ground a disciplinary dismissal,[1614] in relation to social media, the employee's obligation of loyalty will gain special importance.

In the case of a *non-disciplinary dismissal*, the reason for dismissal is not the misconduct arising from the breach of obligations, but is connected to the person of the employee. In this case, the element of personal life justifies a dismissal if it causes a "characterised serious disorder" ("trouble objectif caractérisé") in the organization and the functioning of the workplace (taking into consideration the function and purpose of the workplace).[1615] In the latter case it is not the element pertaining to the employee's personal life which in itself creates the disorder and results in the dismissal, but its repercussions on the functioning of the workplace – taking into consideration the employee's position.[1616, 1617] It is important that as there is no breach of an obligation arising from the employment, the dismissal for disorder can only constitute a non-disciplinary dismissal.[1618, 1619]

[1611] Cass. soc., 23 juin 2009, N° 07-45256.; Cass. soc., 3 mai 2011, N° 09-67464

[1612] Or it must be connected to the professional life of the employee (e.g. committed in the workplace, or by using the employer's equipment). Source: Beyneix – Rovinski 2016. p. 37.; Casaux-Labrunée 2012. p. 339. and Icard 2014. p. 642. The Court of Cassation referred to the criteria of connecting to the corporate life of the undertaking to confirm dismissal notably in its judgments of Cass. soc., 2 décembre 2003, N° 01-43227 (withdrawal of a driver's driving licence because of driving in a state of drunkenness – even beyond working hours), or Cass. soc., 17 novembre 2011, N° 10-17950 (an employee benefiting from his functions as a guard in a castle stored and illegally manufactured alcohol in the castle).

[1613] Conseil d'État: N° 316856, 4ème et 5ème sous-sections réunies, 15 décembre 2010

[1614] Casaux-Labrunée 2012. p. 340.; Loiseau 2011. p. 1569.

[1615] Principle posed by the *Painsecq case* in 1991. In this case the Court of Cassation ruled that the dismissal of an assistant sacristan based on his homosexuality could only constitute a reason for dismissal if it caused a characterised serious disorder in the functioning of the undertaking. (Cass. soc., 17 avril 1991, N° 90-42636) This principle was reinforced by the decisions of Cass. soc., 22 janvier 1992, N° 90-42517 (a Renault employee bought a Peugeot car: the Court of Cassation ruled that in his private life the employee is free to buy the product of his choice and the simple acquisition of the car did not cause a characterised serious disorder); Cass. soc., 16 décembre 1998, N° 96-43540

[1616] Waquet 2006. p. 307.

[1617] For example, the Court of Cassation held that an employee, who worked as a security agent and outside of working hours committed shoplifting from one of the clients of the enterprise, discredited the employer and caused a disorder. (Cass. soc., 20 nov. 1991, n° 89-44.605) The same conclusion was reached in a case when a sales agent stole an article from a hypermarket that belonged to his sector and the client threatened to never work again with the employer. (Cass. soc., 3 déc. 2002, n° 00-44.321)

[1618] Cass. soc., 23 juin 2009, N° 07-45256.; Cass. soc., 9 mars 2011, N° 09-42150

[1619] See more on private/personal life and dismissals in: Loiseau 2011. pp. 1568–1569.; Casaux-Labrunée 2012. pp. 339–342.

In *Hungarian law* if the employee breached his/her obligations arising from the employment contract and did not act in accordance with the requirements set by the HLC, the employer is entitled to terminate the employment relationship. In Hungarian law as well, it is possible to dismiss the employee based on his/her breach of obligations, but also due to other personal features not constituting a breach – however, the appellation of these dismissals is different than in French labour law. In Hungarian labour law, a difference is made between termination by notice and dismissal without notice.[1620]

According to Subsection (2) of Section 66 of the HLC *on termination by notice*, "[a]n employee may be dismissed only for reasons *in connection with his/her behaviour in relation to the employment relationship*, with his/her ability or in connection with the employer's operations."[1621] Among these three cases, behaviour in relation to the employment relationship is important for the research subject. The employee's behaviour in connection with the employment relationship primarily consists of cases when the employee culpably violates obligations arising from the employment relationship.[1622] Employees expressing their opinion on SNSs or public behaviour can be covered by this Section, and therefore can serve as reason for the termination of the employment.[1623]

Termination without notice is possible when the employee either "*willfully or by gross negligence commits a grave violation of any substantive obligations arising from the employment relationship*;"[1624] or "*otherwise engages in conduct that would render the employment relationship impossible.*"[1625] The first case supposes a serious breach of duty[1626] (basically being the equivalent to the French disciplinary dismissal), while in the second case maintaining the employment relationship becomes objectively impossible, with the lack of serious breach of duties[1627] (similar to the French non-disciplinary dismissal, where the breach of duty is missing). Usually behaviour which is capable of shaking the trust between the parties can serve as a basis,[1628] typically including cases connected to the employee's behaviour outside work making it impossible to maintain the employer relationship.[1629] For example, a Facebook post might result in a loss of trust,[1630] serving as a ground for termination without notice.[1631]

As such, both in France and in Hungary personal life is protected during the termination of employment. However, it does not mean that personal life can never constitute a reason

---

[1620] Subsection (1) of Section 64 of the HLC

[1621] Emphasis added by the author.

[1622] Gyulavári 2013. p. 202.
E.g. refusing to comply with the employer's legitimate orders without valid grounds (BH1996. 286.), consuming alcohol during working hours or appearing at work being under the effects of alcohol consumption (BH1986. 384.), the development of conflict due to not respecting working hours and due to the behaviour of the employee (Csongrád Megyei Bíróság 2. Mf. 20. 566/1997.).

[1623] Zaccaria 2016. p. 16.

[1624] Item a) of Subsection (1) of Section 78 of the HLC

[1625] Item b) of Subsection (1) of Section 78 of the HLC

[1626] E.g. revealing business secrets (Mfv. I. 10.264/2002/2.), consuming alcohol during working hours at a dangerous workplace (Szegedi Munkaügyi Bíróság 4. M. 1159/1994.), leaving the workplace on several occasions without authorization (BH 2008. 132.)

[1627] Gyulavári 2012. p. 216.

[1628] Hajdú – Kun 2014. p. 167. E.g. he/she engages in conduct unworthy of his/her job by leading a lifestyle of revelry and alcoholism, substantiated suspicion of committing a serious criminal offence.

[1629] Cséffán 2016. p. 309.; Gyulavári 2012. p. 216.

[1630] Kozma 2013. p. 10.

[1631] Mfv.I.10.469/2013/4 Cited in: Cséffán 2016. p. 311.

for terminating the employment relationship: in the light of the obligations of the employee, both countries provide exceptions to this general rule, as well as the case when there is no breach of obligation, but the behaviour still has serious repercussions on the employment. In France, the limits of these exceptions were elaborated by case law, while in Hungary, Section 8 of the HLC itself already limits employees' behaviour in the course of their personal lives.

After reviewing the general legal framework regulating dismissal, the specific features of SNSs must be addressed. Employees' off-duty conducts on SNSs can take several forms and can constitute a ground for disciplinary and non-disciplinary dismissal (France), as well as for termination by notice and without notice (Hungary). In order to exhaustively present these conducts, the differentiation proposed by certain scholars[1632] will be followed, according to which the employee's conduct can relate, on the one hand, *directly* to the workplace (e.g. the content of activity relates to the workplace) or on the other hand, it can *indirectly* relate to the workplace (where the content of the activity is independent of the employment, the only connection to the workplace is the user's person, who is the employee). First, in *Section 1* employees' behaviour directly connected to the employment will be examined, followed by employees' behaviour not directly connected to the employment in *Section 2*.

Section 1. Online activity with direct connection to the employment

Employees' SNS activity can relate to the employment in several ways: from complaining of the employer on a colleague's Facebook wall,[1633] through liking the competition's Facebook page,[1634] till sharing information relating to the clients of the employer[1635]… and the list goes on. Although the subject will be discussed from the angle of French and Hungarian law, as the phenomenon is universal, reference and examples will be often taken from other jurisdictions as well, in order to illustrate certain matters.

During the research, the question of determining the boundaries of employees' personal lives was most often raised in relation to their *(A)* freedom of expression on SNSs – where the question to be answered is whether and to what extent employees can express themselves outside of the workplace, *a priori* in the course of their personal lives. Nevertheless, freedom of expression is not the only conduct that can directly relate to the employment: employees have *(B)* other ways that take place beyond the working hours but still have a direct connection to the employment. Such conduct can be, for example, the revealing of business secrets on SNSs or carrying out whistleblowing on SNSs. However, as a preliminary point, it should be observed that these "other" ways do not substantially challenge the boundaries of work and personal life and seem to raise specific issues in relation to employees' personal life to a lesser extent.[1636]

[1632] Pók 2012a. p. 160.; Zaccaria 2016. p. 16.
[1633] CA Reims, chambre sociale, 9 juin 2010, n° 09/03205
[1634] USA: District court for the Eastern District of Virginia: Bland v. Roberts, 4-11cv45 (E.D. Va.; Apr. 24, 2012)
[1635] https://index.hu/tech/2012/01/04/banktitkot_sertett_egy_magyar_mikroblogger/(Accessed: 7 September 2018)
[1636] Pók 2012. p. 13.

§1. Employees expressing themselves on social network sites

As the growing number of news in media and litigations in courts demonstrate it, on SNSs employees often criticize employers, colleagues, clients in very harsh style, using offensive vocabulary – resulting in their dismissal.[1637] An employee criticizing[1638] the employer is not a new phenomenon,[1639] but social media brought considerable changes in this field, raising the question whether the previously established rules are adequately applicable to this new situation, or whether they should be modified. These changes concern particularly their publicity, permanence, style and the possible identification of the employer.

Regarding *publicity*, while earlier these statements did rarely leave the employees' close environment (e.g. gossiping around the coffee machine or criticizing the employer at a friends'/family gathering during the weekend), with the advent of social media they take place in front of a considerably bigger, often public audience – making it also easier to be discovered by the employer. Also, while criticising the employer orally was less discoverable and clearly less reproducible, on SNSs communication/content stays *permanently*, as it is not feasible to completely remove a content once it was published.[1640] Another change is the *style* of communication: on the Internet users often use vocabulary that is different compared to what they would use face-to-face.[1641] SNSs also facilitate *identifying* the employer of the author of the post,[1642] creating a link between the employee's post and the employment. These observations suggest that the employee can cause increased damage to the employer, in contrast to statements made prior to the proliferation of SNSs.

Regarding *France*, first, the obligation of good faith ("obligation de loyauté") must be addressed, which imposes limitations on the employee's freedom of action. The obligation of good faith can also enter into collision with the employee's freedom of expression, making it necessary to address the specific limitations on freedom of expression. The employee's *obligation of good faith* originates from the Civil Code's (former) Article 1134,[1643] stating that contracts shall be executed in good faith – a principle that applies to the parties of the employment relationship as well.[1644] According to the obligation of good faith, the employee must refrain from disloyal conducts and notably has the duty of

---

[1637] See, for example: https://www.businessinsider.com/17-people-who-were-fired-for-using-facebook-2014-7 (Accessed: 30 July 2019); https://www.awesomeinventions.com/fired-posting-on-facebook/(Accessed: 30 July 2019)

[1638] However, in some cases the employee can go even further than mere criticism and can deliberately harm the employer's reputation. See, for example, the case of an employee who directly encouraged people not to support the employer, as it "ripped off a bunch [of people]." Ellickson – Atkinson 2013. p. 264.

[1639] For example, employees expressing their opinion in relation to the employer through the publication of a book (BH2000. 267.), or through wearing a placard on the work uniform (BAG 2 AZR 620/80 1982. cited in: Jónás 2010. p. 38.) or through publishing an article containing the employee's negative opinion (1050/2004. számú munkaügyi elvi határozat).

[1640] As *Jean-Emmanuel Ray* referred to the classic proverb: "*Words fly away, writings remain*." underlying that once something was published on an SNS, it can be retrieved by a third party and used even years later. Ray 2011. p. 133.

[1641] It is enough to take a look at the comment section under an article, where often complete strangers are at each other's throats and insult people using extremely offensive vocabulary – what most of them probably would not do during a face-to-face encounter.

[1642] E.g. especially if the employee identified his/her employer in the "bio" part, but a simple Google search on the user's name might reveal the employer's identity in a few seconds, or even other users can reveal it.

[1643] Today, Article 1104 of the Civil Code.

[1644] Article L1222-1 of the FLC: "*Employment contracts must be performed in good faith*."

loyalty, duty of non-concurrence and duty of confidentiality – and more importantly for the subject of the monograph: exercising the freedom of expression in an abusive manner can constitute the violation of the obligation of good faith.[1645] The Court of Cassation also associated an obligation of probity with the obligation of good faith,[1646] and an obligation of morality considering the functions of the employee.[1647] This obligation of probity can be more specific in the case of ideologically or faith-oriented enterprises[1648] ("entreprise de tendance").[1649]

Such an obligation of good faith can collide with employees' freedom of expression: employees are entitled to the *freedom of expression* within and outside the workplace as well.[1650] However, exercising this freedom cannot be limitless, the main obligation arising from the employment contract – notably the duty of loyalty – must be respected even beyond working hours.[1651] The Court of Cassation formulated the principle of employees' freedom of expression in 1999, when it stated that "*except in the case of abuse, the employee enjoys the freedom of expression within the workplace and outside of it; which can only be restricted by a restriction justified by the nature of the task to be performed and proportionate to the aim sought.*"[1652] This means that the employee is entitled to express his/her opinion as he/she wishes, including subjects relating to the employment,[1653] even to criticise the employer, as long as these expressions are not insulting, defamatory or excessive.[1654] If the employee oversteps the limits of the freedom of expression, he/she can be sanctioned for it – and in the most serious cases can be dismissed.[1655]

As regards SNSs and assessing whether employees can be sanctioned for expressing themselves on social media, it must be examined whether the expression constituted an abuse. However, prior to examining the abuse, *first*, (a) it must be examined whether the content was publicly accessible (the private or public nature of SNSs): did the employee's act belong within his/her private life? *Then*, (b) if the remarks are considered to be public and they were obtained lawfully, it can be examined whether they are of an abusive nature or not.[1656]

Just like the FLC, the *HLC* also contains a declaration on good faith (and mutual cooperation) through stating that "*[i]n exercising rights and discharging obligations, the parties involved shall act in the manner consistent with the principle of good faith and fair dealing, they shall be required to cooperate with one another, and they shall not engage in any conduct to breach the rights or legitimate interests of the other party*."[1657] However, in contrast to the FLC, in Section 8, it is explicitly defined what the duties of the employee are when it comes to respecting the employer's rights and legitimate business interests.

[1645] Richard de la Tour 1999.
[1646] Cass. soc., 25 févr. 2003, n° 00-42.031
[1647] Corrignan-Carsin 2011. p. 40.
[1648] An ideologically oriented enterprise is an enterprise which has a particular orientation, which can be syndical, political or religious.
[1649] Corrignan-Carsin 2011. p. 40.
[1650] Cass. soc., 14 décembre 1999, N° 97-41995
[1651] Beyneix – Rovinski 2016. p. 39.
[1652] Cass. soc., 14 décembre 1999, N° 97-41995
[1653] Waquet – Struillou – Pécaut-Rivolier 2014. p. 299.
[1654] Le Cohu 2018. p. 58.
[1655] Cass. soc., 25 janvier 2000, N° 97-45044
[1656] Grégoire 2018. p. 437.
[1657] Subsection (2) of Section 6 of the HLC

Among these provisions Subsection (2)[1658] of Section 8 imposes limitation on employees' conduct during and *outside* working hours, while Subsection (3)[1659] regulates specifically the question of employees' freedom of expression. These provisions aim to determine the legitimate extent to which employees can be bound to respect certain limitations imposed on their personal lives. In addition, Subsection (1)[1660] contains provisions on the protection of the employer's legitimate economic interests, while Subsection (4)[1661] on the protection of the employer's business secrets.

The first problem that is encountered is that it is not evident how Subsections (1)–(3) of Section 8 relate to each other.[1662] Although Subsection (1) relates to the jeopardizing of the employer's legitimate interest, and primarily covers competing activities, it is not unimaginable that judicial case law would add to this category employees' freedom of expression on the Internet, with regard to the frequent occurrence of such conducts.[1663] Subsection (2) relates to employee behaviour outside working hours, while Subsection (3) deals with employees' freedom of expression: which is at the same time an activity conducted outside working hours. The stakes are high, as the different Subsections lay down different requirements towards the employee, against the different interests of the employer, and as a consequence they sanction different conducts.

Although Subsection (1) of Section 8 sets forth a general rule of conduct that can be applied to behaviour outside working hours as well, it will be examined separately in part (B), for the reason that this provision mainly relates to competing activities, and not to freedom of expression. Compared to this general requirement, Subsection (2) of Section 8 narrows down the respect of the employer's legitimate interest with regard to the employee's job or position in the employer's hierarchy, therefore such a restriction could be applied in exceptional situations. Also, instead of jeopardizing, Subsection (2) of Section 8 requires the behaviour to have the potential to *directly and factually* jeopardize not only the employer's legitimate economic interests, but also the employer's reputation or the intended purpose of the employment relationship. It is not obvious whether this more detailed formulation has real content or simply constitutes a wordier formulation.[1664] Moreover, Subsection (2)

[1658] Subsection (2) of Section 8 of the HLC: "*Workers may not engage in any conduct during or outside their paid working hours that – stemming from the worker's job or position in the employer's hierarchy – directly and factually has the potential to damage the employer's reputation, legitimate economic interest or the intended purpose of the employment relationship. The actions of workers may be controlled as defined in Subsection (2) of Section 9. When exercising such control, the workers affected shall be informed in writing in advance*."

[1659] Subsection (3) of Section 8 of the HLC: "*Workers may not exercise the right to express their opinion in a way where it may lead to causing serious harm or damage to the employer's reputation or legitimate economic and organizational interests*."

[1660] Subsection (1) of Section 8 of the HLC: "*During the life of the employment relationship, workers shall not engage in any conduct by which to jeopardize the legitimate economic interests of the employer, unless so authorized by the relevant legislation*."

[1661] Subsection (4) of Section 8 of the HLC "*Workers shall maintain confidentiality in relation to business secrets obtained in the course of their work. Moreover, workers shall not disclose to unauthorized persons any data learned in connection with their activities that, if revealed, would result in detrimental consequences for the employer or other persons. The requirement of confidentiality shall not apply to any information that is declared by specific other legislation to be treated as information of public interest or public information and as such is rendered subject to disclosure requirement*."

[1662] Pók 2012a. p. 162.

[1663] Pók 2012a. p. 163.

[1664] Pók 2012a. p. 162.

of Section 8 also refers to Section 9 on the restriction of employees' personality rights, requiring the same conditions to be applied when it comes to restricting personality rights.[1665]

Subsection (3) of Section 8 of the HLC contains a provision explicitly aiming to regulate freedom of expression through stating that: "*[e]mployees may not exercise the right to express their opinion in a way where it may lead to causing serious harm or jeopardizing the employer's reputation or legitimate economic and organizational interests[,]*"[1666] but it is not specified whether it relates to behaviour during or outside working hours, or to expression relating directly or indirectly to the employment. When assessing *expression connected to the employment*, jurisprudence has already elaborated the limits of employees' freedom of expression, through posing three criteria. First, it must be taken into account whether the expression is indeed capable of jeopardizing or influencing the functioning and the efficiency of the employer; second, whether the employee has respected the obligation of moderation (regardless of whether the content was true or false) and third, regardless of whether the recipients can be identified or not.[1667], [1668]

(A) Facebook: private or public space?

It was already referred to that both in France and in Hungary as a main rule, the dismissal cannot be based on employees' personal life. It will be presented in the following paragraphs that employees often allege that as they published the contested content in the course of their private life, it does not constitute a valid basis for dismissal. While it is true that in this case employees usually publish the questionable matter during non-working hours, from their own devices, from a place other than the employer's premises, it is not evident whether these communications have a private or a public nature.

Determining whether SNSs are private or public spheres has importance in both examined countries. *(a)* In *French labour law* if the employee expressed himself/herself in the course of a private correspondence, then he/she cannot be sanctioned based on the content with regards to the protection ensured by the right to respect for private life.[1669] The boundaries of public and private were determined by jurisprudence, ruling on several occasions on the nature of SNSs. *(b)* In *Hungarian labour law*, prior to the amendment in 2019, Subsection (1) of Section 11 of the HLC stipulated that the "*[t]he private life of workers may not be violated[,]*"[1670] requiring the protection of employees' private lives. This is the reason why it is important to determine whether SNSs are considered to be a public or a private sphere, as it will influence the monitoring.

[1665] Subsection (2) of Section 8 will be further presented in Section 2.

[1666] Subsection (3) of Section 8 of the HLC

[1667] Conclusions drawn from BH2009.255. cited in Pók 2012a. p. 162.

[1668] As these requirements were already clarified by the case law under the previous HLC, *László Pók* raises the question what the relations between Subsections (1), (2) and (3) are, whether specifying these three scenarios are substantially necessary. See more in: Pók 2012a. pp. 162–163.

[1669] Cour de cassation, chambre mixte, 18 mai 2007, N° 05-40803

[1670] Although the reasoning of the amendment argued that even without explicitly stating the prohibition of monitoring employees' private life, the existence of it is derived from the Fundamental Law and from the Civil Code. Source: *T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról*, 2019. p. 102.

a) Jurisprudence of French courts

Regarding the criterion of constituting a private or public sphere, in a private sphere, each individual is entitled to express himself/herself as he/she wishes: in such a case, even using excessive language is acceptable. However, this protection ends when the individual leaves this private sphere – the limits of which were set by case law.[1671] If the employee expressed himself/herself in the course of a private correspondence, then he/she cannot be sanctioned based on the content with regards to the protection ensured by the right to respect for private life.[1672] However, if the expression did not take place during a private correspondence, the case has to be assessed on the grounds of the freedom of expression (and it has to be examined whether abuse is present).[1673] In sum, if the expression took place during a *private* conversation, the case should be examined from the angle of the right to respect for private life, meaning that the employee cannot be sanctioned, even if the expression was abusive. However, if the expression did not take place during a private conversation, the affair will be examined from the angle of freedom of expression, where abusive remarks can be sanctioned by the employer.[1674]

Therefore, it is of crucial importance to determine whether SNSs are considered to be private or public space. Usually private correspondence takes place if the message is exclusively destined to one or several natural or legal persons who are determined or individualized.[1675] According to the Tribunal de Grande Instance de Paris, correspondence is protected if the content is exclusively destined by a defined person to another defined individual, in contrast to messages made available to the public.[1676] Therefore, courts had to deal with the question of whether communication taking place on SNSs are covered by the notion of private correspondence. Especially the use of privacy settings – when access to the content is limited and maybe accessible only to the friends of the employee – raised questions regarding the nature of SNSs. *(α) Courts* already addressed this question; however, their rulings were not always uniform. *(β)* Finally, the *Court of Cassation* clarified the issue; notably, through its Civil Chamber in 2013, and finally the Social Chamber in two decisions from 2017 and 2018.

(α) Assessment of the courts

During the last few years lower courts received several cases in relation to "Facebook firings". Generally, it can be said that these cases concerned employees who were dismissed because they published remarks on SNSs (typically on Facebook), relating to the workplace, employer or colleagues, which the employer found abusive. Employees pleaded that these matters took place in the course of a private conversation/correspondence; therefore, as they are entitled to the right to respect for private life, their dismissal could not legally be based on these remarks.

[1671] Caron 2018. p. 131.
[1672] Cour de cassation, chambre mixte, 18 mai 2007, N° 05-40803
[1673] Corrignan-Carsin 2018. p. 1762.
[1674] Loiseau 2018a. p. 23.; Corrignan-Carsin 2018. p. 1762.
[1675] TI Puteaux, 28 sept. 1999. Cited in: Lepage 2000. p. 25.
[1676] TGI Paris, 17e ch., 2 nov. 2000, n°9725223011 cited in: Bitan 2011.

The decisions of the courts were not always coherent[1677] regarding the private or public nature: as the exact circumstances could influence the decision, in some of them it was held that Facebook is a public sphere,[1678] therefore the employer could take these remarks into consideration; while other decisions stated that the communication remained in the private sphere, therefore it was protected by the right to respect for private life.[1679] However, several factors can influence the decision, such as the exact place where the content was published (e.g. on someone's own profile, on someone else's profile, in a private message, etc.), whether privacy settings were used (and if yes, exactly which settings were chosen) or whether the use of privacy settings could be proved.

One of the main factors to be considered is whether the employee *published* the content to his/her own *wall* or to another user's wall. In the case of publishing content to another user's wall, the employee loses control over the information, as it is subjected to the privacy settings chosen by the other user. In one case at the *Court of Appeal of Reims*,[1680] the employee contested the warning for misconduct that, as the employer alleged, he received for abusing his freedom of expression and breaching his duty of loyalty by posting insulting and defamatory remarks against his supervisor. The remarks were published to the wall of another employee and were available to everyone: the employer argued that Facebook is a public space, while the employee argued that Facebook is rather similar to an e-mail account and is considered as private correspondence. The Court of Appeal of Reims recalled that it cannot be ignored that Facebook, which is accessible through a simple Internet access, does not always guarantee the necessary confidentiality. According to it, posting a remark to the wall of another user potentially exposes the content to the public – depending on the privacy settings chosen by the other party, the use of which was not proved in the case. In addition, a private correspondence supposes that a message should not be read by someone to whom it was not destined: in order to have a private conversation, the employee should have sent a private message through the messaging service of Facebook.[1681] Therefore, the secrecy of correspondence was not violated by the employer.

The *Court of Appeal of Besançon*[1682] had to rule in a case relating to the dismissal of an employee who had a discussion on the wall of a former employee abusing the freedom of expression. The employee held that the discussion was a private conversation, as it took place on the wall of the former employee, available only to his Facebook contacts. In contrast, the employer held that the conversation was public as it could have been available to every user and if the employee wanted to have a private conversation, he should have used the function of sending private messages. The Court of Appeal stated that the aim of

---

[1677] As an illustrative example: on the very same day in cases relating to a dismissal based on the use of Facebook, the Court of Appeal of Besançon (CA Besançon, chambre sociale, 15 novembre 2011, n° 10/02642) ruled that Facebook is considered to be public, while the Court of Appeal of Rouen (CA Rouen, chambre sociale, 15 novembre 2011, N° 11/01827) ruled that is private.

[1678] E.g. CA Reims, chambre sociale, 9 juin 2010, n° 09/03205; CA Besançon, chambre sociale, 15 novembre 2011, n° 10/02642; CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343

[1679] E.g.: CA Rouen, chambre sociale, 15 novembre 2011, n° 11/01827 and CA Rouen, 15 novembre 2011, N° 11/01830; CA Bordeaux, chambre sociale, section A, 12 février 2013, n°12/01832; CA Rennes, 8e chambre prud'homale, 2 mars 2018, n° 16/07806

[1680] CA Reims, chambre sociale, 9 juin 2010, n° 09/03205

[1681] The *Court of Appeal of Rouen* held that the private messaging system of Facebook is considered to be of private nature. Source: CA Rouen, chambre sociale, 10 février 2015, n° 14/03335 and CA Rouen, chambre sociale, 15 mars 2018, n° 15/06042

[1682] CA Besançon, chambre sociale, 15 novembre 2011, n° 10/02642

Facebook is to display and create a network of contacts between different users, supposed to grow in an exponential way through the application of the principle "the contacts of my contacts become my contacts". Also, to a conversation taking place on the wall of a user, everyone could have access unless the user applied the privacy settings. It is the employee's responsibility to either use the alternatives offered by the site or, in the case of publishing content to another user's wall, to make sure prior to the publication that this user restricted access to his/her wall. Therefore, considering the basic nature and aim of the site and the fact that the employee had alternatives to ensure the private nature of the communication (through sending a private message), such conversation taking place on the wall is to be considered public.

However, when it comes to publishing content to the "wall", sometimes courts seem to ignore the functioning of Facebook. This is supported by the use of different terminology (e.g. publishing content to the "wall"[1683] or to the "public wall"[1684]). The word wall is particularly misused when a court stated that Facebook is considered to be a public space by its nature, unless the user takes precaution and creates "a wall" to prevent free access to the site.[1685] The *Court of Appeal of Pau*[1686] held that publishing content to the "private and public walls" without being able to prove that only the employee's contacts had access to the content on the "private wall" is considered to be public communication. Using the expression "private and public *walls*" is extremely confusing, as it is not clear what the Court of Appeal meant by that expression. In reality, every user has *one* "wall", which can be either public, private or customized depending on the chosen privacy settings.

In another case at *Court of Appeal of Reims*,[1687] an employee of a hypermarket was dismissed for a *comment* that he posted under a Facebook article of a journal, discussing the opening of the supermarket of Sundays. In his comment he encouraged customers to boycott the opening on Sundays and not to come to the supermarket on Sundays. The court of appeal started its analysis by pointing out that the employee is entitled to the freedom of expression both inside and outside the workplace. Then, it recalled that the expression constitutes an abuse if offensive, excessive or defamatory terms are employed.[1688] According to the court of appeal, the language used was excessive. As regards the public/private nature of the expression, the court of appeal found that such a comment goes beyond the 12 users who liked the comment, as the journal itself had 112,000 followers, and the article received 453 likes; therefore, the comment could potentially have been read by numerous users. As a result, such an abuse on the part of the employee constituted the breach of the obligation of good faith, making it impossible to maintain his employment relationship.

[1683] CA Montpellier, 4e chambre sociale, section A, 14 mars 2018, n°14/09173

[1684] CA Lyon, chambre sociale B, 22 novembre 2012, n° 11/05140

[1685] CA Fort-de-France, Chambre sociale, 21 décembre 2012, n° 12/00053. In Facebook, a "wall" is not created: if the user decides to post something to his/her profile, it will go to the wall, where access can be restrained through the use of privacy settings.

[1686] CA Pau, chambre sociale, 6 septembre 2018, n° 17/01648

[1687] CA Reims, chambre sociale, 15 novembre 2017, n° 16/02786

[1688] Also, the employee used the expression "we", making it obvious that he was an employee of the concerned workplace. The court of appeal also took into consideration that the comments were posted only 2 days before the opening.

Usually, the *use of privacy settings* has crucial importance.[1689] Employees often argue that content available to a limited audience such as "friends" or "friends and friends of friends" is considered to be private communication. Allowing access to friends and friends of friends is considered to be public: in 2011 the *Court of Appeal of Rouen*[1690] held that depending on the use of the privacy settings, Facebook can be considered either a private space or a public space.[1691] In the given case it was not proved whether the privacy settings chosen allowed access to an undetermined number of users (e.g. providing access to friends of friends), in a way that would make the conversation lose its private character. In addition, it was unknown how the employer had access to the content: it cannot be excluded that one of the participating users made him aware of the conversation. The *Court of Appeal of Paris*[1692] reached a similar conclusion in relation to a case where an employee limited the access to the content (only available to friends), and though the employee had 449 friends, the employer could not prove that members of the management or clients were amongst these friends, and the only fact that a colleague transferred the page to the management is not enough to establish the public nature of the wall.

The *employment tribunal* ("conseil de prud'hommes") *of Boulogne Billancourt*[1693] had to rule[1694] in a case where an employee who worked as a recruitment officer at the Société Alten Sir was dismissed for serious misconduct for sharing remarks that were inciting to rebellion and were denigrating on one of her colleague's Facebook wall. The employment tribunal stated that this colleague chose the privacy settings of sharing the content with "friends and their friends", as such ensuring a public access to the remarks, with the possibility especially for colleagues and former colleagues to access them. Such an access exceeds the private sphere, therefore the content is a legitimate proof, and the employer did not violate the employee's right to respect for private life.[1695] Such reasoning reflects common sense and is in line with the functioning of SNSs,[1696] but still ensures the possibility that if the appropriate steps are taken and limited access is set, it can be a private space.[1697]

Not limiting access will cause that the communication will take place in a public space. According to the *Court of Appeal of Fort-de-France*, Facebook is considered to be a public space by its nature, unless the user takes precaution and creates "a wall" to prevent free access to the site.[1698] Courts held that publishing content to the "wall"[1699] or

---

[1689] As a reminder, before introducing customizable privacy settings, Facebook offered the choice of available only to friends, to friends and friends of friends, to every Facebook user and to everyone.

[1690] CA Rouen, chambre sociale, 15 novembre 2011, n° 11/01827; CA Rouen, chambre sociale, 15 novembre 2011, N° 11/01830

[1691] In contrast, the *Court of Appeal of Douai* held that participating in a social network site excludes confidentiality. Source: CA Douai, ch. soc., 26 janv. 2018, n° 16/0068 referred to in: Caprioli 2018. p. 43.

[1692] CA Paris, Pôle 6, chambre 5, 20 septembre 2018, n° 14/04515

[1693] CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343

[1694] This case is quite significant and received much attention as it was the first decision in France addressing the private or public character of SNSs. Sordet 2010. p. 2228.

[1695] The tribunal then assessed whether the expressions used were abusive – which subject will be treated in part (b).

[1696] Hardouin 2011. p. 55.; Ray 2010a. p. 12.

[1697] Picq 2011. p. 2. (Page number referring to the online version of the article downloaded from: http://www.revuedlf.com)

[1698] CA Fort-de-France, chambre sociale, 21 décembre 2012, n° 12/00053

[1699] CA Montpellier, 4e chambre sociale, section A, 14 mars 2018, n°14/09173

to the "public wall",[1700] or "to the wall without using privacy settings to allow access only to the authorized persons",[1701] to "the wall to which every Facebook user had access",[1702] or to "a Facebook page without limiting the audience in any way"[1703] is considered to be public communication. The *Court of Appeal of Pau*[1704] held that publishing content to the "private and public walls" without being able to prove that only the employee's contacts had access to the content on the "private wall" is considered to be public communication. However, by stating that it is a public space because the employee was not able to prove that only his contacts had access to the content assumes that if only his contacts (which can mean a number up to several hundreds of users) had had access, the content would have been considered private.

The *Court of Appeal of Bordeaux*[1705] stated that the public nature of the conversation could not be proved, as there was no available information relating to the number of friends of the employee, or to the chosen privacy settings. However, earlier the court of appeal held that the user can choose between different privacy settings, such as allowing access to friends, to friends of friends or to every Facebook user – where the latter would make the conversation lose its nature of private correspondence. This could be interpreted as meaning that if friends and friends of friends had access, then – according to the court – the private nature of the communication would be established. The *Court of Appeal of Rennes*[1706] held that the bailiff stated that the employee's Facebook wall was accessible and therefore public, so communication on it was not considered as conversation between friends. However, it was not proven that the remarks were published on the wall. Therefore, they were reserved to friends and took place in a private setting. Thus, it is of great importance to define in a uniform matter whether SNSs are presumed to have a public or private nature as, if they are presumed to be public, the employee shall prove that despite all, the remarks were private, while if they are presumed to be private, the employer shall rebut the presumption by proving their public character.[1707]

Communicating within the *private messaging* system usually does not pose challenge, as it is usually recognized by courts that sending messages through the instant messaging service is considered to be private communication. The Court of Appeal of Reims held that as private correspondence supposes that a message should not be read by someone to whom it was not destined to, in order to have a private conversation, the employee should have sent a private message through the messaging service of Facebook.[1708] The *Court of Appeal of Rouen*[1709] held that the private messaging system of Facebook is considered to be of private nature, while the *Court of Appeal of Besançon* remarked that sending

---

[1700] CA Lyon, chambre sociale B, 22 novembre 2012, n° 11/05140

[1701] CA Aix-en-Provence, 9e chambre A, 27 mars 2015, n° 13/20847

[1702] CA Versailles, 17e chambre, 4 octobre 2017, n° 15/03872; CA Aix-en-Provence, 17e chambre B, 4 février 2016, n° 14/13125

[1703] CA Lyon, chambre sociale A, 13 mars 2013, n° 12/05390

[1704] CA Pau, chambre sociale, 6 septembre 2018, n° 17/01648

[1705] CA Bordeaux, chambre sociale, section A, 12 février 2013, n°12/01832

[1706] CA Rennes, 8e chambre prud'homale, 2 mars 2018, n° 16/07806

[1707] Inforeg 2015. p. 68.

[1708] CA Reims, chambre sociale, 9 juin 2010, n° 09/03205

[1709] CA Rouen, chambre sociale, 10 février 2015, n° 14/03335 and CA Rouen, chambre sociale, 15 mars 2018, n° 15/06042

private message within Facebook constitutes a solution to ensuring the private nature of communication on this primarily public sphere.[1710]

However, employees need to be cautious when accessing SNSs from their work computers as in certain cases private communication can lose its nature and protection. In a case in front of the *Court of Appeal of Toulouse*,[1711] the court found that the conversation of an employee who *forgot to disconnect* from her Facebook account when accessing this site from her work computer, which therefore was visible on the screen of the computer by anyone present in the workplace, lost its private nature. In another case at the *Court of Appeal of Caen*[1712] an employee accidentally accessed her colleague's Facebook account when typing Facebook into Google – as the latter forgot to sign out. There she saw her colleague's conversation that she found degrading, humiliating and violent, and reported it to the employer. However, when examining the documents provided by the parties, the court noted that when the employee accidentally accessed the Facebook account of the employee, she could have accessed the messaging system only after clicking on the button "messages" and then on this particular conversation. As such, the employer took into consideration messages that were identified as private (and without the presence of the employee) in irregular circumstances, not making it possible to rely on their content.

In sum, it is not unambiguous from courts' case law what exact conditions are necessary to be met in order to qualify the content on SNS as private – and ensure the protection of the right to respect for private life to it: in the light of the circumstances of the given cases, courts either found that Facebook was a public sphere,[1713] or a private one.[1714]

In most cases, courts – according to my opinion, correctly – ruled that Facebook is by nature a public sphere, except for the case of sending a private message, which was considered the most prominent example of ensuring private communication in this mainly public space. However, what is not clear is to what extent access should be limited, as courts mainly held that the content was deemed to be public because the user did not limit the access, but often stayed quiet regarding to what extent access should be limited. Although it seems accepted that a certain kind of limitation should be necessary in order to be qualified as private, for example, it is not clear whether access to friends is enough (also, such a concept is highly dependent on the number of friends as well). While the settings "friends and friends of friends" was deemed to provide access to an undetermined number of users and therefore was considered to be public, the formulation of other decisions suggested that only the "public" setting does not merit protection. In addition, questions of proof might constitute difficulties when addressing the private/public nature of SNSs, when it

---

[1710] CA Besançon, chambre sociale, 15 novembre 2011, n° 10/02642

[1711] CA Toulouse, 4e chambre sociale, 2e section, 2 février 2018, n° 16/04882

[1712] CA Caen, 1re chambre sociale, 27 janvier 2017, n° 15/04417; CA Caen, 1re chambre sociale, 27 janvier 2017, n° 15/04402

[1713] CA Reims, chambre sociale, 9 juin 2010, n° 09/03205; CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343; CA Besançon, chambre sociale, 15 novembre 2011, n° 10/02642; CA Reims, chambre sociale, 15 novembre 2017, n° 16/02786; CA Montpellier, 4e chambre sociale, section A, 14 mars 2018, n°14/09173; CA Lyon, chambre sociale B, 22 novembre 2012, n° 11/05140; CA Aix-en-Provence, 9e chambre A, 27 mars 2015, n° 13/20847; CA Versailles, 17e chambre, 4 octobre 2017, n° 15/03872; CA Aix-en-Provence, 17e chambre B, 4 février 2016, n° 14/13125; CA Lyon, chambre sociale A, 13 mars 2013, n° 12/05390

[1714] CA Rouen, chambre sociale, 15 novembre 2011, n° 11/01827 and CA Rouen, chambre sociale, 15 novembre 2011, N° 11/01830; CA Bordeaux, chambre sociale, section A, 12 février 2013, n°12/01832; CA Rennes, 8e chambre prud'homale, 2 mars 2018, n° 16/07806; CA Versailles, 17e chambre, 7 février 2018, n° 15/05739

could not be proved with certainty who had access to the content. Because of the lack of clarity, it was much needed that the Court of Cassation pronounces on this question – which luckily happened during the last years.

(β) Decisions of the Court of Cassation

The Court of Cassation addressed the subject of private or public nature of SNSs notably in three cases. The first one was held by the Civil Chamber in 2013,[1715] which contributed to unifying the divergent practice of lower courts. Then, in 2017[1716] finally the Social Chamber issued a judgement in the subject – although it was heavily criticized by several authors.[1717] Finally, in 2018,[1718] the Social Chamber pronounced another judgement, which contains important guidance when it comes to assessing the nature of employees' communication on SNSs.

In the case of *Civ. 1re, 10 avr. 2013, n°11-19530*, the main question to be decided was whether the content published by an employee of *Agence du Palais* was considered as public or as non-public insults. The employee, the author of the remarks, posted content such as "should pass an act for exterminating pain-in-the-ass managers, like mine !!!" or "exterminating pain-in-the-ass managers" and "eliminate our bosses and especially uptight bosses [using a feminine noun in French language] who are ruining our lives!!!" She posted these matters to the sites Facebook and MSN, in a way that it was only available to a determined number of users (a group with 14 members), who she personally allowed to access the content.

Regarding the *decision* itself *and its significance*, in this case, the Cour de cassation ruled the first time[1719] that "*[i]t is not a public insult if it is published on a social network account accessible only to authorized persons, in a very limited number by the author of the insults and who together form a community of interest*." In order to be qualified as non-public insult, the following three conditions must be meet: limited number of users has access, the owner of the profile has authorized them to participate in the conversation and they form a community of interest.[1720]

Regarding the limited number of users, it becomes clear that using the privacy settings "friends of friends" – the majority of user profiles – will not be included in this case.[1721] However, an important question arises: how many friends are acceptable? Qualifying them as *persona grata* does not cover cases when the employee accepts (maybe several hundreds of) friend requests, but refers to a more personalized authorization when the user is truly aware to whom he/she has granted access, cases where "only" the "friends" of the user have access without further distinction, should not be qualified non-public.[1722]

[1715] Cour de cassation, chambre civile 1, 10 avril 2013, N° 11-19530

[1716] Cass. soc., 20 décembre 2017, N° 16-19609

[1717] See notably the analysis provided by *Grégoire Loiseau* and *Sébastien Mayoux*. To be presented when analysing the decision.

[1718] Cass. soc., 12 septembre 2018, N° 16-11.690

[1719] Pierroux 2015. p. 5.

[1720] Since this decision, lower courts also adopted the same approach, e.g. the *Court of Appeal of Versailles* recalled that it cannot be stated that Facebook is a public space if it is not contested that it was only limited to the "friends" of the employee who formed a community of interest and was only available only to those persons in a limited number, authorized by the employee. Source: CA Versailles, 17e chambre, 7 février 2018, n° 15/05739

[1721] Ray 2013. p. 17.

[1722] Of course, the case is different if the user has 6 friends (15? 31?) or 873 friends.

When determining whether the participating individuals form a community of interest,[1723] judges adopt a casuistic and intuitive approach through examining the *in concreto* aspects of the case,[1724] as the exact notion of community of interest is yet to be determined.[1725] According to the decision itself, a community of interest consists of persons bound by a common membership, shared inspirations or objectives.[1726] In the light of this definition, a closed Facebook group assembling employees from the same workplace in order to discuss a specific matter or subject would be considered as a community of interest.[1727]

Although today Facebook allows users to use differentiated and customized privacy settings (making it possible to easily grant access to members of the community of interest), several other sites (e.g. Twitter or Instagram) opt for the all or nothing approach, not making the use of tailored privacy settings possible.

In the case of *Soc., 20 déc. 2017, n°16-19609* the employee, who worked at a foodservice company, was successively the victim of physical aggression when leaving the workplace and the victim of an attempted armed robbery within the workplace. The day after the attempted robbery, she was on leave because of her depressive state, and the employer made her sign a new employment contract. In order to declare the contract void due to the defect in consent, she provided proof establishing that even before the attempt she had been taking antidepressants and her state got worse due to the attack. In order to contest this argument, the employer produced as evidence information obtained from the work cellphone of (not the employee who contested the contract but) another employee.[1728]

The Court of Cassation ruled that "*having noted that the minutes of the bailiff's report […] requested by the company […], relating to information extracted from the Facebook account of the employee, obtained from the work cellphone of another employee, information reserved to authorized persons, […] the employer could not have access to them without posing a disproportionate and unlawful interference in the private life of the employee.*" In its reasoning by using both the expressions "disproportionate" and "unlawful", the Court of Cassation referred to two separate matters.[1729] *Grégoire Loiseau* notes that this judgement was particularly wrongly reasoned, as it mixed the separate questions of the ways of obtaining proof (question of legality of proof) and tracing the private or public nature of SNSs (question of right to respect for private life). Therefore, according to him, this decision failed to make a significant contribution.[1730]

According to *Sébastien Mayoux*, it is important to note that it was the first time that the Social Chamber ever ruled in relation to Facebook, still, the decision is far from being satisfying despite its importance and reveals a multitude of unanswered questions.[1731] For

---

[1723] Through the concept of "community of interest" it is acknowledged that individuals usually address a specific group composed of several individuals – without the intention of reaching people outside of this circle. Cassart 2013. p. 102.

[1724] Pierroux 2015. p. 6.

[1725] See the definitions and approaches presented by *Ronan Hardouin* in: Hardouin 2011. p. 55.

[1726] This definition is very similar to the one proposed by professor *Yves Mayaud*. He defined community of interest as "*common membership, shared inspirations or objectives […] of persons who form an entity closed enough for not to be perceived as involving third parties in relation to the author of the remarks.*" Mayaud 1998. p. 104.

[1727] Ray 2013. p. 16.

[1728] Péronne – Daoud 2018. p. 315.

[1729] Ray 2018. p. 11.

[1730] Loiseau 2018a. p. 23.

[1731] Mayoux 2018. pp. 24–25.

the subject of the monograph notably the (interconnected) questions of the way of obtaining access through the other employee and the question of when and whether these private matters can become public are relevant.

The decision is contrary to the previously established practice of courts according to which if the access to the content was restricted, the employer could not rely on it, and the same applied if he/she succeeded in obtaining it through a surreptitious way. However, if an individual who was originally granted access to the content decides to extract the information and to transmit it outside of the restricted access, it becomes public in a way that the employer can rely on it as proof.[1732] However, the Court of Cassation did not state precisely the way the employer obtained access through the other employee: did the employee voluntarily shared the information with the employer or did the employer accessed the information through exercising his/her right to monitor the use of professional equipment?[1733]

The Court of Cassation also stays silent regarding when such private content might become public. In addition, if the decision is interpreted extensively, it can lead to the re-examination of the existing practice, as it would make quasi impossible for the employee to reveal those matters to the employer.[1734] Besides, it was not specified what exactly is meant by information reserved to authorized persons.[1735]

Although the Social Chamber of the Court of Cassation finally ruled in the case of Facebook, the decision did not really help to establish a clear practice, as it mixed two distinct areas: the protection of the private life of the employee and the way of obtaining proof. Besides, the decision also lacked precision. Therefore, it was still necessary that the Social Chamber pronounces a decision in which it establishes the legal framework applicable to the exercising employees' freedom of expression on SNSs. Luckily, this happened in the decision of 18 September 2018.[1736]

In the case of *Soc., 12 sept. 2018, n°16-11.690*, the Court of Cassation had to rule again in a case concerning an employee of *Agence du Palais*, for exchanging remarks eerily similar to those in the 2013 case of the Civil Chamber. The employee was member in a Facebook group entitled "Exterminating pain-in-the-ass managers", where she published insulting and offensive remarks relating to her employer. These remarks were only accessible to a closed group of 14 persons, authorized to have access by the owner of the account. As a result of her comments, she was dismissed for serious misconduct.[1737]

The Social Chamber held that "*the disputed remarks do not constitute a serious misconduct if published on a Facebook account created by the employee, accessible only to persons authorized by him/her composing a closed group of fourteen people, as such comments constitute a conversation of private nature.*" By this, instead of referring to the wider notion of community of interest applied by the Civil Chamber in 2013, the Social Chamber applies the concept of private circle ("cercle privé") to determine the conditions of being qualified as private communication. Originating from copyright law, private circle in the context of social media and employment should refer to the circle of family and also

[1732] Mayoux 2018. p. 24.
[1733] Mayoux 2018. p. 24.
[1734] Mayoux 2018. p. 25.
[1735] Icard 2018. p. 85.
[1736] Loiseau 2018a. p. 23.
[1737] CA Paris, Pôle 6, chambre 8, 3 décembre 2015, n° 13/01716

to persons beyond family with whom private relations are usually maintained, designating a closed community or a network limited to close contacts who have close relations with each other or at least with one person from the group.[1738] In relation to SNSs, it is important to evoke that the Court of Cassation already pointed out that the term "friend" used in the context of SNSs referring to contacts within these sites is not identical to the term friend used to describe relationships in the traditional sense of the term.[1739] Therefore the private circle should not be merged with the online "friends" of the individual, as in order to be qualified as private communication, the determination of the persons who have access to the remarks is also necessary.[1740] Also, the number of persons having access to the content should be limited.

Besides this close relation between the participants in the conversation, there are two other important conditions that have to be met in order to qualify the communication as private: the number of persons having access and the determination of the persons who have access to the remarks. Regarding the number of users, it should be low: therefore, the question arises what is considered to be a low number in this context? As it is impossible to give a precise answer adequate to all situations, it will be the trial judge's task to determine these boundaries.[1741, 1742]

To sum up the *conclusions* drawn from the decisions of the Court of Cassation, the use of privacy settings in itself (opting for the use of "private" profile, which in reality rather means "not public") does not automatically qualify the information as private. The use of privacy settings making content available only to "friends" is considered public in the age when users often have several hundreds of contacts on these sites. Having a limited number of contacts (although it is not evident what is considered to be limited number) in itself is still not enough: persons having access to the communication have to be part of a private circle, meaning that they must have some kind of close relationship with each other. In addition, they cannot have automatic access, their access has to be determined by the individual owning the account. For example, a small group of colleagues discussing work-related matters would fall under this category.

In the context of *Facebook*, it means that creating, for example, a private group, or customizing the privacy settings of the posts to only share content with the members of the private circle would be a way to ensure the private nature of communication. *On other SNSs* – which do not allow the use of customized privacy settings –, creating chat rooms (instead of discussing those matters on the profile of the individual) for those few, chosen persons (colleagues in the context of employment) can be a way to ensure that the communication has a private nature.

b) Activities beyond working hours: the Hungarian Labour Code

In contrast to France, in Hungary, there is no abundant *jurisprudence* in relation to labour law and SNSs,[1743] as such it should be examined whether conclusions drawn from the French

[1738] Loiseau 2018a. p. 24.
[1739] Cour de cassation, chambre civile 2, 5 janvier 2017, N° 16-12394
[1740] Corrignan-Carsin 2018. p. 1762.
[1741] Loiseau 2018a. p. 25.
[1742] For example, the Court of Appeal of Aix-en-Province held in a case that having 179 friends does not constitute a private space for exchange. Source: CA Aix-en-Provence, 5 février 2016, n° 14/13717
[1743] Kardkovács 2016. p. 47.

case law can serve as a guidance for Hungary as well. In Hungary notably the following cases should be mentioned.

In 2013 the Curia ruled in the case of an employee who was dismissed due to his Facebook activity.[1744] With the statements used in the post, the employee threatened and insulted the employer and encouraged the fellow employees to get organized against the employer. The court of first instance held that the post was available to anyone, thus it was a public post and its content was able to cause the misjudgment of the employer.[1745] It also observed that the employee identified himself on his Facebook profile as an employee of the given employer – thus it was unquestionable who the post related to. The second instance court upheld this judgement and added that the post indeed could not be considered private and the language used overstepped the limits of the freedom of expression. The Curia affirmed this decision and argued that with the post in question the employee indeed breached his obligations, thus the dismissal was lawful.

Another case in Hungary related to a prosecutor, in which case the prosecutor's employment relationship was terminated due to the use of SNSs. The reason for termination was that the prosecutor shared three posts with political content during the election campaign in 2018. As a reaction to these posts, the prosecutor's office initiated disciplinary proceedings, and finally terminated the employment relationship of the prosecutor.[1746] The prosecutor turned to court, which held at the first instance that two posts were protected by the prosecutor's freedom of speech, and only the third one constituted a disciplinary offence.[1747] However, the court held that the sanction was excessive, and instead of the termination of the employment relationship, it ordered to decrease the payment category of the prosecutor.[1748]

[1744] Mfv. 10.469/2013/4.

[1745] It is important to note that the decision was based *on the previous HLC*, more precisely on its item c of Subsection (1) of Section 103 stating that emplyoees shall "*cooperate with their co-workers and perform work, and otherwise proceed in a manner without endangering the health and safety of others, without disturbing their work and causing financial detriment or damaging their reputation*;"

[1746] https://adozona.hu/munkajog/Pert_nyert_az_ugyesz_akit_harom_Facebookpos_RUXHRH (Accessed: 9 January 2020)

[1747] The *first post* was uploaded on 15th of March (a national celebration day in Hungary), a picture of a flock of sheep where the prosecutor wrote the caption "this is all that I am going to remember about the celebration of today. I stayed at home, sleeping, watching movies, reading. I hope that this time next year I will have the mood to go out." On this day the political opposition held protests and also a peaceful march was organized. According to the court, this post did not constitute political activity and did not have an effect on the work of the prosecutor or an impact on the independency of the prosecutor's office.
The *second post* was sharing a picture from the page "those who have been banned from the page of Orbán" (This is a reference to Viktor Orbán, Prime Minister of Hungary). In the picture uniting hands were seen, with a logo of the opposing parties on them and with the text: "If 1 million users share this picture, there will be cooperation! Now is the time, now or never!". The court held that it belonged to the freedom of expression of the prosecutor to share such a post, as it did not cause direct disadvantage for the image of the prosecutor's office.
The *third post* was the most problematic one. The prosecutor shared an article on a political person who might have participated in a fraud affair. The prosecutor wrote the caption "well, every 'accused' can choose his/her defense, we will laugh at him/her at most. Good luck… yeah, and 8th of April." (8th of April 2018 being the date of the then upcoming elections.) According to the court, from the circle of friends it was revealed that he worked as a prosecutor and as such, the post indeed endangered the prestige of the prosecutor's profession.

[1748] https://index.hu/belfold/2019/05/10/facebook_per_ugyesz_ugyeszseg_kirugas_itelet/ (Accessed: 9 January 2020)

The prosecutor's office appealed the decision, but in November 2019 the second instance court took the same position.[1749]

In the *media* a growing number of news can be observed, reporting the case of employees who were sanctioned or dismissed based on their activities. For example, in 2009 a telecommunication employee was dismissed for publishing a post on his Twitter account (although on the official and not his personal one) in relation to the temporary shutdown of a competitor service provider. Albeit the post was intended to be humorous, the employer found it unprofessional and contrary to fair competition.[1750] In 2016, an employee was dismissed for a Facebook post, in which he complained about the Sunday work that was ordered by the employer. Even though the post did not contain the employer's name, other employees commented it, and the employer found that by publicly questioning his measures, the employee discredited the employer and adversely influenced work ambiance.[1751, 1752]

As the examination of Hungarian case law does not provide answer to the private-public nature of SNSs, attention should be paid to the *doctrine*. However, the arising challenge is that, compared to French doctrine, the number of Hungarian authors dealing with this subject is more limited. Moreover, the question of the private-public nature of SNSs is raised in a different context. When examining Subsection (2) of Section 8 of the HLC, it is likely that this Subsection can be applied to the off-duty SNS use of employees[1753] – naturally, if other requirements are met. It was in relation to (former) Section 11 prohibiting the monitoring of employees' private lives that the question of whether off-duty SNS use falls under "private life" was raised.

At first sight, Section 8 and the protection of employees' private life might seem contradictory, as Section 8 seemingly authorizes the employer to monitor the private life of the employee, while former Section 11 stipulated that the employee's private life cannot be subjected to monitoring. *Gábor Mélypataki* and *Zoltán Rácz* resolve this contradiction by reasoning that difference should be made between the right to control (Section 8) and the right to monitor (Section 11). Namely, while Section 11 provides the employer a true power to monitor the employee (direct monitoring), Section 8 does not necessarily grant the right to monitor employees' behaviour outside working hours, but rather ensures the possibility to sanction the behaviour of the employee, as an indirect form of monitoring.[1754]

According to *László Pók*, although Section 8 authorizes the employer to restrict employees' behaviour outside working hours, the monitoring of such behaviour seems to be problematic, as it would be hard not to qualify behaviour outside working hours as pertaining to the private life of the employee. According to him, it is hardly acceptable to monitor employees' online SNS activity, conducted outside working hours and with the use

---

[1749] https://index.hu/belfold/2019/12/23/jogeros_vissza_kell_venni_a_facebook-posztjai_miatt_kirugott_ugyeszt/ (Accessed: 9 January 2020)

[1750] https://index.hu/tech/cellanaplo/2009/12/09/kirugtak_a_twitterezo_vodafonost/ (Accessed: 5 November 2018)

[1751] https://index.hu/belfold/2016/10/15/az_allasaba_kerult_hogy_a_facebookon_azt_irta_jo_iranyba_halad_a_szeker/ (Accessed: 15 November 2018)

[1752] Or see, for example, the case of a chancellor of a university resigning as a result of a scandal after posting pictures of refugees [https://index.hu/belfold/2015/09/28/lemondott_devecz_miklos_a_szegedi_egyetem_kancellarja/(Accessed: 3 May 2018)], a teacher posting about Nazi propaganda [https://444.hu/2015/09/10/kirugtak-a-tanitonot-aki-ket-hitler-kep-kozott-uzent-a-tankonyvekrol-a-facebookon/ (Accessed: 15 November 2018)] – all being referred to througout the Title.

[1753] Pók 2012. p. 15.

[1754] Mélypataki – Rácz 2018. p. 679., p. 682.

of their own devices.[1755] In contrast to this position, *Edit Kajtár* expresses a more nuanced opinion and recalls that the formulation of Section 11 allows the employer to monitor the behaviour of workers *to the extent pertaining to the employment relationship*, implying that the monitoring *per se* is not forbidden: if requirements are met, the employer might be allowed to monitor off-duty conducts as well.[1756] *Ildikó Rácz* joins this position and argues that with regard to Section 8, although only to a limited extent, the employee's off-duty online behaviour can be subject to monitoring.[1757]

Based on the above, according to the monograph, it is correct to interpret the HLC's provisions as allowing the employer to monitor off-duty SNS use. However, this monitoring cannot be unlimited: as in Hungarian law as well the concept of private life is associated with concealment, and protection is afforded against *intrusion* into the private life of the individual. According to *Gábor Mélypataki* and *Zoltán Rácz*, the arising legal question is whether an SNS post can be qualified as private secret. According to them, through a background check, the employer might gain access to information which can be qualified as private secret.[1758] However, they do not specify what scenario they mean by conducting background checks: the employer systematically going through the publicly available data on employees or the employer using stratagems to access data that the employee tried to seal from him/her?[1759] Neither do they define what exactly is understood under private secret in this context, and as a result, it is difficult to assess what they understand by private secret in the context of SNSs (Accessing private messages somehow? A closed group? A profile accessible only to contacts?).

According to civil law, the concept of "private secret" refers to any data, information or knowledge the keeping or isolation of which the owner of the secret is interested in[1760] – however, as it was addressed in Part I., privacy is a concept going beyond mere secrecy. With regard to the expressions "keep" or "isolate" the given information from the outside world, it is unlikely that the protection afforded to private secrets would apply to cases where the individual voluntarily decided to ignore the existence of privacy settings and to share the information publicly in social media. However, this concept can be evoked when the employer bypasses the employee's efforts to conceal the information, and somehow gains access to it; the consideration of SNSs as *per se* private spaces would constitute the complete ignorance of the basic functioning and nature of SNSs. It would be unreasonable to expect the employer not to look at the information which the employee voluntarily shared with the public. Of course, the situation might be different when the employee applied the privacy settings or made other steps to conceal the information from the public. Also, acknowledging the public character of such sites would not leave the employee without any protection, as data protection requirements must be met regardless of the public-private

---

[1755] Pók 2012a. p. 164.

[1756] Kajtár 2015. p. 203.
Kajtár also interprets the HLC as it only forbids to *violate* employees' private life and does not forbid it to be the subject of monitoring. Although in my opinion this conclusion does not obviously follow from the wording of the HLC in Hungarian, it is indeed reflected in its official English translation.

[1757] Rácz 2015. p. 285.

[1758] Mélypataki – Rácz 2018. p. 682.

[1759] Although they argue that the application of a "snitch regime" through encouraging employees in internal policies to report their colleagues in case they detect a questionable SNS post is considered illegitimate. Mélypataki – Rácz 2018. p. 682.

[1760] Commentary to Section 2:46 of the Civil Code.

nature of SNSs.[1761] According the monograph, French jurisprudence found the balance (even though it still needs to be refined in certain detail) – and therefore could serve as an example for Hungary as well –, according to which SNSs are considered to be public spaces unless the employee restricted the access to a considerable extent. French courts have already identified important criteria that should be taken into consideration at the decision-making, such as the use of privacy settings, the nature of the people who can have access to the post, etc. – which might serve as a guidance for Hungarian courts as well when they decide in similar cases.

(B) Criticising the employer?

In France, employees' freedom of expression comprises the right to criticize the employer or the workplace.[1762] However, the limit of this freedom is abuse: abuse is clearly identified in cases when freedom of expression no longer serves the freedom of expressing opinions and impart information objectively presenting a link with the professional activity, but rather constitutes a way of incriminating the morality or integrity of the employer or one of the managers, denigrating a supervisor or jeopardizing the employer's reputation or image.[1763] In *Hungarian law* as well, it was already elaborated that although the employee has the right to freedom of expression, including that he/she can criticize the employer, it does not mean that he/she can express his/her opinion in a way contrary to the economic and organizational interests of the employer, harming or jeopardizing them, ignoring the requirement of moderation.[1764]

In relation to SNSs it is not uncommon that the posts serving as a basis for dismissal contained excessive expressions and abused the employee's freedom of expression. As a result, it must be examined what the limits of such freedom are on SNSs. First *(a)* French case law will be addressed, *(b)* followed by Hungarian regulation.

a) Abusing freedom of expression: France

The employee's expression constitutes an abuse if he/she uses insulting, defamatory or excessive remarks.[1765] The limits of defamation and insults are defined by the Act on the freedom of press,[1766] while defining what constitutes an excessive remark depends on the

[1761] The NAIH already addressed the question from a data protection point of view: though it made statements in relation to the recruitment phase, these statements can be adequately applied to the case of employees' off-duty conduct and SNSs. According to the NAIH, it would be unrealistic to expect employers not to consult all these freely available information on prospective employees. Source: NAIH 2016. p. 19.

[1762] For example, the Court of Cassation found that – amongst others – the employee has the right to criticize the employer's commercial policy, or a project of the undertaking, or has the right to hand out flyers questioning managerial practices at the exit of the workplace. Loiseau 2014. p. 396.

[1763] Loiseau 2014. pp. 400–401.

[1764] 1050/2004. számú munkaügyi elvi határozat

[1765] Cass. soc., 30 octobre 2002, N° 00-40868

[1766] Article 29 of the Act of 29 July 1881 on the freedom of press: "*any allegation or attribution of an act that damages the honour or reputation of the person or entity against which the allegation or attribution is made constitutes defamation[,]*" and "*[a]ny offensive expression, term of contempt or invective which does not contain a specific allegation constitutes an insult*".

context.[1767] It can be determining, for example, if the remark has left the workplace and has become available to exterior persons, such as, for example, to clients.[1768] The position of the employee is also important: naturally, when it comes to expression on social media, the expectations are also higher towards someone who is in a higher position or is professionally recognized.[1769, 1770] Particularly three aspects of the subject will be examined: *first*, what kind of expressions are considered to be excessive, *second*, can humour or the use of smileys make the remarks lose their serious nature, and *third*, what importance the identification of the workplace/employer can have.

French courts already had to address the question of *abuse in relation to expression* on SNSs. The severity of the employee's acts was also well-founded in a case[1771] in which an employee published a comment under a grotesque picture representing the effigy in wax of an obese Louis X. having crutches as the king of gout – in which he compared this king to his manager in an injuring way. During the preceding year, the manager had to wear crutches for months, as she had broken her leg. The comment said that "anyway, he seriously reminds me of a manager that I knew" and it was publicly available for months. According to the court, the conjunction of the reported facts results in the impossibility of the employment relationship.

For example, courts held that an employee who consoled a former employee who had recently been dismissed, stating on the wall of the latter that "yes, it is clear, this company disgusts me" and "yes, it is certain that you are going to find something, it will enable you to see other horizons, but it still sucks the way they did it, they deserve to have the shitty workplace set on fire" was violent and excessive.[1772] In another case,[1773] the employee acted in an disrespectful way and it constituted a serious misconduct when she qualified her colleagues as "piece of trash" or wished her colleague "a nice day with the fools", approved of calling her boss a "stupid fat asshole" who is "disgusting with [her] but she's not gonna get far with her enterprise", adding that "she works with big pussies". Also, an employee's comment in relation to the opening of the supermarket on Sundays using the expression "bunch of assholes"[1774] was considered to be an excessive term.[1775] In another case,[1776] the court found the severity of the acts established when the employee posted a picture of a woman pointing a gun towards the lenses of the camera, with the description "feeling of the day" and repeated death threats against the personnel of the workplace. According to the court, as these remarks were not destined to a specific person, they did not constitute a death threat in a criminal law way; however, they had an extreme nature, as she alluded to committing a violent act against a part of the personnel.

[1767] Caron 2018. p. 132.

[1768] Caron 2018. p. 132.

[1769] Ray 2011. p. 136.

[1770] That was the case when a recruitment officer – who is in contact with job applicants and prospective employees – published excessive remarks relating to the workplace in a public discussion. Source: CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343

[1771] CA Orléans, 28 février 2013, N° 12/01717

[1772] CA Besançon, chambre sociale, 15 novembre 2011, N° 10/02642

[1773] CA Toulouse, 4e chambre sociale, 2e section, 2 février 2018, n° 16/04882

[1774] He stated that "Goin there n workin on Sundays bunch of asshole its not you who wake up and who hav a family life do not piss us of by goin there Sundayy !!!!!!!"

[1775] CA Reims, chambre sociale, 15 novembre 2017, n° 16/02786

[1776] CA Versailles, 17e chambre, 7 février 2018, n° 15/05739

Today, it is part of popular culture that *users use different smileys* during online written communication, especially on informal sites such as Facebook. Smileys can "express" different feelings such as happiness, sadness, anger, etc. However, the exact meaning of smileys is harder to be interpreted than interpreting their equivalent feelings in the offline world. Therefore, employees might try to reason that due to the use of smileys, their remarks were not serious, but had a funny or humorous[1777] nature instead of being excessive.[1778]

In the case of Barbera v. Société Alten Sir,[1779] where employees participated in a conversation on one of their colleague's Facebook wall, the employee argued that the remarks that she wrote were only jokes and should not be taken seriously. She supported this statement by recalling that at the end of the remark she added "ha-ha-ha" (encouraging a colleague to join the local ritual and "piss [the manager] off" the "whole day without her noticing it" and then "make her life impossible for months, ha-ha-ha"), which therefore made the content humorous. However, the employment tribunal found that in this context these remarks ending with the phrase "ha-ha-ha" could not be interpreted in a humorous way and they were able to damage the employer's reputation and therefore the dismissal was well-founded.

The humorous character of the remarks was not established by the *Court of Appeal of Paris*[1780] in a case where the employee, a professor posted certain incriminating remarks in the Facebook group of his year. He made exchanges of particularly displaced familiarity with his students: he teased and taunted certain of them and said, amongst others, regarding the upcoming oral exams that "formal attire is required […] the one who comes dressed as Jabba the Hutt, I will give him/her 20 out of 20,[1781]" or alluded to the fact that he could be bribed: "OK I admit, 10 euros for a bonus point, I give in". He defended himself by stating that he was not abusing his freedom of expression, as these remarks were humorous, they were taken out of their original context. However, according to the court, a professor engaging in such conduct of teasing his students and of adopting such familiarity, even if the students are of age, constitutes a wrongful conduct and an abuse of his freedom of expression. From these cases it seems that the excessive nature of the content does not seem to be affected by the use of smileys.

Being able to *identify who is concerned in these posts* can have an importance. Employees regularly argued that these remarks did not relate to the employer/workplace, and therefore they did not constitute a breach of their obligation arising from the employment contract. In a case at the *Court of Appeal of Besançon*,[1782] the employee took part in a discussion taking place on the wall of a former colleague and defended herself by arguing that she never named the employer in the discussion: the employer's identity was revealed later by another employee, after she had logged out from the site. However, according to the court of appeal, although the employee did not identify the employer, still, the latter was identified and the lack of intent of the employee to identify the employer had no effect as long as her imprudent conduct led to the same result – even if she had logged out from the site.

[1777] According to the Court of Cassation, the use of a humorous style can be considered as an attenuating circumstance. Source: Dabosville 2012. p. 276. referring to Cass. soc., 2 février 2011, N° 09-69351

[1778] Picq 2011

[1779] CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343

[1780] CA Paris, Pôle 6, chambre 9, 3 décembre 2015, n° 15/04533

[1781] 20 is the highest mark that a student can have in the French educational system.

[1782] CA Besançon, chambre sociale, 15 novembre 2011, N° 10/02642

In another case at the Court of Appeal of Rennes,[1783] the employee cited the lyrics of a song stating "the bosses, the bosses, they are like pigs"[1784] and argued that it was not established that it related to the employer. However, the court noted that he posted this text as a response to an employee's post, which clearly related to the employer and all happened two days after there was a misunderstanding at the workplace in relation to premiums. From this context it was unquestionable that the text related to the employer. In the case[1785] where the employee complained in an excessive comment regarding the opening of the workplace (a supermarket) on Sundays, the fact that he used the expression "us"[1786] made it obvious that the comment came from an employee of the supermarket – contributing to establishing the existence of the abusive nature of the remarks.

At the *Court of Appeal of Fort-de-France*[1787] the employee did not contest the insulting nature of her remarks,[1788] but argued that the remarks were not relating to her supervisors, but to a third person who was a manager in an association where she did voluntary work. The Court of Appeal did not accept this reasoning, as according to it, this phrase spoke for itself, especially because it was published in a particularly tense atmosphere, as the day before a meeting was organised, where the management – composed of women originating from the French mainland – confronted the employees over a previous incident.

However, the *Court of Appeal of Reims*[1789] did not find the link established between the employer and the employee's remarks in a case where the employee stated "our boss, he is really autistic, do you know a special centre where she could be treated?". The court remarked that on the one hand, no one was named in the text, and the expression boss ("*chef*" in French) is used not only to designate the professional relationship within the employment context. Also, even the employer itself was not certain who was targeted by this text (he hesitated between a colleague and a member of the management). Therefore, it was not unambiguous who this text was about, as consequence, it did not constitute a breach of the employee's obligation.

In conclusion, the criteria that can help French courts in assessing whether the expression used was excessive is the style used (which is not alleviated by smileys) and also the identifiability of the employer. French courts typically found that the use of excessive expressions is present when the employees expressed themselves through employing typically vulgar expressions or through serious content, such as death threats. Although employees might try to argue that these expressions were only humorous due to, for example, the use of smileys, such argumentation is not accepted by courts. Also, being able to identify the employer or the workplace can have an importance: without explicitly naming the person/company to whom the remarks are destined, courts often establish the link between the remarks and the workplace from the context.

[1783] CA Rennes, 8e chambre prud'homale, 2 mars 2018, n° 16/07806

[1784] Song of *Les sales majestés* entitled *Les patrons*. In French the original lyrics was "les patrons, c'est comme les cochons".

[1785] CA Reims, chambre sociale, 15 novembre 2017, n° 16/02786

[1786] "Goin there n workin on Sundays bunch of asshole its not you who wake up and who hav a family life do not piss us of by goin there Sundayy !!!!!!!"

[1787] CA Fort-de-France, chambre sociale, 21 décembre 2012, n°12/00053

[1788] "but when your management treats you like a last piece of shit, you can flip out, especially when it's a White who comes to make rules in your country"

[1789] CA Reims, chambre sociale, 9 juin 2010, N° 09/03205

b) Freedom of expression: Hungary

In Hungarian law the employee can express his/her critical opinion towards a supervisor or a colleague without being sanctioned/reprimanded for it if it is based on real facts and states nothing which is capable of disturbing the order and discipline at work or discredit or insult the employer. Therefore, an employee can express his/her opinion in a "neutral", not insulting way, without aiming to influence other employees, while the use of harsh words and unspeakable forms is not permissible.[1790, 1791] Although criticizing the employer is comprised in the right to freedom of expression, the employee cannot exercise this right by ignoring the requirement of moderation and jeopardizing the employer's interests, as that would constitute the infringement of the obligation of cooperation.[1792] He/she cannot exercise this right by making any possible shortcomings public in the press, in a way detrimental or harmful to the economic and organizational interests of the employer.[1793, 1794]

When it comes to restricting employees' off-duty behaviour, Subsection (2) of Section 8 refers to the conditions set in Subsection (2) of Section 9, namely that such a restriction shall be strictly necessary for reasons directly relating to the intended purpose of the employment relationship and shall be proportionate for achieving its objective. Therefore, *completely* prohibiting employees to express their opinion in relation to the employment seems contrary to the principle of proportionality, while it is legitimate to impose limitations on the way they do it.

Employers are not the only target of employees' posts: they can also aim at colleagues. According to a decision[1795] relating to sexual harassment, it was held that the obligation of cooperation comprises mutual respect and conduct taking into consideration the dignity of the other employees, therefore any conduct infringing these requirements can be sanctioned. However, the employee can express his/her opinion on the behaviour or professional conduct of a colleague in a way which is not offensive and does not influence other employees.[1796]

Thus, the employee cannot post on SNSs content which would be disparaging, smearing, degrading or offensive in relation to his/her employer. The publication of such matters is

---

[1790] BH 1991/47.

[1791] For example, it is not considered to be the breach of the duty of cooperation if the employee – through exercising the freedom of expression – summarizes and presents information that was already said in a public hearing from the employees' point of view.

[1792] 1050/2004. számú munkaügyi elvi határozat

[1793] 1050/2004. számú munkaügyi elvi határozat

[1794] However, the following case should be mentioned, which did not take place in social media or did not involve the use of excessive expression, yet it resulted in the breach of Section 8. In the case the employee, who worked as a teacher in the very school attended by his child as well, signed a petition as a parent with the aim to achieve that the same teachers teach the pupils for a certain period of time. As a result, the employer asked him to provide a report containing what he would propose as a solution to the situation and also why he took a position against the school. According to the employee, asking for such a report is contrary to the freedom of expression.

The Curia noted that the letter was then intended to be forwarded to supervisory institutions as well and contained a statement that "we believe that the change would influence the educational and mental development of our children in a negative way." According to the Curia, the content of the letter was capable of questioning the legality and appropriateness of the employer's measure – as a result, the employer's request of a report did not breach the right to freedom of expression. Source: Kúria, Mfv.II.10.609/2017, par. 25.

[1795] BH 2006.201.

[1796] BH 1991. 47.

considered as a breach of obligation.[1797] However, what was stated in relation to French law is adequately applicable to Hungarian law as well: the boundaries of expressing opinion in an excessive way are already established, SNSs do not fundamentally change these boundaries, they rather favour the use of more excessive expressions, which an employee/user normally would not use in an offline, face-to-face communication.

The Constitutional Court provided more criteria as regards the limits of employees' freedom of expression in *Decision No. 14/2017. (VI. 30.)*. In this decision the Constitutional Court examined the limits of employees' freedom of expression,[1798] and draw attention to the already existing criteria in this field. Among them it must be examined (1) whether the content has a connection to public life or professional life,[1799] (2) whether it is composed of facts or rather constitutes a value judgement,[1800] (3) whether the expression caused damage, (4) whether the employee acted in good faith[1801] and (5) what sanctions were applied by the employer.[1802]

In conclusion, different factors should be taken into consideration when assessing whether an expression on SNSs is included in employees' freedom of expression: the criteria that can determine the easiest way is whether the expression was excessive – which can notably be determined through the style used. However, the existence of other criteria might be more challenging, such as whether it was a public expression or not,[1803] whether it related to a public affair, etc.

c) Is a "like" considered as expressing opinion?

An expression can take several shapes, such as posting, commenting, writing a blog entry (supposing the user actively creates content), etc. Although the presented cases mostly concerned expression as a post or a comment, the question still arises whether – in contrast to creating content – simply "liking" an already existing content on social media can be considered as an expression of the employee's opinion?

[1797] Kun 2013. p. 15.

[1798] The original case related to an employee who worked as a human resources management specialist at the employer. In his free time he published blog entries to a blog dealing with HR questions, with the aim of sharing knowledge, identifying himself as an expert in the field. The employer found out about the blog, and terminated the employment relationship with the reason that the employee jeopardized the employer's legitimate interests and breached his obligation of confidentiality through posting blog entries in a field and in a subject where he was directly involved in his workplace. Source: Mfv. 10.655/2013/6.

[1799] In the case the Constitutional Court held that publishing the blog entries belonged to the professional life and did not constitute a public affair ("közügy"), as such they were not afforded protection as a fundamental right, suggesting that the expression is protected to an increased extent if it relates to the discussion of public affairs. Source: Decision No. 14/2017. (VI. 30.) of the Constitutional Court, par. 40.

[1800] The Constitutional Court held that opinions expressing value judgment require greater tolerance, whereas as regards statements expressing facts or rumors, greater care can be required from the employee (both when the opinion relates to a public affair or when it is not). Source: Decision No. 13/2014. (IV. 18.) of the Constitutional Court, par. 41.

[1801] The expression should not receive protection if it merely or intentionally aims to damage the employer's reputation or to insult the employer/supervisor/etc. Source: Decision No. 14/2017. (VI. 30.) of the Constitutional Court, par. 33.

[1802] Decision No. 14/2017. (VI. 30.) of the Constitutional Court, par. 34.

[1803] To determine this, the analysis of French case law and the above-drawn conclusions from it might constitute a guiding point.

Different solutions appeared to address this question: a US and a Belgian case will be addressed briefly, as they relate directly to this matter and might serve as an example to France and Hungary in similar cases. In 2012, in the *US* in a case relating to whether a "like" is considered to be a manifestation of free speech (and therefore entitled to legal protection under the first amendment) adverse decisions were adopted by the district court and the court of appeal. The case related to six employees who, during the campaign of the re-election of the sheriff, liked Facebook pages supporting the sheriff's opponent. After the re-election of the sheriff, they alleged that they were not reappointed because of exercising their freedom of expression and contested the decision. The *district court* held that simply liking a Facebook page is insufficient to merit constitutional protection, as no actual statements were made through liking.[1804] However, the *court of appeal* ruled that by liking the content, the employees unmistakably approved of the opponent's candidacy, and added that from a constitutional point of view there was no difference between liking the page, or expressing the same support through typing a supportive message. According to the court of appeal, liking the opponent's Facebook page is to be deemed equivalent to displaying a political sign in one's front yard – which is accepted as substantive speech.[1805]

In *Belgium*, the labour court of Liège had to rule in a case where an employee was dismissed for liking controversial content relating to "*quenelle*", which can be interpreted as a disputable sense of humour, with publicly known anti-Semitic connotation. The antecedents were that in 2013 the employee *posted* links to his Facebook wall, relating to "*quenelle*". Following these posts, the employer organised a meeting and made the employee sign a written commitment, stating that in the future he is not going to post such controversial content, as it can influence other employees and might put him and his posts in false light. However, in 2014 he *liked* content relating to "*quenelle*" and was dismissed as a result. The labour court of Liège held that a "like" can be understood as a sign of interest, but also as an approval, and in the light of the commitment that he had signed, it constituted the expression of the employee's opinion and validated the dismissal.[1806, 1807]

However, "likes" might not always mean that the given individual truly likes or approves of the content. Meanings of likes are not always unambiguous, as was pointed out by *Emmanuel Netter*. He underlined that over a thousand people "liked" an article which appeared in Le Monde entitled "Argentina: several French killed after a collision of helicopters". At that time pressing the like button was the only way to rapidly express "emotion", besides writing a comment or clicking on the "neutral" share button. So, what does "like" mean in this context? Did users like the fact that they were rapidly informed of the event? Or the style of the article? Did they express their support to the victims' families? Did they truly like what happened? The signification of the use of a simple like button can often be ambiguous; therefore one must be careful before drawing conclusions

---

[1804] United States: District court for the Eastern District of Virginia: Bland v. Roberts, 4-11cv45 (E.D. Va.; Apr. 24, 2012)

[1805] United States: Court of Appeals for the Fourth Circuit: Bland v. Roberts, No. 12-1671, Filed: September 23, 2013

[1806] Cour du travail de Liège (3e ch.) – Arrêt du 24 mars 2017 – Rôle n° 2016-AL-94

[1807] In Switzerland a user was fined for liking defamatory posts written by a third party that accused an animal rights activist of anti-Semitism, racism and fascism. The court held that by liking the content, he endorsed and further distributed the comments. https://money.cnn.com/2017/05/31/technology/facebook-like-defamation-switzerland/ (Accessed: 15 October 2018)

from it.[1808] According to *László Pók*, considering a "like" as expressing opinion would lead to an exaggerated, unrealistic approach, which would unnecessarily restrict employees' possibilities to use SNSs. According to him, a like does not necessarily express the employee's endorsement, but rather raises attention to a matter, making it unreasonable to draw far-reaching conclusions.[1809]

However, it should be mentioned that ever since Facebook introduced the so-called "reaction" buttons in 2016, more nuanced reactions can be expressed than a simple like, such as "like", "love", "ha-ha", "wow", "sad" and "angry". Although this function gives users the possibility to express other types of feelings, in line with the above-mentioned doubts relating to the meaning of "like", a simple "reaction" should not necessarily be treated as the user's substantive attitude towards a matter.

To summarize, different views exist regarding whether a like constitutes freedom of expression or not. These views illustrate that it is challenging to provide an answer to this matter valid under all circumstances. Thus, circumstances of the specific case should be taken into consideration (such as whether liking was a one-time activity or it is regular, existence of a previous warning) as they can be determinant when assessing a case. First, it is even possible to accidentally hit the like button (either from a computer, but especially from the small screen of a smartphone), therefore far-reaching conclusions should not be drawn from a few likes. Naturally, the situation is different if the employee systematically likes content that can place the employer into a disadvantageous situation or be otherwise compromising. Second, special circumstances can justify the strict appreciation of likes, such as previous warnings addressed to the employee. That was the case in the previously presented labour court of Liège's decision, where raising awareness and warning the employee were determining factors in judging the dismissal to be lawful. Nothing indicated that the court would have arrived at the same conclusion if the employee had not been explicitly warned before.[1810]

§2 Other conducts

Employees might – intentionally or negligently – jeopardize the employer's legitimate interests and rights in other ways than by expressing their opinion. Notably, the cases of *(A)* revealing confidential information and business secrets and *(B)* jeopardizing the employer's legitimate economic interests through working for the competition must be mentioned. However, these cases seem to raise specific privacy issues to a lesser extent,[1811] compared to freedom of expression on SNSs. In my opinion, revealing confidential information or business secrets on SNSs or engaging in a competing activity does not substantially raise questions in relation to the personal life of the employee and to the established/blurred boundaries of personal and professional life. As the focus of the monograph is on employees' personal life, these cases will be presented only briefly in the following paragraphs. Also, through social media and SNSs, employees can eternalise and share

[1808] Netter 2015. p. 54.
[1809] Pók 2012a. p. 163.
[1810] https://www.droit-technologie.org/actualites/perdre-emploi-a-cause-dun-jaime-cest-possible/ (Accessed: 15 October 2018)
[1811] Pók 2012. p. 13.

(C) various pranks with the public, which might jeopardize or damage the employer's reputation.

(A) Business secrets

In *France* employees are required not to reveal information that they obtained during exercising their functions.[1812] Some, such as union representatives, employee advisors, the delegation of the members of the personnel of the social and economic committee[1813] are bound by the professional secret and obligation of discretion. Similarly to French regulation, Subsection (4) of Section 8 of the *Hungarian Labour Code* states that employees have the obligation to respect confidentiality and the employer's business secrets.[1814] Although through the advent of social media the possible disclosure of business secrets on these platforms is a growing issue due to the ease of using these platforms and the lack of awareness of employees[1815] (especially the use of professional SNSs, such as LinkedIn can raise problems),[1816] the examination of these questions will not be included in the monograph, as they primarily relate to the employer's personality rights and not to the personality rights of the employees.

SNSs can serve as a means to reveal confidential information.[1817] As the advent of social media made it easier to commit abuses and to discover them, in the case of employees' expression, the discoverability or revealing business secrets either intentionally or negligently is higher as well. In one of the *French cases*, although it related to the public sphere, a police officer's employment was terminated for revealing confidential information on SNSs. The officer was substituting someone at the municipal police as a technical assistant and a disciplinary dismissal was given for breaching his professional obligations, which consisted in revealing SNS pictures and other information relating to the organisation of the municipal police, and especially to the video surveillance system applied in the municipality.[1818]

Hungarian media reported the case in which the employee, who was chief legal counsel at a bank, sent a message to his girlfriend, stating that he is investigating someone's case. Although he did not identify the client – who was a well-known actor –, he used his monograms, and added that as the case seems to be problematic, now he can have revenge for a certain Hungarian television show. As he named the show, the client became identifiable through his monograms. His girlfriend shared this message and commented it as "[t]hat's

---

[1812] Lahalle 2016. par. 146.

[1813] Article L2143-21, Article L1232-13, Article L2315-3 of the FLC

[1814] Subsection (4) of Section 8 of the HLC. More detailed regulation is to be found in Act LIV of 2018 on the protection of business secrets.

[1815] Warren – Pedowitz 2011. p. 100.

[1816] https://jogaszvilag.hu/szakma/a-kozossegi-media-hasznalata-munkaltatoi-szemmel/ (Accessed: 6 September 2018)

[1817] For example, one employer in Canada terminated the employment relationship of a maintenance employee for reasons of breaching confidentiality, who – after a patient committed suicide – posted two pictures of the scene to social media. Maier 2013. p. 297.

[1818] Conseil d'Etat: N° 393320 (ECLI:FR:CECHR:2017:393320.20170320), 3ème – 8ème chambres réunies, 20 mars 2017

how things go when one's boyfriend is a chief legal counsel at a big Hungarian bank!" On the ground of sharing bank secrets, his employment was terminated.[1819, 1820]

In relation to restricting employees as regards revealing information that they learned during the exercise of their functions, the phenomenon of *whistleblowing* should be mentioned.[1821] Employees can benefit from the publicity of SNSs and might also use them as platforms to realize whistleblowing, and to raise the public's attention to illegal acts, abuses or misdeeds taking place within the workplace.[1822] Technically, in these cases the employee commits a breach of obligation (as revealing illegal acts of the employer will damage the employer's reputation, and/or will consist of revealing confidential information that would have otherwise stayed hidden). For several reasons (e.g. rapidity, ease, size of the audience that might be reached, etc.) SNSs might constitute a forum to reveal those illegal acts – in which case the employee's online activity on SNSs will realize the breach. Even though whistleblowing through SNSs raises several challenges,[1823] according to the monograph such conduct does not substantially concern the boundaries of employees' personal lives, as it reveals something that the employer committed, instead of revealing a part of the employee's personal life. For this reason, it will not be addressed in detail in the monograph.

[1819] https://index.hu/tech/2012/01/04/banktitkot_sertett_egy_magyar_mikroblogger/ (Accessed: 7 September 2018)

[1820] An Austrian court held the violation of bank secret in the case where the employee, who was a cashier in a bank, engaged in a conversation on his Facebook wall, relating to the reappearance of – previously missing – 15,000 euros. Kajtár 2016. p. 161.

[1821] Both in France (Act N. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernization of the economy) and in Hungary (Act CLXV of 2013 on Complaints and Public Interest Disclosures) a whistleblowing act regulates these matters. Also, the EU's new whistleblowing directive [Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law] regulates the question at an EU-wide level.

[1822] For example, in 2006, *Michael De Kort*, who worked as a project manager at the global company Lockheed Martin in the aerospace, defence, security, and technologies industry. In 2004 he became aware of certain security risks in relation to ships that were sold to the US coastguard. He repeatedly reported those security risks to his supervisors, who did not react to this. Then, he uploaded a 10-minute-long video to YouTube, in which he presented these security risks in detail. https://www.youtube.com/watch?v=qd3VV8Za04g&t=316s (Accessed: 16 April 2018)

Brandon Huber worked at the Golden Corral restaurant, where he noticed that the meat that was to be prepared was stored outside the restaurant, directly next to the rubbish bins, in not acceptably hygienic conditions. According to him, after he reported this to the management, they did nothing to solve the situation. In response, he made a video, in which he showed how meat was stored and uploaded it to YouTube. https://www.youtube.com/watch?v=yb0yrdDOy0g (Accessed: 16 April 2018)

Johannes Izak Beaurain worked as a nurse in the Groote Schuur Hospital in the Republic of South-Africa. On several occasions he reported different abuses, which were investigated, but finally were not found well-established. He did not agree with the outcome of the investigations, and he revealed the alleged abuses to the public in a Facebook post. He was dismissed for his actions, and he challenged the decision at court. However, the court held that Mr. Beaurain's allegations were not well-established. http://www.seesa.co.za/whistle-blowing-on-social-media/ (Accessed: 22 April 2018)

[1823] See more on whistleblowing and social media in: Hajdú, József – Lukács, Adrienn: *Whistleblowing és a közösségi média szerepe a korrupció elleni fellépésben*. Nemzeti Közszolgálati Egyetem, Budapest, 2018

(B) Employer's legitimate economic interests and rights and competition

According to Subsection (1) of Section 8 of the *HLC*, "*during the existence of the employment relationship, employees shall not engage in any conduct which would jeopardize the legitimate economic interests of the employer, unless so authorized by the relevant legislation.*" This provision requires employees to refrain from such conduct.[1824] There exists no exhaustive list enumerating what conducts are capable of jeopardizing the employer's legitimate economic interest and therefore what limitations can be imposed on employees: particularly, performing work for another employer should be mentioned, but limitations on employees' freedom of expression or the obligation to respect the employer's business secrets also fall into these categories[1825] – the latter two are regulated by specific provisions.

Under Subsection (1) it is already elaborated what conducts the employee should refrain from, such as, for example, the employee performing work for another employer, creating competition under any legal relationship, contributing to the activity of a competing business, etc.[1826] In this regard, social media does not represent a substantial challenge, as its use does not affect the freedom of action and through it the boundaries between personal and professional life; instead, it can contribute to the *discoverability* of the possible infringement.

French labour law contains similar provisions in order to protect the employer's legitimate economic interest. Naturally, employees are subject to a non-compete obligation:[1827] in the light of the duty of loyalty, they should not engage in competing activity.[1828] For example, the Court of Cassation held that the following employees violated the duty of loyalty: an employee having a high position, who during his paid leave engaged in an identical activity at a directly competing company, in the same geographic zone;[1829] or an employee, who worked as a mechanic, and during his sick leave had a vehicle repaired by asking another employee to help, but on his own behalf;[1830] or the fact that an employee took part in a training at the employer's competitor constituted the breach of the duty of loyalty.[1831]

Similar challenges may arise not only during the existence of the employment relationship but *after the employment relationship* as well. According to *French labour law*, following from the fundamental principle of free exercise of a professional activity and Article L. 1121-1 of the FLC,[1832] the parties can conclude that after the termination of the employment relationship, the employee should refrain from engaging in the same sector of activity as the employer.[1833, 1834] The exclusivity clause should also be mentioned here: although it does not concern the time period after the employment, in my opinion for the

---

[1824] *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről*, 2011.

[1825] Kardkovács 2016. p. 44.

[1826] On this subject and on the relevant case law see more in: Kardkovács 2016. pp. 44–45.; Ember 2015. pp. 115–119.; Szladovnyik, Krisztina – Horváth, István: A munkáltató jogos gazdasági érdekeinek védelme. *Adó*, 30(14), 2016. pp. 92–96.

[1827] Ray 2018. p. 443.

[1828] Waquet – Struillou – Pécaut-Rivolier 2014. p. 71., p. 311.

[1829] Cass. soc., 5 juillet 2017, N° 16-15623

[1830] Cass. soc., 21 octobre 2003, N° 01-43943

[1831] Cass. soc., 10 mai 2001, N° 99-40584

[1832] Cass. soc., 10 juillet 2002, N° 00-45135

[1833] Waquet – Struillou – Pécaut-Rivolier 2014. p. 309.

[1834] The detailed conditions (being indispensable for the protection of the legitimate interest of the employer, limited in time, limited in space, providing financial counter value, taking into consideration the functions of the employee) were laid down by the Cass. soc., 10 juillet 2002, N° 00-45135

subject of the present monograph it raises challenges similar to the ones encountered in the non-competition agreement. An exclusivity clause forbids the employee to engage in any other professional activity – even if the activity would not have a competing nature.[1835]

The *HLC* states that the employer and the employee can decide to conclude a non-competition agreement, in which they state that the employee shall not engage in any conduct – for up to two years following the termination of the employment relationship – by which he/she would infringe upon or jeopardize the rightful economic interests of the employer.[1836] Usually these agreements pertain to future employment at the competition; however, they might as well stipulate that the employee should refrain from certain acts in social media.[1837] Nonetheless, even in the absence of a non-compete agreement, general provisions laid down in civil and penal regulations will provide protection to the employer.

SNSs do not only serve to keep in touch with friends and family, but employees also use these services to forge online relationships with colleagues, clients or customers (especially professional SNSs such as LinkedIn). Therefore, their use might constitute the violation of a non-compete agreement. Differentiation should be made particularly between two scenarios. *First*, while the use itself might not constitute a violation, SNSs can serve as evidence of violation, such as when former employees update their professional status, revealing their new position.[1838] *Second*, SNS use *itself* might be considered as a violation when it comes to restraining from certain conduct: several questions arise, such as: does "friending" constitute a violation? Or accepting a friend request? How to prove who initiated the contact? Do concerned employees have to unfriend existing contacts with clients? Who has ownership of a LinkedIn account?[1839]

(C) Employee "pranks"

Employees can also jeopardize the employer's reputation in more "creative" ways, notably through different "pranks" – at the same time serving as evidence of breaching requirements of hygiene or workplace safety. According to the HLC and French labour law as well, the employee must respect the employer's reputation.[1840] The issue is that in some cases these activities can be directly linked to the workplace, e.g. due to a uniform, taking place on the premises of the workplace etc., thus having possible consequences on the employee's employment relationship and/or on the employer's reputation.

[1835] Waquet – Struillou – Pécaut-Rivolier 2014. pp. 73–74., p. 313.

[1836] Subsection (1) of Section 228 of the HLC

[1837] Pók 2012. p. 15.

[1838] For example, in the cases Cour d'appel, Paris, Pôle 1, chambre 3, 28 Mai 2013 – n° 13/06055 and Cour d'appel, Saint-Denis (Réunion), Chambre commerciale, 15 Juillet 2013 – n° 12/01321 both employees who allegedly violated their non-compete agreements updated their professional status on LinkedIn. Source: Nivelles 2014. p. 12.
Another example is the case of *Kelly Services, Inc. v. Marzullo* in the US, in which the employer found out about the violation of the non-compete agreement through information posted on the employee's LinkedIn profile commenting on his new position. Source: Anderson 2011. p. 896.

[1839] See more on the arising questions and the answers that can be possibly given to them in: Anderson 2011. Warren – Pedowitz 2011. pp. 99–114.; Mooney, Joshua A.: Locked Out on LinkedIn: LinkedIn Account Belongs to Employee, not Employer. *Intellectual Property & Technology Law Journal*, 25(6), 2013. pp. 16–18.

[1840] Subsection (2) of Section 8 of the HLC and the duty of loyalty (obligation de loyauté).

Often, such behaviour also constitutes the violation of workplace rules (e.g. safety, health, hygiene). Examples include the US case, where the prank made by two employees of a restaurant chain seriously compromised the company's reputation in a few days. The two employees made a video and uploaded it to YouTube, in which one of them prepared food for delivery completely violating health-code standards (e.g. by putting cheese up his nose or nasal mucus on the sandwiches). Although the employees alleged that the food was never delivered, the video was seen by more than a million Internet users and caused a true crisis for the restaurant.[1841] Similar examples include restaurant employees who bathed in the utility sink and eternalized this moment in social media.[1842]

Another case is the *Taylor v Somerfield Stores Ltd* case from the *UK*. The case related to the termination of employment in a case where the employee uploaded a video to *YouTube* in which his colleagues during working hours, on the premises of the workplace, wearing the employer's uniform, hit him on the head with a plastic bag full of plastic bags. The employer found that the publication of such a video jeopardized its reputation. However, the employment tribunal ruled that the termination was unlawful, as there was no obvious connection between the video and the employer (the name of the employer was not visible on the uniform, only its colours could have given away its identity, while the video was recorded in a storage room, anonymous to an outsider). In addition, the video was only available for three days and was viewed by eight persons (three of them were managers at the company).[1843]

Sometimes such conduct can go beyond being a simple prank: in 2018 the employees of a well-known low-cost airline company made a "prank" by publishing a fake photo that later caught considerable media attention. They published a picture to Twitter, after a tense period due to repeated strikes, in which the employees were lying in their uniform on the floor and creating the impression that they were forced to sleep on the floor. However, the photo was staged as was revealed by the security footage published by the company. The company dismissed the employees for gross misconduct.[1844]

The circumstances that gained importance in the above cases – and which might be used in the future when assessing similar situations – were the following: the nature of the activity (Does the act itself relate to the workplace? The nature of the behaviour: does the act qualify as a breach of workplace safety rule, or is it ill-intentioned – or is it rather a harmless prank?), as well as the identifiability of the employer (Could the behaviour be linked to the employer? Did the employee wear a uniform? Or was the employer identifiable in another way?).

In conclusion, direct connection between the workplace and the employee's activity on SNSs can be established in several ways: the content can directly relate to the workplace/employer/colleagues (e.g. publishing negative opinion), it can take place at the workplace (e.g. bathing in restaurant sinks) or the employee can wear the employer's uniform in a picture. The most common form of possibly questionable content relates to the employees' expression and not to other conducts, such as pranks.

[1841] https://www.nytimes.com/2009/04/16/business/media/16dominos.html (Accessed: 3 May 2018)

[1842] http://www.nbcnews.com/id/26167371/ns/us_news-life/t/burger-king-worker-fired-bathing-sink/#.XUgxoo4zbct (Accessed: 5 August 2019) or shorturl.at/bcuwG (Accessed: 5 August 2019)

[1843] Taylor v Somerfield Stores Ltd. Case no: S/107487/07 Held at Aberdeen on 24 July 2007

[1844] https://www.theguardian.com/business/2018/nov/07/ryanair-sacks-six-cabin-crew-after-staged-photo-sleeping-on-malaga-airport-floor (Accessed: 19 November 2018)

In the course of their personal life employees often think that they are free to do anything, including expressing themselves in social media – as it is demonstrated by the growing case law of "Facebook firings". Although both in France and in Hungary employees are entitled to the freedom of expression, which can even include the right to criticize the employer, this right is not unlimited: expressing themselves in an abusive way[1845] can result in the termination of their employment relationship. Even though the personal lives of the employees are protected, the majority of case law and scholars – correctly – found that expressing oneself on SNSs goes beyond the personal sphere, unless strict precautions are taken and the access is limited to a few other users who are in a close relationship. However, the existence of these criteria must be assessed on a case-to-case basis as no universal rule can be established.

The presented case law and media cases illustrated that on SNSs employees tend to use extreme or vulgar expressions, a harsh, insulting style. Combining this with the fact that these expressions are often available to the public (due to either not using the privacy settings or letting a big audience access it), and with the increased possibility to identify the employer, employees' off-duty behaviour on SNSs can cause considerable harm to the employer's reputation.

Section 2. Off-duty conduct without direct connection to the employment

Although most articles dealing with off-duty conduct and SNSs focused on the limits of the employees' freedom of expression in relation to the employment, it is also important to address the question of employees' behaviour independent of the workplace: employees' posts on SNSs can relate not only to the workplace but also to other subjects, without a direct connection with the employment. As a preliminary point it should be noted that in such cases, the possible intrusion into the employees' private life is more intense, therefore if the application of a restriction or legal consequences is possible, it must meet even stricter requirements and safeguards than in the case of behaviour with a direct connection to the employment.

What was understood by direct connection to employment is expression explicitly aimed at the workplace/employer/colleagues or content recorded in a uniform or on the workplace premises. Indirect connection refers to cases other than direct connection: here, no link can be established with the workplace at first sight. However, such behaviour, too, can have consequences for the employment or can reflect badly on the employer: employees might express themselves in a way that can result in jeopardizing the employer's legitimate interests through especially inciting public outcry. This is notably the case of expressing political opinion,[1846] opinion in relation to current events,[1847] news, religion, science (e.g.

[1845] E.g. by using insulting or vulgar expressions.

[1846] Although in the following case it was not the employee who decided to upload the content in question, SNSs still functioned as a channel for publicity: an employee got dismissed after the wide publication of a photograph of her in social media, where she is seen showing her middle finger towards the President of the US's motorcade. https://www.washingtonpost.com/local/flipping-off-president-trump-has-changed-julibriskmans-life--and-exposed-our-divisions/2017/11/07/19efab02-c3f6-11e7-afe9-4f60b5a6c4a0_story.html (Accessed: 14 August 2019)

[1847] See, for example, the case of a paramedic employee who, after an 88-year-old man opened fire in a museum, was injured but was finally saved by paramedics, expressed his disagreement and stated that it was the

"flat Earth believers", antivaccination, esoteric, etc.) etc.[1848] Besides freedom of expression, employees' lifestyles can also raise the question of whether such conduct can jeopardize the employer's legitimate interests, and if yes, what requirements should such behaviour fulfil? Such behaviour might be connected to revealing employee's lifestyles, such as the consumption of alcohol,[1849] cigarettes, drugs,[1850] or leading a promiscuous lifestyle – and documenting it on social media. Although it takes place purely in the course of the employees' private lives, employers might not be enthusiastic about employees documenting on Facebook their wild Saturday nights or the details of their love (or even sexual) lives – especially if the individual can be linked to the workplace as an employee.[1851]

To such cases *(§1)* in *French law* a different set of rules is to be applied – that of non-disciplinary dismissals – where it is not a breach of obligation that serves as a basis for the termination of employment but the existence of a so-called characterised serious disorder. In contrast, *(§2)* in *Hungarian labour law* the same, already-presented provisions (Section 8) are applicable, with the difference that they should be interpreted in a stricter way, as employees' "purely" private lives are at stake. Also, in Hungarian law, it is possible to terminate the employment relationship without notice in cases when the employee did not commit a serious breach of duties but engaged in behaviour to shake the trust between the parties,[1852] typically including cases connected to the employee's behaviour outside work, making it impossible to maintain the employment relationship.[1853] For example, a Facebook post might result in a loss of trust,[1854] serving as a ground for termination without notice.[1855]

---

paramedics' chance to make a difference, and also suggested that the other guards should go to target practice. Mgrditchian 2015. pp. 117–118.
Another example is the case of J*ustin Hutchings* from London, Ontario, who was fired in 2012 because he published offensive content to a memorial website of a teenager who committed suicide after being a victim of bullying for years ("Thank God this B---- is Dead"). Mr. Hutchings identified his employer in his profile, and one of the users easily "tracked him down" from that information and reported his behaviour to his employer. http://rabble.ca/columnists/2012/10/employees-beware-perils-posting-facebook (Accessed: 11 May 2018)

[1848] An example can be mentioned from Canada, where *Christopher Maximillian Sandau*, then hockey coach was fired for content on his Facebook profile, promoting Nazi propaganda. Parents and officials discovered the content. http://www.cbc.ca/news/canada/british-columbia/delta-hockey-coach-christopher-sandau-fired-over-nazi-posts-on-facebook-1.2825623 (Accessed: 3 May 2018)

[1849] See, for example, the already presented case of *Ashley Payne*, an American high school teacher, who was dismissed for posting pictures of herself holding a pint of beer and a glass of wine in her hand during her trip to Europe. https://www.californiabusinesslitigation.com/2013/05/high_school_teacher_files_an_a.html (Accessed: 3 May 2018)

[1850] However, a strict separation is not possible between personal and professional life: although as a main rule these activities take place in the course of the employee's personal life, they can have an effect on his/her health resulting in labour law consequences as well (e.g. sick leave).

[1851] This was the case when an employee had a blog where he shared his otherwise inappropriate opinion in a context where he did not criticise the employer, only mentioned him. In his blog, he identified himself as an employee and also shared pictures of himself taken at the workplace. The issue was that in the same blog, he also shared his admiration for Hitler and shared racist and violent content. Ellickson – Atkinson 2013. p. 265.

[1852] Hajdú – Kun 2014. p. 167. E.g. he/she engages in conduct unworthy of his/her job by leading a lifestyle of revelry and alcoholism, substantiated suspicion of committing a serious criminal offence.

[1853] Cséffán 2016. p. 309.; Gyulavári 2012. p. 216.

[1854] Kozma 2013. p. 10.

[1855] Mfv.I.10.469/2013/4 Cited in: Cséffán 2016. p. 311.

§1 Non-disciplinary dismissals and characterised serious disorder

In French law according to the main principle, an element pertaining to the personal life of the employee cannot constitute misconduct.[1856] As it was demonstrated, in order to pronounce a disciplinary dismissal, the employee must breach an obligation arising from the employment contract. However, the employer can still apply *non*-disciplinary dismissal[1857] if the employee's actions realised in the course of his/her personal life caused a *(A)* characterised serious disorder in the functioning of the workplace.[1858] In such a scenario, it is not the employee's actions themselves that justify the dismissal, but rather the disruption in the functioning of the workplace:[1859] the characterised serious disorder that is caused. *(B)* Such a characterised disorder can appear not only in the offline world, but on SNSs as well.

(A) Characterised serious disorder

In contrast to disciplinary dismissals, where the breach of obligation justifies the dismissal, in the case of a characterised serious disorder it is the sufficiently serious consequences of the employee's conduct for the functioning of the workplace which allow the employer to terminate the employment contract,[1860] as the behaviour of the employee affects the functioning of the workplace to such an extent that it is not possible to continue to employ the employee without causing damage to the workplace.[1861, 1862]

When assessing the severity of the caused trouble, the judges take into consideration the nature of the duties of the employee, the company's purposes and the effects of the employee's behaviour outside and inside of the workplace.[1863] Regarding *the company's purposes*, this requirement initially aimed ideologically oriented enterprises or faith oriented enterprises ("entreprise de tendance"),[1864] where the specific orientation of the workplace can have an effect on the expectations towards the behaviour of an employee in the course of his/her personal life.[1865] Later, it was extended to "everyday" workplaces not having a particular orientation, and the Court of Cassation acknowledged that even these enterprises

---

[1856] Cass. soc., 16 déc. 1997, n° 95-41.326

[1857] It cannot be emphasized enough that regardless of the consequences that this act caused to the workplace, such a characterised serious disorder does not allow in itself to apply a disciplinary sanction against the employee. Source: Cour de cassation, chambre mixte, 18 mai 2007, N° 05-40803

[1858] The two regimes cannot be mixed: if the employer issues a disciplinary dismissal against an employee for causing a characterised serious disorder, courts will qualify the dismissal unjustified. Baugard 2015. p. 87.

[1859] Gillier 2009. p. 213.

[1860] Inforeg 2015. p. 68.

[1861] Antonmattei 2012. p. 10.

[1862] For example, the existence of a characterised serious disorder was established in a case when a director of a centre hosting protected persons was accused of sexual molestation of a minor (Cass. soc., 21 mai 2002, 00-41.128), or in a case when an employee deliberately hit his girlfriend, herself an employee of the workplace as well, in the close proximity of the workplace and the incident gave rise to reactions from the stuff. Source: Richard de la Tour 1999

[1863] Inforeg 2015. p. 68.

[1864] Jacquelet 2008. pp. 270–271.

[1865] E.g. it can be reasonably expected that an employee working for political party A does not actively and publicly support political party B on his/her SNSs.

can have such a purpose that can justify the dismissal of an employee based on his/her private live.[1866] However, as such a dismissal should meet very strict requirements, it is rare that an ordinary enterprise can rely on a characterised serious disorder.[1867] When it comes to the *functions of the employee*, it can be stated in general that the higher the position is, the more exemplary behaviour can be expected from the employee.[1868]

When it comes to the characterised serious disorder itself, it is important to state that not any disorder can be qualified as such: as the denomination itself suggests, it has to be characterised and *serious*, implying that the disorder has to be sufficiently perceivable and obviously disturbing so that a third person could consider them as such.[1869] It is not only the employer who should perceive the employee's acts as disturbing, but they have to be objectively qualified as disturbing for the functioning of the workplace.[1870] Such a disorder must be more than a simple inconvenience created for the employer, and must be truly harmful for the employer.[1871]

The disorder should also be *characterised*, meaning that a slight disorder is not sufficient: it must be serious and persistent.[1872] What needs to be assessed is whether the employee's actions have discredited the workplace, resulted in negative reactions from clients, from the public or from employees, or have jeopardized the employer's interests considering its functions, responsibilities, its size, its sector of activity, reputation.[1873, 1874]

(B) Characterised serious disorder and social network sites

Just like their behaviour in the offline world, employees' behaviour on SNSs can also result in a serious characterized disorder. Such might be the case when the employee posts an offensive content which results in public outcry and other users reporting the case to the employer. The advent of SNSs gains importance in two regards when it comes to non-disciplinary dismissal: on the one hand, it facilitates the discoverability of employees' behaviour and on the other hand, it can facilitate proving the existence of a disorder.

First, in order that a dismissal to be lawful on the ground of causing a characterised serious disorder, strict requirements must be met, as the purpose of the workplace and the functions of the employee must be considered in addition to determining the existence of a characterised serious disorder. What social media notably changed is the *discoverability* of such conducts: a possibly reprehensible conduct (e.g. buying a Peugeot car while working for Renault, being interested in swinger parties, practising psychic activity while being a doctor's assistant[1875])

[1866] Jacquelet 2008. p. 272.
[1867] Perraki 2015. p. 438.
[1868] Jacquelet 2008. p. 509.
[1869] Jacquelet 2008. p. 276.
[1870] Perraki 2015. p. 440.
[1871] Aubert-Monpeyssen 2007. p. 588.
[1872] Perraki 2015. p. 440.
[1873] Corrignan-Carsin 2009. p. 46.
[1874] On the characterised serious disorder see more in: Waquet 2006. pp. 304–310.; Perraki 2015. pp. 435–447.; Jacquelet 2008. pp. 266–280.; Antonmattei 2012. pp. 10–13.
[1875] These are references to the cases: Cass. soc., 22 janvier 1992, N° 90-42517; Cour de cassation, chambre mixte, 18 mai 2007, N° 05-40803; Cass. soc., 21 oct. 2003, n° 00-45.291. Although these conducts did not take place on SNSs, in my opinion they could have resulted in a characterised serious disorder if they had taken place on SNSs.

can be widely "advertised" by users.[1876] Due to the publicity of content published or activities taking place in social media, it is more probable that the reprehensible conduct of the employee becomes known by interested parties (e.g. clients, employees or the public) – while before, their discoverability by the employer remained more incidental.

Second, SNSs can highly facilitate *proving* the existence of an objective disorder, as the characterised disorder can be manifested also in negative reactions from clients, from the public or from employees. While earlier, in the pre-SNS era it required more time and effort to submit a complaint (e.g. buying an envelope, writing a letter, addressing and sending it), today e-mail and the official Facebook pages dedicated to a company have made it considerably easier and faster to express dissatisfaction or indignation relating to the conduct of an employee. As a result, possibly more people are keen to express their dissatisfaction on SNSs than in the offline world. It is another change that usually the style of these online complaints is also less official and more overheated[1877] – making it more plausible to establish indignation from these people.

Consequently, in such cases, the SNS post itself cannot be enough to establish the existence of a characterized serious disorder: its effects as well must be taken into consideration. However, SNSs made it easier to detect the public's indignation because if a post goes viral, it might result more easily in public outcry (e.g. messages sent to the employer, public comments under the post or under the shared post, its appearance in news portals): thus it is able to constitute the basis of a non-disciplinary dismissal.

§2 Off-duty conduct and the Hungarian Labour Code

Compared to French law, in Hungarian regulation there is no such differentiation between disciplinary and non-disciplinary dismissals:[1878] if the conditions required are met, Section 8 applies as well to off-duty behaviour not directly relating to the employment. More precisely, Subsection (2) on behaviour outside of working hours and Subsection (3) on employees' expression are of particular importance with regard to the subject. Although professional articles usually focus on the employees' freedom of expression, this question includes wider matters: besides expression, employees' behaviour (e.g. photo or video) should also be examined.

In the case when the content published to SNS directly relates to the employment, the legal basis is provided by the employee's duty of loyalty, which means that the employee must not harm the employer's reputation. Although every employee is entitled to the freedom of expression, it was determined that following from their status as employees,

---

[1876] Although the example does not relate to the employment, the scandal of a low-cost airline in 2019 can illustrate how widespread a simple post can become: after boarding, a passenger found that the woman seated next to him had a chair with no back. He took a picture of it and posted it to Twitter. The tweet soon went viral: it received more than 6,000 re-tweets, and appeared in the headlines of several news portals – while in reality the passenger was reassigned the seat and no one was sitting on the backless chair. In the pre-SNS age a similar story might have stayed within the circle of the passenger's friends and family. https://edition.cnn.com/travel/article/easyjet-backless-seats-scli-gbr-intl/index.html (Accessed: 7 August 2019)

[1877] Ray 2018. p. 12.

[1878] Even though such categories do not exist in Hungarian law as the cases of dismissal are regrouped according to a different logic, it was already presented that in Hungarian law as well it is possible to dismiss an employee without the breach of obligations.

this freedom is not limitless. In the case of content (or behaviour) not directly relating to the employment, stricter conditions must be met in order to be able to sanction the employee. Due to the visibility/publicity of SNS posts, a possibly compromising content can easily go viral and result in the other users' indignation – making it easier, compared to the pre-SNS age, to sanction the employee for behaviour committed solely in the course of his/her personal life.

(A) Behaviour outside of working hours

Although in the public sector it is accepted that public employees are bound by certain restrictions even outside working hours, it was questioned whether such restrictions can be applied to the employees of the private sector.[1879] In Decision No. 56/1994 (XI. 10.), the Constitutional Court laid down important ground rules relating to public employees' behaviour outside working hours, and later the substance of it inspired Subsection (2) of Section 8. Since the adoption of the HLC, as a new provision, it imposes restrictions on the behaviour of employees outside working hours, by stating that "*[w]orkers may not engage in any conduct during or outside their paid working hours that – stemming from the worker's job or position in the employer's hierarchy – directly and factually has the potential to damage the employer's reputation, legitimate economic interest or the intended purpose of the employment relationship.*"[1880]

Although Decision No. 56/1994 (XI. 10.) relates to public servants ("közalkalmazott"), it provides a point of interpretation for restricting private employees' behaviour.[1881] In this decision, the Constitutional Court examined a provision of the Act XXXIII of 1992 on the Legal Status of Public Servants, stating that public employees shall behave in a way worthy of a public employee, taken into consideration his/her job and position, even outside the workplace.[1882] Although the Constitutional Court did not find this provision unconstitutional, it identified the conditions of the application of such a rule. It highlighted that even within the public sphere differentiation must be made between public employees, as public servants bear public functions to a lesser extent than civil servants. In the case of the latter, the general underlying public interest is not present in the case of every public servant, and as a consequence, such a restriction should be subjected to the strict requirement of proportionality and necessity. Therefore, restricting public employees' behaviour outside the workplace is only necessary and proportionate if the behaviour is unworthy with regard to the job or position of the public employee and has a substantial and real, direct effect on it and causes the harm of the employer's interests.[1883] However, in the case of private employees public functions are completely absent: here, the employer's private interests face employees' fundamental rights.[1884]

Subsection (2) of Section 8 (on employees' conduct during or outside paid working hours) of the HLC is connected to the obligation of cooperation incumbent upon the

[1879] See more on the subject and on the relevant case law in: Kardkovács 2016. p. 45.
[1880] Subsection (2) of Section 8 of the HLC
[1881] Pók 2012a. p. 161.
[1882] Subsection (2) of Section 39 of Act XXXIII of 1992
[1883] Decision No. 56/1994 (XI. 10.) of the Constitutional Court
[1884] Pók 2012a. p. 160.

employer and the employee. The employment relationship is a long-term, trust-based relationship, which affects not only the parties' conduct during the performance of rights and obligations, but to a certain extent also the private life of the employee. This requirement is also enshrined among the employees' obligation, namely, that the employee shall perform work in such a way that demonstrates the trust vested in him/her for the job in question.[1885] This means that the employee cannot behave in a way, even outside the workplace, that would influence maintaining his/her employment. Demonstrating trust vested in him/her for the job in question does not relate to the non-respect of the employees' obligations, but rather to circumstances making it impossible to maintain the employment. Naturally, the position of the employee within the hierarchy of the employer has importance when assessing the questioned behaviour.

However, the restriction of employees' conduct outside working hours is influenced by two circumstances according to Subsection (2) of Section 8: by the employee's job or position within the employer's organisation and by the effects of the conduct.[1886] Following from the requirement of what can normally be expected in the given circumstances, an employee's conduct is weighed differently according to *his/her job or position* within the hierarchy of the employer. According to *László Lórodi*, the nature of the employer should also be considered when judging, as there is a difference whether a factory worker out of thousands of workers publishes, for example, a sexually explicit content on social media, or if a teacher does that.[1887] Regarding the effects of such conduct, the HLC regulates *what kind of behaviours* are capable of harming the employer's interests: the conduct must present a direct and factual potential to damage the employer's specified interests.[1888]

According to Subsection (2) of Section 8, it is possible to *restrict* employees' conduct, but a restriction is only permissible if it meets the requirements set in Subsection (1) of Section 9 relating to the restriction of personality rights. Namely, it must be deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and proportionate for achieving its objective. Subsection (2) also adds that when the employer exercises such control, the employees affected shall be informed in writing in advance.

These provisions laid down in Subsection (2) of Section 8 are applicable and therefore impose limits on the employees' online behaviour on SNSs. However, these limits must be interpreted very strictly: they depend on the position of the employee, and can only relate to behaviours which have the potential to directly and factually damage the employer's different interests.[1889] Especially with regard to the absence of the public function in private sector employment law, such a restriction should be limited to a narrow circle and to exceptional cases, to the case of severe harm of the employer's legitimate interests, when the possible harm exceptionally, in a well-defined way outweighs the employees' right to privacy.[1890]

[1885] Item d) of Subsection (1) of Section 52 of the HLC

[1886] *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről*, 2011. pp. 99–100.

[1887] http://munkajogportal.hu/mik-azok-a-munkajogi-alapelvek-es-mire-valok/ (Accessed: 6 September 2018)

[1888] Subsection (2) of Section 8 of the HLC. This is a stricter requirement compared to Subsection (1) of Section 8, which requires simple jeopardizing.

[1889] Kun 2013. p. 14.

[1890] Pók 2012a. p. 161.

Regarding the categories of persons, it is likely that executive employees[1891] are primarily concerned by these provisions, requiring them to act according to more severe expectations.[1892] On a case-by-case basis, not only executive employees, but those who have an outstanding importance in the functioning of the employer or who occupy a position of trust might be concerned as well.[1893] Regarding the content of the behaviour, one picture taken in a bar seems to be tolerable, while a video showing an employee in a nearly unconscious drunken state might be proven problematic.

The criteria set for the case of behaviour having a direct connection with the employment (e.g. identifiability of the employer) can accordingly play a guiding role in the case of not having a direct connection. In addition, with regard to the lack of public function, limiting employees' behaviour and expression must be an exceptional measure. Its application might depend on the *position* of the employee, and should not be broadly interpreted.[1894]

(B) Freedom of expression

In relation to Subsection (3), the reasoning of the HLC clearly states that the employees' freedom of expression cannot be restricted if the opinion is not connected to the employment.[1895] I understand these provisions, according to which the employees' expression cannot be restricted on the grounds of Subsection (3), however, in the light of Subsection (2) such an expression might be capable of directly and factually damaging the employer's reputation, legitimate economic interest or the intended purpose of the employment relationship. (In extreme cases) expression on SNSs can fall under Subsection (2). For example, it is enough to think of cases relating to the promotion of Nazi propaganda or racist comments.

Even though they did not reach courts, certain cases were publicized: in 2013, a journalist was dismissed for an offensive comment, blaming the victim of a rape,[1896] while in 2016 another journalist was dismissed for posting an excessive comment in a case related to sexual abuse.[1897] Although the following two cases are not from the private sector, they are worth mentioning in order to portray the growing topicality of the subject: in 2015 investigations were initiated against a primary school teacher who used her Facebook profile to inform parents and at the same time to share anti-Semitic posts.[1898] The second case relates to the

---

[1891] Subsection (1) of Section 208 of the HLC: "*'Executive employee' shall mean the employer's director, and any other person under his or her direct supervision and authorized – in part or in whole – to act as the director's deputy.*"

[1892] For example, different behaviour is expected from a secretary or from a CEO.

[1893] Pók 2012a. p. 163.

[1894] For example, to cases when the employee is shown during an illegal activity (e.g. consuming drugs or violating other rules) or in a state of excessive consumption of alcohol.

[1895] *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről*, 2011. p. 99.

[1896] https://hvg.hu/itthon/20130727_blikk_kirugas (Accessed: 22 November 2018)

[1897] https://nepszava.hu/1090759_kirugtak-facebook-posztja-miatt-aczel-endret (Accessed: 15 November 2018)

[1898] *Kúria tájékoztatója a Kúria M.I. tanácsa által tárgyaláson kívül elbírált Mfv.I.10.098/2019. számú ügyről.* 2019. The Curia held that it is incompatible with the profession of teacher to post on a Facebook profile racist, exclusionary or extreme content. In its reasoning the court drew attention to the specific responsibilities teachers have, and their effects on teachers' expected behaviour outside the workplace. As teachers have increased responsibility in educating children, these expectations are higher towards them than towards a private sector employee.

chancellor of a Hungarian university (the second highest position at the university), who posted a picture to Facebook – in a period when the whole Hungarian media was reporting about refugees arriving – in which there were 14 naked women in a boat. In the picture it was written: "finally, welcome refugees!" On his profile, the chancellor identified that he worked at the University and (more seriously) his profile picture was the logo of the University. The case resulted in a public outcry. The chancellor claimed he was not the author of the content but was a victim of a cyber-attack and finally gave in his resignation in order to spare the University from more humiliation.[1899]

In conclusion, different factors should be considered to determine whether the employees' expression not directly relating to the employment damaged/jeopardized the employer's reputation or legitimate economic interest. As in private employment employees do not have a public function, limiting their expressions (or sanctioning them) must relate to exceptional cases. First of all, the *subject* of the expression should be examined: expressions relating to subjects judged by public perceptions (e.g. promoting Nazi propaganda, hate speeches) might become subjects of such restrictions. The *style* can also play a role: the use of excessive expressions (potentially constituting slander or defamation) or expressions representing heated feelings such as aggression or hate[1900] might make the expression lose the protection. Finally, the *position* of the employee is important, as greater care is required from employees working in higher positions with increased responsibility. From among the above, these are the elements that should be analysed during the assessment of the expression in a given case.

To *conclude Chapter 1.*, while employees' freedom of expression or behaviour outside working hours is already regulated both in France and in Hungary, SNSs put these already existing conducts into new perspective, through being platforms where employees often express themselves in an abusive and excessive way, possibly to a wide audience, with the increased possibility to identify the employer. This is true both in the case of expression/behaviour with a direct connection to the workplace and in the case of expression/behaviour with an indirect connection to the workplace.

While both in France and in Hungary the employee has the right to express himself/herself, even including the expression of a negative opinion towards the employer, this expression cannot constitute an abuse. In the case of an activity indirectly having a connection with the employment relationship, even stricter conditions must be met, as the activity is more closely connected to the personal life of the employee. Throughout Chapter 1 different criteria were identified (position of the employee, nature of the expression, public or private nature, etc.), which can help establish whether the employee overstepped the limits of his/her freedom of action granted by the relevant regulations.

[1899] https://index.hu/belfold/2015/09/28/lemondott_devecz_miklos_a_szegedi_egyetem_kancellarja/ (Accessed: 3 May 2018)

[1900] See, for example, the already mentioned case of *Justin Hutchings*. http://rabble.ca/columnists/2012/10/employees-beware-perils-posting-facebook (Accessed: 11 May 2018)
Or, see the case of an intern at a car factory who commented a picture in which firefighters sprinkled Syrian children with water in the summer heat. It was obvious from the picture that the children were having a good time. However, the intern commented that instead of water, a flamethrower would have been a better option. The employer was identifiable from the intern's Facebook profile, and outraged users reported the comment to the employer – who in response terminated the internship. http://munkajogportal.hu/felmondhatunk-a-munkavallalonak-egy-facebook-bejegyzes-miatt/ (Accessed: 27 May 2017)

Chapter 2: Regulating and monitoring employees' presence on SNSs

In addition to determining the boundaries of employees' personal life when it comes to off-duty conduct and social media, *Section 1* will examine this question from the employer's perspective: namely, how exactly monitoring and imposing restrictions on employees' behaviour can and should take place. In this regard, the employer's role and responsibility are crucial, as within a specific workplace he/she is the key actor when it comes to planning the conditions of monitoring and defining the limits of how employees should behave while using SNSs.

However, challenges relating to the use of SNSs go beyond the workplace, therefore, it is not only the employer's task to solve the uncertainties and to prompt employees to adopt a more responsible conduct through drafting and implementing an internal social media policy. Rather, it is a complex matter, where the interaction of different actors in different fields is required – as it will be seen in *Section 2*. Outside the workplace, technological solutions and awareness raising can contribute to a more conscious use of SNSs (not only by employees but also by users in general), which in my opinion can highly contribute to preventing arising challenges with respect to the misconceptions surrounding the public-private nature and the general functioning of SNSs.

Section 1. What can employers do?

Employers' roles are crucial, as within the framework of the legal regulations, they can determine the exact behavioural requirements that employees must comply with, and they can also take a huge responsibility in raising awareness among employees. Under Section 1, it will be discussed what legal rules employers must respect during the monitoring and the regulation of employees' online activities. While assessing whether SNSs are of public or private nature, the privacy approach was dominant, when it comes to *how* the monitoring of employees' behaviour is possible, a data protection approach provides more answers. First, *(§1)* it will be examined whether the employer can completely prohibit the use of SNSs – with regard to the increased harm employees can cause, then *(§2)* it will be addressed what rules must be respected during monitoring employees' online activities.

§1 Prohibiting the use of SNS?

In relation to employee monitoring usually the employees' more vulnerable position is mentioned, in contrast to the employer abusing his/her powers in monitoring employees (playing a local Big Brother by installing cameras everywhere, monitoring every keystroke employees make, recording every meter they drive in the company car, etc.). *Gábor Mélypataki* and *Zoltán Rácz* argued that although the employee can jeopardize the employer's legitimate interests through off-duty SNS behaviour, it is still the employee who is in the more vulnerable position.[1901] However, other authors argue – in my opinion, correctly – in favour of the existence of reversed vulnerability between the parties. *Edit Kajtár* argued

[1901] Mélypataki – Rácz 2018. p. 683.

that in contrast to these premises, when it comes to using SNSs, tables have turned, and it is the employer who is in need of an increased protection against employees' wrongful conduct.[1902] The development of ICT has a huge impact on enforcing the employer's rights and legitimate interests,[1903] resulting in the reversed vulnerability of the employer.[1904] In the social media era it is true that it has never been easier for a few persons to cause huge damage to the employer's fragile reputation. On SNSs an ill-intentioned content – that is extremely easy to publish, only Internet connection and a few minutes are needed – can rapidly go viral, causing damage, which a simple employee could not easily do in the pre-Facebook age.[1905] This "new" vulnerability has to be taken into consideration when establishing the balance between the employees' and the employer's rights.

From the employer's perspective, the most straightforward solution might seem to be the prohibition of the use of SNSs, preventing all the possible challenges. However, from a legal point of view,[1906] even taking into account the employer's increased vulnerability, this solution would raise several problems.

According to the former *UN's Special Rapporteur* on the promotion and protection of the right to freedom of opinion and expression, "*[t]he Internet has become one of the most important vehicles by which individuals exercise their right to freedom of opinion and expression, and it can play an important role to promote human rights, democratic participation, accountability, transparency and economic development. […]*"[1907] Access to the Internet does not only comprise exercising freedom of expression, but is also a means to exercise other rights, such as the right to education, the right to freedom of association, the right to full participation in social, cultural and political life and the right to social and economic development.[1908] As SNSs are an important part of everyday life, the UN Special Rapporteur's words apply to their case as well. SNSs are more than simply a way of entertainment; they are important platforms of self-expression and communication. Besides, they also represent a way of collecting information, as they are one of the main platforms of learning about events of not only friends and acquaintances, but also of the world. Completely prohibiting employees to use them would constitute a very extreme measure, especially considering that they do not even hold public functions.[1909] *Proskauer Rose LLP*, in its third annual global survey about social media use analysing the jurisdiction of sixteen countries from all over the world,[1910] concluded that in none of the examined jurisdictions did the employer have the right to prohibit the use of social media *per se*.[1911]

As it was already discussed, both the FLC and the HLC require proportionality when it comes to restricting employees' rights – and although there exists no explicit right to social media, given its role in the 21st century, completely prohibiting their use seems

---

[1902] Kajtár 2015. p. 199.
[1903] Majtényi 2006. p. 333.
[1904] Balogh et al. 2012. pp. 96–97.
[1905] Ray 2010a. p. 10. and Ray 2018. p. 11.
[1906] Also, from a practical point of view, such a prohibition might only lead to the creation of profiles under fake names or pseudonyms.
[1907] La Rue 2011. par. 78.
[1908] La Rue 2011. par. 61.
[1909] Pók 2012a. p. 161.
[1910] The jurisdictions covered were Argentina, Brazil, Canada, China, Denmark, France, Germany, Hong Kong, India, Ireland, Italy, Japan, Spain, The Netherlands, the United Kingdom and the United States.
[1911] Proskauer Rose LLP 2014. p. 10.

to constitute a disproportionate limitation of the employees' right to privacy. As regards France, *Jean-Emmanuel Ray* expressed that prohibiting the use of SNSs from the employees' home seems to be problematic.[1912] In Hungary, *Edit Kajtár* reached the same conclusion, stating that completely prohibiting employees from using social media would be extremely disproportionate.[1913] Although limited to the expression of employees, *Márton Leó Zaccaria* likewise held that completely prohibiting the employee from expressing his/her opinion on SNSs would not be acceptable.[1914] Based on the above views, the monograph is of the opinion that in accordance with the requirements laid down in national regulations, complete prohibition is not possible;[1915] instead, the employer should only *restrict* the use of SNSs – the increased harm possibly caused by employees should be taken into consideration when determining the limits of such restriction. As a result, the employer is entitled to impose limitations on employees' conduct on SNSs – its suggested limits will be addressed in Section 2.

§2 Employee monitoring and data protection

When it comes to determining in detail the employer's available means in relation to controlling off-duty conduct on SNSs, in addition to the privacy approach (namely the public or private nature of these platforms), the assessment from a data protection point of view is needed in order to ensure the protection of employees' rights. First, parallel to the private-public nature of SNSs, as a preliminary question it should be assessed whether the systematic monitoring of these platforms is possible. Then, as the employer has several ways to access data, it should be examined *(A)* what ways of access are considered to be lawful. Finally, *(B)* the specific challenges relating to the enforcement of data protection requirements will be addressed.

In addition to the privacy approach (the assessment of the public or private nature of SNSs), the matter can also be viewed from a *data protection* angle, meaning that it should be examined whether it is possible for the employer to systematically monitor[1916] the employees' online behaviour and presence. As it was already established, although usually it is the individual who decides to share the content on his/her profile, even if it is done without the use of the privacy settings, it does not mean that the employer can process the personal data in any way he/she wishes, without any limitations. The data protection requirements still have to be respected.[1917]

In *France*, the monitoring of the publicly available information is possible.[1918] If the employer monitors such a public content, the violation of the employee's right to respect

---

[1912] Ray 2011. pp. 138–139.

[1913] Kajtár 2016. p. 174.

[1914] Zaccaria 2016. p. 16.

[1915] Except for a very few cases – e.g. for individuals working in high positions in the military, in national security, etc.

[1916] In practice, usually three scenarios are employed: 1) no monitoring at all, 2) *ad hoc* monitoring (e.g. when managers and employees are connected on an SNS), 3) systematic, well-planned monitoring. https://allpryme.com/employee-privacy-laws/employee-privacy-laws/ (Accessed: 14 August 2019)

[1917] Fel – Sordet 2010. p. 22.; NAIH/2016/4386/2/V.

[1918] Griguer 2010. p. 64.

for private life is not raised,[1919] as it was the employee himself/herself who chose to publish the given content. However, it does not mean that such a control is exempt from legal requirements: data protection requirements, such as prior information, purpose limitation, proportionality, necessity, data quality, etc. are still going to be applicable.[1920]

As it was already pointed out, in *Hungary*, *László Pók* argued that as it would be hard not to qualify employees' behaviour outside of working hours as pertaining to their personal life, in the light of the HLC's provision on prohibiting the monitoring of employees' private lives, it is hardly acceptable to monitor employees' activity (beyond working hours, by using their own devices) on SNSs. This would leave the employer the possibility to discover the employee's expression only incidentally.[1921] However, *Edit Kajtár* – in my opinion, correctly – argues that on the one hand, the HLC states that the employee can only be monitored to the extent pertaining to the employment relationship (and not during working hours). Therefore, if there is a connection between SNS use and the employment relationship, the monitoring *per se* is not forbidden. On the other hand, she also interprets the HLC as it only forbids to violate employees' private life and does not forbid it to be the subject of monitoring.[1922] Therefore, the systematic monitoring of the employee's SNS activities is legitimate, provided that the employer respects other (data protection) requirements.[1923]

(A) Access

In practice, employers have several ways to access or to gain knowledge of employees' off-duty SNS conduct. It was already asserted that employers are allowed to consult the publicly available content posted by the employee. Even though this is the most obvious way of gaining access due to the lack of the use of privacy settings, other scenarios must also be examined, such as using schemes, friending an employee, and the case of receiving screenshots.

Besides constituting an intrusion into the employee's personal life, the use of *schemes* would also be contrary to the data protection principle of fair processing. The employer cannot use schemes in order to obtain access to the content the employee shared. For example, a colleague cannot be asked to send a friend request to an employee in order to be able to provide screenshots in the case of the publication of a "suspicious" content.[1924] It is also forbidden for the employer to ask another employee, member in a closed group, to report on the activity of other employees[1925] or to use a pseudonym in order to trick the employee into accepting a friend request.[1926] Creating a modern-day "snitch regime" through encouraging the employees to report on each other's online activities would be unlawful according to *Gábor Mélypataki* and *Zoltán Rácz*.[1927] This is in line with the data protection requirements, such as the fairness and the transparency of processing.

[1919] Fel – Sordet 2010. p. 22.
[1920] Caprioli 2012. p. 39.
[1921] Pók 2012a. p. 164.
[1922] Kajtár 2015. p. 203.
[1923] Rácz 2015. p. 285.
[1924] Ray 2018. p. 11.
[1925] NAIH 2016. p. 19.
[1926] Le Clainche 2012. p. 48.
[1927] Mélypataki – Rácz 2018. p. 682.

In contrast to using a pseudonym or fake name when *sending a friend request*, friending an employee while using the employer's real name might reveal different issues. According to *Julien Le Clainche*, if the employer makes part of a "careless employee's" contact list, the employer having access to the disparaging remarks would be considered lawful.[1928] Nevertheless, according to my opinion, the picture is more nuanced, especially when the employer sends a friend request to an employee.[1929] Although it is true that in this scenario the employer does not apply any schemes, the voluntary nature of consenting to letting the employer access this online profile reserved for friends (because if it were set to public, the employer would not need to send a request) can be highly questionable.[1930] Can an employee decline such a request without fearing the possible consequences?[1931]

As a reference, the CoE's and the WP29's already presented documents should be recalled. According to the *CoE's 2015 Recommendation*,[1932] "*[e]mployers should refrain from requiring or asking an employee […] access to information that he or she shares with others online, notably through social networking.*" The explanatory memorandum states that when an employee decides to restrict access to his/her account, his/her will should be respected, and employers do not have the right to ask for access to the profile.[1933], [1934] Although the explanatory memorandum refers to the example of the employer asking for login credentials, sending a friend request to an employee – even if it is far from being as serious as an employer asking for username and password – constitutes requiring access to information as well. Such an interpretation is consistent with the *WP29*'s viewpoint, which noted that "*[t]here is no legal ground for an employer to require potential employees to 'friend' the potential employer, or in other ways provide access to the contents of their profiles*."[1935] Although this provision refers to prospective employees, by analogy it is adequately applicable to the case of employees as well, meaning that the employer should refrain from friending employees.

In the presented French cases, it was quite frequent that the employer became aware of the disparaging remarks through another employee who had access to them and decided to let the employer know as well, typically by providing *screenshots*.[1936] The *employment tribunal of Boulogne-Billancourt* held that such a practice does not violate the employee's

---

[1928] Le Clainche 2012. p. 48.

[1929] In the case when the employee initiates the act, in my opinion, no special legal challenges arise from a legal view.

[1930] However, in contrast to this opinion, *Jean-Emmanuel Ray* notes that it is exceptional that an employee accepts a friend request coming from the employer. Source: Ray 2013. p. 18.

[1931] Although as certain sites, such as Facebook, enable users to apply customized privacy settings, the employee could grant a very limited access to the employer without the latter realizing that he/she is among the "acquaintances" – therefore the employee can have his/her cake and eat it. However, this is not a satisfying solution, as in the case of SNSs with all or nothing privacy settings (e.g. Instagram), the employee cannot have recourse to this solution.

[1932] CoE: *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 2015

[1933] CoE 2015. par. 46.

[1934] The explanatory memorandum also recalls that employers should not obtain access to employees' profile without their knowledge, using an intermediary, or using a fake name or a pseudonym. par. 45.

[1935] WP29: *Opinion 2/2017*. p. 11.

[1936] For example, this was the case in: CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343; CA Rouen, 26 avril 2016, n°14/03517; Cour de cassation, Civ. 1re, 10 avr. 2013, n°11-19530; Cass. soc., 12 sept. 2018, n°16-11.690

right to respect for private life.[1937] According to the practice previously established by courts,[1938] if an individual who was originally granted access to the content decides to extract the information and to transmit it outside of the restricted access (to the employer in this case), the employer can rely on it as proof.[1939] As it was already presented, the Court of Cassation went against this already established practice in its 2017 decision,[1940] extensively limiting employer's possibilities to obtain proof from SNSs. According to this decision, the employer can obtain proof if he/she is amongst the friends of the employee or if the employee's profile is set to fully public.[1941]

(B) Data protection principles

After determining that the existence of a systematic monitoring system can be legitimate, and the ways of access in which employers can obtain personal data, it is necessary to address the question of the enforcement of other data protection principles. It cannot be emphasized enough that just because the employee made the information freely available by not applying the privacy settings, it does not mean that the general data protection requirements would cease to apply.[1942] In the following paragraphs the specific aspects in relation to monitoring off-duty conduct will be addressed, such as *(a)* purpose limitation, necessity, proportionality, *(b)* prior information and *(c)* data quality.

(a) Purpose limitation, necessity and proportionality

Ensuring the employer's reputation, legitimate economic interests and protection of business secrets and confidential information are *purposes* that can justify the existence of monitoring, as online presence and reputation are of crucial importance in the 21st century and an incriminating post might go viral in an extremely short time. In order to ascertain whether employees' online behaviour infringes these interests, it is *necessary* to monitor their public posts.

Proportionality can be twofold: first, it can relate to the content of the monitoring and second, to the scope of the data processing operations. Regarding the *first* aspect, the employer can decide to look for certain keywords (e.g. the name of the employer) or to monitor the activity of certain employees (e.g. managers).[1943] *Second*, as regards data processing operations, the employer is not empowered to store and analyse information relating to employees' public posts: in the light of the above-mentioned requirements, their

[1937] CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343

[1938] See, for example: CA Rouen, 26 avril 2016, n° 14/03517; CA Paris, Pôle 6, chambre 5, 20 septembre 2018, n° 14/04515. The Court of Appeal of Paris adopted a similar position in a case where the remarks were made in a Facebook group, where one of the participants invited the employer. Source: CA Paris, Pôle 6, chambre 9, 3 décembre 2015, n° 15/04533

[1939] Mayoux 2018. p. 24.

[1940] Cass. soc., 20 déc. 2017, n°16-19609

[1941] Mayoux 2018. p. 25.

[1942] Fel – Sordet 2010. p. 22.; NAIH/2016/4386/2/V.
Attila Kun made a similar statement, though in relation to discrimination, that the existence of discrimination cannot be excluded just because the individual shared the personal data. Kun 2013. p. 16.

[1943] However, it is important that the determination of the personal scope of monitoring cannot be arbitrary or discriminative.

storing is only possible if the content is compromising and the employer needs to obtain evidence of such conduct.

(b) Prior information

Both in France and in Hungary, the employer is subject to the obligation of informing employees regarding the limitations of their rights, and the processing of their personal data. In relation to SNSs and off-duty conduct it means that although the employer can monitor the public posts/activity of the employee, employees must be informed of this practice, notably through internal regulations.[1944] This obligation of prior information only applies to cases where the employer decided to systematically monitor employees' online presence in order to verify compliance, and naturally does not apply to cases where a third person (e.g. another employee, client, etc.) informed the employer about the employee's online behaviour.[1945]

(c) Principle of data quality

Data quality issues might arise in relation to the reliability of personal data obtained from SNSs. In a case at the *Court of Appeal of Lyon*,[1946] when the employer learned about the remarks of the employee, he did not provide a bailiff's report, therefore only screenshots provided by other employees were available to support his statement – and the court of appeal held that, in contrast to a bailiff's report, they were not sufficient to support certain allegations of the employer. Copying a conversation might also be insufficient, as courts already ruled that copying and pasting a conversation – instead of a print screen – is insufficient proof, as from them, the accessibility of the account could not be assessed,[1947] suggesting that a print screen might have been considered acceptable. This observation is also in line with the data quality principles.

Not only identifying to whom the remarks relate can be challenging, but also identifying the author of the remarks: the use of pseudonyms, usernames might hide the true identity of the post's author. In a case at the *Court of Appeal of Pau*,[1948] the employee published the remarks to Facebook under a pseudonym. However, the text itself that he published contained enough elements to identify the place of employment, the name of his colleagues, information relating to his private and professional life, and the use of his real first name by other users who reacted to the text.

It is also possible that someone – especially with a common first name and family name – is mistaken for another user having the same name, therefore their online activities might be confused. However, while this might raise more heated issues in relation to recruitment (where the job applicant is an unknown person to the employer), during the course of the employment relationship several clues (e.g. having photos of himself/herself uploaded, indicating the place of employment, having several of other employees amongst his/her

[1944] Griguer 2010. p. 64., NAIH/2016/4386/2/V. and NAIH 2016. p. 19.
[1945] However, following this act he/she has the obligation to inform the employee regarding the further processing.
[1946] CA Lyon, chambre sociale A, 24 mars 2014, n° 13-03463
[1947] Baugard 2015. p. 86.
[1948] CA Pau, chambre sociale, 6 septembre 2018, n° 17/01648

contacts, etc.) can indicate that the user is indeed an employee of the given employer – decreasing the possibility that such data quality questions arise.

In relation to accuracy and reliability, the institution of preliminary interview might be of importance. In *French law*, when an employer considers terminating the employment, he/she must summon the employee to a preliminary interview before taking any decision.[1949] During this preliminary interview, the employer presents the reasons for the proposed decision and listens to the explanations of the employee.[1950] This interview is supposed to serve the protection of the employee, by giving him/her the possibility to provide an explanation to the allegations. Theoretically, such an interview could contribute to the effective enforcement of the data quality principles. However, in my opinion the cases where the data quality principles might be threatened regarding off-duty conducts and SNSs are very limited in practice. Such extreme cases might include hacking the employee's account (therefore he/she is not the author of the compromising content) or mistaking someone else's online activity for the employee's (e.g. through bearing the same name). A difference between the two countries is that in *Hungarian labour law* currently there is no such interview where the employee could explain himself/herself. However, as regards the rarity of the mentioned cases, such a preliminary interview *in itself* would not represent a solution to the arising challenges.

In conclusion, with regard to the importance of SNSs nowadays, a *complete prohibition* of their use outside the workplace does not seem legally acceptable. However, as employees are bound by certain obligations outside the workplace, their use of SNSs can be *restricted* in accordance with the labour law and data protection requirements. Such a restriction is always dependent on the given circumstances, such as the position of the employee or the nature of the workplace, also the assessment of the activity must be based on a case-by-case basis. The employer has the right to monitor employees' activity on SNSs and whether they have complied with restrictions. However, during such a monitoring, data protection requirements must be respected. Notably regarding access, the employer can only process personal data that was publicly available (either for every Internet user or for every user of the given SNS) or that he/she has become aware of through another employee/user who voluntarily decided to share the given information with the employer. Prior information must also be given to employees, and efforts should be made to avoid possible issues arising with respect to the enforcement of the principle of data quality.

Section 2. Best practices and recommendations

Section 2 will enumerate what steps and measures can be taken in order to find a balance between the rights of the two parties and to avoid the emergence of issues related to the use of SNSs outside the workplace. First, *(§1)* it will address what can be done within the workplace, aiming to examine the measures that might be adopted by employers. Then *(§2)* it will discuss what other factors can play a role beyond the workplace.

[1949] Paragraph 1 of Article L1232-2 of the FLC
[1950] Article L1232-3 of the FLC

§1. Inside the workplace

As every workplace is different, it is impossible to provide a universal regulation applicable to all enterprises. Therefore, providing rules at the level of the workplace is crucial. For example, the employer can provide trainings or distribute informational materials in order to remind employees of their obligations and of the restrictions relating to their online behaviour. However, it is a more common solution to adopt social media policies – which will be presented in the following paragraphs.

(A) Adopting internal social media policies

In accordance with what was already stated in relation to internal social media policies regarding the use of SNSs during working hours, internal social media policies can constitute an effective way to clarify what behaviour employees can adopt *on* SNSs. Through laying down the good examples and the forbidden use of SNSs, such an internal policy can often be an effective way to prevent employees from abusing their freedom of expression.[1951] When it comes to determining the content of such a policy,[1952] it must be emphasized that it is not possible to draft a universal policy that could be applicable at every employer without changes. Due to the diversity of legal relationships, job descriptions and workplaces, what might be tolerable at one workplace might violate the reputation at another. During the drafting of such a document several factors shall be taken into consideration (e.g. the type of the workplace, its size, its place, etc.). Those stated here represent a point of reference, but they must be adjusted to the characteristics of the given workplace, such as the workplace environment, the nature of the work, level of employees' education, etc. There exists no one-size-fits-all solution.

Despite its advantages, in *Hungary* it is not a common practice for employers to adopt such documents.[1953] However, with the growing number of employees (allegedly) abusing their rights, more and more employers might tend toward adopting an internal social media policy. One particular case happened within the National Ambulance Service, where an internal social media policy was created in response to paramedics taking pictures of unconscious patients and commenting them on Facebook.[1954] Other employers also started to regulate these matters through adopting different measures.[1955] In the absence of case law

---

[1951] Griguer 2010. p. 64.; Pók 2012. p. 15.

[1952] The present part is highly based on the results of a research project conducted by *József Hajdú*, *Adrienn Lukács*, *Viktória Lechner* and *Attila Turi* between 2016–2017 entitled "*Data protection challenges arising during the use of social network sites in the context of employment*" ("A közösségi oldalak használata során felmerülő adatvédelmi jogi problémák a munkajog kontextusában") financed by the Ministry of Justice of Hungary. (In the meantime the research was supplemented as it progressed.) In the frame of the research, several internal social media policies were analysed in order to establish the best practices that can be drawn from them.

In the research the following social media policies were analysed: Canada: Via Rail Canada, Red Cross; USA: Department of the Interior, Food and Drug Administration; Australia: Equestrian Australia, Volleyball Australia, National Library of Australia; UK: BBC; France: IUT de Rennes, Orange; Global: DELL, NVIDIA.

[1953] Klausz 2013. p. 144.; Rácz 2015. p. 295.

[1954] https://www.hrportal.hu/c/facebook-szabalyzat-a-mentoknel-van-apropoja-20120116.html (Accessed: 15 November 2018)

[1955] https://ado.hu/munkaugyek/facebook-szabalyzat-beleszolhat-a-munkaltato/ (Accessed: 15 November 2018)

it is the employer's duty, and therefore it plays a gap-filling role, to draft and consistently implement internal social media policies in order to provide guidance to employees on the use of SNSs.[1956]

While keeping in mind the impossibility of creating uniform policies applicable to every workplace, the following paragraphs will aim to draw attention to the most important elements of such a policy. It is recommended that employers include the following parts: the aim of the policy, fundamental definitions, scope, common rules of conduct, examples of conducts to be followed or avoided, monitoring of compliance (data protection), sanctions and references.

(B) Recommended content of the policy

Within this part, it is recommended that the employer declares the overall *aim* that he/she wants to reach by adopting the policy and to raise attention to the arising legal (privacy and data protection) challenges. In this part the employer could state that the policy's aim is to determine the conditions and requirements that employees shall respect during the use of SNSs. The policy's main aim is to establish a balance between the employer's rights and legitimate interests and the employees' right, through determining the boundaries of the employees' freedom of expression. The employer should emphasize that although in this scenario employees use SNSs outside the workplace, beyond working hours, from their own equipment, they are still bound by labour law regulation, meaning that they cannot say anything on these forums without facing the possible legal consequences for their employment relationship. Therefore, employees should use SNSs in a way that does not infringe the employer's or other users' rights.

When it comes to *definitions*, it is recommended to provide a general definition of social media and SNSs, to provide certain examples of the most commonly used platforms – as the exhaustive enumeration of existing SNSs is not possible. It is also advisable to remind employees that any kind of content can constitute an infringement: not only texts (e.g. post, comment), but also photos or videos.[1957]

In policies, differentiation should be made between official and non-official use. *Official use* (professional use) is when the employee either handles the official account of the workplace or acts as the official representative of the employer. Only those employees can act as such who were pre-authorized to do so. *Non-official use* (personal use) occurs when the employee uses his/her own profile as a private person (or as an employee), and not as the representative of the employer. Such a use can relate to matters connected to the workplace (e.g. expressing opinion in relation to professional questions, often as an employee of the given workplace) or to matters completely independent of the workplace.

The employer should define the scope of the policy. Regarding the *personal scope*, the employer should clearly state which employees (every employee, a group of them, etc.) the policy is applicable to. Amongst the *material scope*, it is advisable to differentiate between official and non-official use of SNSs and state that the present policy aims to

---

[1956] https://jogaszvilag.hu/szakma/a-kozossegi-media-hasznalata-munkaltatoi-szemmel/ (Accessed: 6 September 2018)

[1957] *Social Media Policy*. http://www.equestrian.org.au/sites/default/files/Social%20Media%20Policy.pdf (Accessed: 19 March 2017) p. 3.

regulate questions relating to non-official use. As non-official use raises the question of the boundaries of professional and personal life, this matter will be examined in detail.[1958] It should also be emphasized that the policy applies to the off-duty use of SNSs (when at first sight no connection is present with the employment, as the employee does not use the employer's device, is outside of the workplace, beyond working hours), while specific provisions aim to regulate the use of SNSs during working hours. Amongst the *temporal scope*, employers should clearly indicate when the policy was adopted, and if it was updated, when it occurred.

In addition to laying down the explicit rules and the restrictions applying to employees, internal regulations should also serve as a *guidance* as regards responsible use of SNSs.[1959] The policy can constitute a good way to raise awareness amongst employees regarding their responsibilities while using SNSs.[1960] It is important to emphasize that SNSs are not *terra nullius*, and their use is subjected to the legal requirements. Employees should be made aware that nowadays the boundaries of work and personal life are blurred, and social media does not constitute an exception from this phenomenon. Therefore, the employee must respect the employer's legitimate interests even while using SNSs in the course of his/her personal life. This means that employees can register and use these sites, they can express their opinion, however they are not completely free to post anything without any restriction:[1961] obligations arising from the employment contract are binding in the case of SNSs as well. But how exactly can an employee express his/her opinion on SNSs? It is important to emphasize that employees have the right to express themselves in matters relating to the workplace, but they have to respect their other obligations (e.g. duty of loyalty) arising from the employment relationship. Therefore, the employer can restrict employees' behaviour on SNSs, but this restriction cannot be limitless (e.g. the employer can prohibit the infringement of his/her reputation, but he cannot state that the employee is not allowed to criticise the employer at all).[1962] The boundaries of these restrictions are going to be further addressed in the part "examples". It is even recommended that the employer provides an indicative list, determining which conducts in general are factually capable of damaging or jeopardizing the employer's legitimate interests.[1963]

Employees should also be reminded of general conducts to be adopted while using SNSs. Such conducts would include staying courteous and polite while using SNSs,[1964] or being honest and accurate.[1965] They should also be aware that in extreme cases, non-appropriate

---

[1958] In contrast, while official use should also be regulated, it does not raise specific privacy/data protection challenges, as such a use is basically part of the work.

[1959] Németh 2013. p. 98.

[1960] Fel – Sordet 2010. p. 22.

[1961] See, for example: *Social Media Policy*. 2010. Available at: https://edit.doi.gov/sites/doi.gov/files/migrated/notices/upload/DOI-Social-Media-Policy-Final-Redacted.pdf (Accessed: 19 March 2017) p. 4.; *Volleyball Australia Social Media Policy.* 2012. Available at: http://www.volleyballaustralia.org.au/_literature_152757/Social_Media_Policy (Accessed: 19 March 2017) p. 2.

[1962] *Social Media Policy*. Available at: http://www.nvidia.co.uk/object/social-media-guidelines-uk.html (Accessed: 23 March 2017)

[1963] Rácz 2015. p. 301.

[1964] *Social Media Guidelines*. Available at: https://www.orange.com/sirius/smg/FR_Guides_Medias_Sociaux.pdf (Accessed: 22 March 2017)

[1965] See Walmart's social media policy, which by the way was considered as a perfect policy by the National Labor Relations Board in the US in 2012. The policy is available on the last three pages of the report of Lafe E. Solomon, general counsel: Solomon 2012

use of SNSs can be qualified as a punishable act according to penal law regulation (e.g. libel, defamation).

It is also recommended that attention is drawn to the basic functioning of SNSs. Employees should be reminded that SNSs are essentially public forums, and a content might easily become available to a larger audience than originally intended by the employee. Therefore, the use of privacy settings is highly recommended. In the meantime, even when such settings are applied, caution should still be exercised, as it is still possible that the content will become available to a larger audience. Amongst other challenges, on the Internet the perception of anonymity might be deceiving, information can be easily misinterpreted as it can be taken out of its context and the Internet does not forget. For these reasons, it is strongly recommended that employees think over what they post to these sites, and they should keep in mind that they should only post content that they would feel comfortable with if it was broadcasted in the news, told to his/her mother or transferred to his/her supervisor.[1966]

In order to be truly helpful, SNS policies should provide concrete *examples* telling employees what they can and what they cannot do, providing real substance to the above-presented common rules of conducts (e.g. in what forms the employee can express his/her opinion, the use of what expressions indicates the existence of an abuse, etc.). As such, it can contribute to making employees understand exactly what expectations the employer has towards them when using SNSs.

During the use of SNSs employees should not suggest that they act as the representative of the employer. Therefore, the configuration (e.g. registering with the work e-mail address, using the logo of the employer, identifying the employer, etc.) of the user profile has key importance.[1967] In order to achieve this separation of professional and personal life, employers can prohibit registering to SNSs using the professional e-mail address, or referring to the workplace or to the position of the employee in the user name or in the name. Regarding the use of the company's logo: the employer can completely prohibit its use, and it is especially recommended to prohibit its use as profile or cover picture. However, indicating amongst the biographic data that the employee works at the given company should be allowed.

In order to prevent any confusion between official and non-official use, several policies suggested using a disclaimer indicating that the employee's remark does not reflect the employer's position.[1968] However, the effectiveness of such a disclaimer is debated, as it might just draw unnecessary attention to the identity of the employer.[1969]

Even when the employee does not reveal the identity of his/her employer in the biographic information, there is no guarantee that this information will stay concealed. A comment originating from another user, or a simple Google search might easily reveal the

---

[1966] See, for example: Canadian Red Cross (no date) *Social Media Guidelines for Canadian Red Cross Staff and Volunteers*. Available at: http://www.redcross.ca/crc/documents/What-We-Do/Violence-Bullying/partners/social-media-guidelines-2013.pdf (Accessed: 19 March 2017) p. 3., 4., 5. and DELL (no date) Global Social Media Policy. Available at: http://www.dell.com/learn/uk/en/ukcorp1/corp-comm/social-media-policy?c=uk&l=en&s=corp (Accessed: 23 March 2017)

[1967] IUT de Rennes (no date) *Charte d'utilisation des réseaux/médias sociaux numériques IUT de Rennes*. Available at: http://partages.univ-rennes1.fr/files/partages/Services/IUT_administration/Internet/doc/IUTrennesCharteRSN.pdf (Accessed: 21 March 2017) pp. 3-4. and Orange (no date) Social Media Guidelines. Available at: https://www.orange.com/sirius/smg/FR_Guides_Medias_Sociaux.pdf (Accessed: 22 March 2017)

[1968] Walmart's policy in: Solomon 2012

[1969] Kajtár 2015. p. 211.

identity of the user's employer. Therefore, during any use of SNSs, against any other user, employees should respect the other users' dignity and should not use excessive, insulting or defamatory expressions: employees should refrain themselves from committing libel or defamation, or inciting hatred. The publication of vulgar, humiliating jokes or content should be avoided. It is also forbidden to harass or attack competitors (e.g. through sending SPAM). Employees should publish an appropriate and respectful content, while staying honest and accurate. The publishing of misinformation should be quickly corrected.[1970]

In addition to these general requirements, employees should respect the employer's reputation and cannot publish content that violates the reputation. The employee can still express his/her opinion (even if it is a negative one), however, it cannot constitute abuse or be seriously detrimental to or threaten the good reputation, legitimate economic and organizational interests of the employer. The position of the employee is also important: the higher the position occupied is, the more loyal the employee should be. The use of language has key importance, vulgar, insulting, excessive expressions should be avoided, and the opinion should be of a neutral nature (even though it can even criticise the employer).

The employee should respect the employer's business secrets: confidential information cannot be shared on these sites. The same goes for the personal data of clients, sharing information relating to upcoming products, etc.

Besides regulating employees' conducts, employers can also *monitor compliance* with the rules set by the policy. However – in accordance with the general requirement of transparency laid down both by data protection and labour law regulations –, if the IT section starts to systematically monitor employees' online publicly available actions, they must be informed of these measures prior to the monitoring. It cannot be stressed enough that the employer can only monitor the *public* posts/activity of the employee (without using any schemes in order to gain access). Also, the requirement of prior information persists in spite of the fact that it is the employee who made the content public.[1971]

If the employer opts for monitoring, privacy and data protection matters are separated. If the employer monitors such a public content, the violation of the employee's right to respect for private life is not raised,[1972] as it was the employee himself/herself who chose to publish the given content. However, it does not mean that such a control could be exempt from legal requirements: data protection requirements, such as prior purpose limitation, proportionality, necessity, data quality, etc. are still going to be applicable.[1973]

In the part "*sanctions*" employees' attention should be drawn to the fact that in the case of the non-respect of the regulation what (especially labour law related) legal consequences might be applied (e.g. issuing warnings, or even terminating the employment relationship).

Finally, among *references* it is recommended that the employer refers to the legal basis of the policy (labour code, data protection act, etc.), to the other existing policies (e.g. code of ethics, code of conduct, etc.) and notes where the employee can obtain more information relating to the subject (both within the organisation, for example, from the HR team, and outside of it, for example, from a DPA).

[1970] Walmart policy in: Solomon 2012.
[1971] Griguer 2010. p. 64.
[1972] Fel – Sordet 2010. p. 22.
[1973] Caprioli 2012. p. 39.

§2. Outside the workplace

Albeit regulating and raising awareness internally is a crucial step towards preventing employee misuse of SNSs, other factors external to the workplace can also contribute to achieving this result. First, *(A)* the development of different technological features can empower users to use SNSs in a more privacy-friendly way, while *(B)* educating users at a societal level can contribute to adapting a more conscious attitude towards SNSs.[1974]

(A) Technology

From a technological point of view, *SNS service providers* can contribute to helping to establish the balance between the employer's legitimate interests and the employees' rights through the adoption of built-in privacy and data protection features. Although the documents examined during the research mainly aim to ensure enhanced privacy protection on SNSs in general[1975] and do not focus specifically on challenges related to employment, their findings can be useful in the employment context as well. Here, those elements will be presented that have special significance when it comes to the use of SNSs and off-duty conducts.

Through developing more *customizable privacy settings* (instead of the often used all or nothing approach), users would have the possibility to exercise their right to informational self-determination and carefully determine what audiences can have access to what kind of content. Also, privacy setting should be *by default enabled* (therefore the user should decide *not* to use them, and not the other way around).[1976] In several cases, the remarks were considered to be public because of the lack of use of the privacy settings, so this measure would contribute to decreasing the number of cases when the employee abuses his/her freedom of expression.[1977]

The possibility to use *pseudonyms* is considered to be a way to contribute to better protecting privacy on SNSs.[1978, 1979] Although indeed it is a way to establish more effective privacy protection, it should be emphasized that it does not mean that employees are free or encouraged to state anything while hiding under pseudonyms. Regardless of the chosen username – whether it is the real name of the employee, a fake name, or a pseudonym – the employee's conduct should not overstep the limits of freedom of expression, as the limits

---

[1974] It must be emphasized that these recommendations, such as technological developments and raising awareness/educating users, are crucial not only as regards off-duty conducts and SNSs but are also extremely important during all phases of employment: during the course of hiring and SNS use during working hours. Therefore, the findings of the following paragraphs can adequately be applied to other phases of the employment relationship as well.

[1975] See, for example: 30th International Conference of Data Protection and Privacy Commissioners 2008; CoE: *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*, 2012; WP29: *Opinion 5/2009*; International Working Group on Data Protection in Telecommunications 2008

[1976] WP29: *Opinion 5/2009*. p. 7. and International Working Group on Data Protection inTelecommunications 2008. p. 6.

[1977] Although Article 25 of the GDPR on the requirement of data protection by default is a huge step ahead.

[1978] 30thInternationalConferenceofDataProtectionandPrivacyCommissioners2008;InternationalWorking Group on Data Protection in Telecommunications 2008. p. 4.

[1979] For example, Facebook's Terms of Service states that users must "use the same name that [they] use in everyday life", rejecting the possibility to use pseudonyms.

drawn by labour law are still valid. In this regard, pseudonyms (if they are well-chosen) can contribute to making it more difficult to identify the link between the given content and the employer, through masking the true identity of the author of the content. However, as it could be seen from the case law, even pseudonyms do not guarantee 100 % anonymity, as the identity of the author or of the subject of the remarks can be later identified by third persons (e.g. in a comment).

Jean-Emmanuel Ray points to an application that can contribute to preventing employees from sending compromising e-mails while being under the influence of alcohol.[1980] An application called *Goggles* allows users to practice self-control through verifying that the user indeed possesses his/her mental capacities. During certain previously set periods (e.g. from Saturday 21h to Sunday 13h), if the user wants to send an e-mail, he/she has to solve certain mental calculations, and if the solution is not found during one minute, the e-mail is not going to be sent.[1981] Although this method was established for e-mails and would not prevent employees from exercising freedom of expression in an excessive way, with certain modifications it might contribute to decreasing the number of such remarks. A solution might be the development of an algorithm that would detect when a user posts a content containing excessive, extremely insulting expressions. Then after hitting the post button, a warning message might appear, informing the employee that insulting expressions were detected and asking the user's confirmation that despite the content, he/she still wishes to publish it.[1982]

(B) Raising awareness and educating

Raising awareness has a crucial importance in order to contribute to the promotion of a more conscious SNS use and the prevention of the occurrence of labour law issues related to the use of SNSs. Awareness raising can take place at several levels, such as educating users in general, educating employees or even at the level of the legislator/judges.

It often seems that users (and amongst them, employees) do not even realize that they are not free to post anything to SNSs without bearing the consequences, or what they post to SNSs is not of private nature. When using such platforms, users should be aware of whether the information they share has public or private character and they should be aware of the consequences of choosing to share an information publicly.[1983] Employees

---

[1980] For example, in the already discussed case of Taylor v Somerfield Stores Ltd., the employee posted the "incriminating" video to YouTube after having a few drinks with his colleagues and admitted that he probably would not have uploaded the video if he had been sober. Source: Taylor v Somerfield Stores Ltd. Case no: S/107487/07 Held at Aberdeen on 24 July 2007, par. 11.

[1981] Ray 2009. p. 34.

[1982] A similar idea was raised by *Jay Parikh*, a vice-president of Facebook, in relation to posting children's photos to Facebook. He said the service was considering setting up a system to notify parents who put photographs of children online without restricting their privacy settings. If a parent wanted to accidentally share a picture of his/her child with everyone, the system would notify this person that a child is in the picture, and ask whether he/she truly intended to share it publicly, instead of sending it in a message only destined to the members of the family. https://www.telegraph.co.uk/news/worldnews/europe/france/12179584/French-parents-could-be-jailed-for-posting-childrens-photos-online.html (Accessed: 30 November 2018)

[1983] CoE: *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies)*, 2012. Appendix

should be educated that their acts might abuse their freedom of expression – even outside the workplace and beyond working hours. This could contribute to *preventing* abuses of freedom of expression, as employees would be more aware regarding how social media works and by what legal rules and how they are bound.

Raising awareness is a complex matter, where several actors might have roles. Even though the employer can highly contribute to preventing these issues by laying down the rules to be respected through adopting internal social media policies, awareness raising at a more general, societal level would also be welcomed. This could be realised, for example, with the participation of DPAs[1984] and with different state actions. Finally, as employees are not only passive actors waiting to be saved by DPAs or the state, their role and responsibility has crucial importance as well.

The *state* should take active steps in order to fight against "analphanetism"[1985] and to educate users regarding the challenges of protecting private life in the age of ICT. Younger users' (under 15 years old) "civic-digital" education should be reinforced by raising their awareness relating to intimacy and identity.[1986] Also, informing them on the privacy risks related to Internet use should be part of the education system, while steps should be taken to educate older users as well (e.g. developing online materials).[1987]

The different documents all emphasized[1988] the *SNS provider's* responsibility as regards providing enough information and education to users regarding how they should use these sites, how privacy settings are used, what possible legal consequences SNS can have, how they can delete content, etc. Besides raising awareness, their role is crucial in determining the technical functioning of SNSs, for example, by establishing what types of data protection rules can be applied, whether it is possible to use pseudonyms, etc.

No matter how complex and well-structured a state's educational programme on the Internet and privacy is if *users* do not take steps to ensure their own protection.[1989] Individuals as well should recognize that they have to play an active role in protecting their own privacy in the information society.[1990] The already presented "Grandmother rule"[1991] should also apply in the case of employees, and not only prospective employees. Employees should recognize that SNSs do not always guarantee the desired level of confidentiality, and a content published can become available to a larger audience than originally intended to. As a response to these uncertainties relating to SNSs, *Patrik Polefkó* even suggests users should be a little paranoid, which means they have to keep in mind that on SNSs not everything is as it seems.[1992]

[1984] What was already said in the case of prospective employees in Title 1 should apply accordingly.

[1985] Expression used by Jean-Emmanuel Ray in: Ray 2011. p. 133.

[1986] Türk 2011. p. 148.

[1987] Mendel et al. 2013. pp. 131–132.

[1988] CoE: *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*, 2012. Appendix.; WP29: *Opinion 5/2009*. p. 7.; International Working Group on Data Protection in Telecommunications 2008. p. 5.; ENISA 2007. p. 3.; 30th International Conference of Data Protection and Privacy Commissioners 2008. p. 4.

[1989] Mendel et al. 2013. pp. 131–132.

[1990] Székely 2010. p. 119.

[1991] Byrnside 2008. p. 474.

[1992] Polefkó 2011. p. 109.

According to certain authors, such as for example *Vanessa Nivelles*,[1993] or the *Liga Szakszervezet* (Liga Trade Union),[1994] the best solution would be to refrain from any discussion relating to the workplace. However, according to my opinion, such conduct – although it would indeed eliminate the problem of employees abusing their freedom of expression – would self-restrict employees in a disproportionate way. According to the regulation, it is not forbidden to discuss work related matters or to express opinion in relation to the employment. What is forbidden is to do so in an excessive way. *Ian Byrnside* expresses his similar opinion (although in relation to prospective employees) arguing that job applicants should not erase their SNS profiles, but rather learn how to post according to the nature of these sites and keep in mind the possible consequences.[1995]

However, it is not only employees who need to be educated on the functioning of the Internet and SNSs. It is an additional problem that sometimes even lawmakers or judges are not aware of the functioning of social media and other Internet-based platforms. An illustrative example is Facebook founder and CEO, *Marc Zuckerberg*'s two days of testimony before the US Senate in 2018, following the Cambridge Analytica scandal, where he received certain questions, which demonstrated complete ignorance of the basic functioning of these online services. Such questions included "Is Twitter the same as what you do?" (Twitter is a different platform), "If I'm email — if I'm mailing — emailing within WhatsApp […]" (WhatsApp is a chat messaging system that is not capable of sending e-mails) and "Well, if [there will always be a version of Facebook that is free], how do you sustain a business model in which users don't pay for your service?" (by running ads).[1996]

Judges might not always fully understand the functioning of SNSs. Another example is pointed out by *Marie-Claire Pottecher* and *Zartoshte Bakhtiari*, who brought attention to the judge's observation in a case relating to the use of Twitter during working hours, according to which it takes one minute to make a tweet. However, according to the authors, the judge did not take into account how Twitter works in reality: constructing a tweet requires more time and attention than the one minute that it technically takes to write down 140 characters.[1997] Another example is the already mentioned observation of the Court of Appeal of Pau's,[1998] in which the court referred to the "private and public walls" of the user, applying quite confusing vocabulary, which can hardly be interpreted in the light of the true functioning of Facebook, as every user possess one "wall".

Naturally, in order to be able to adopt up-to-date legislation in the field of ICT or SNSs, it is crucial that lawmakers understand the functioning of these services that they aim to regulate. Also, judges must know and understand the functioning of these sites in order to make judgements correctly. If these actors are not aware of the most basic technical aspects of SNSs, the adoption and the application of laws might become problematic.

In conclusion, in order to successfully address the question of employees' use of SNSs outside the workplace, a complex approach should be adopted, taking measures at several levels: the employer, the state, SNS providers and the individual.

[1993] Nivelles 2014. p. 13.

[1994] https://ado.hu/munkaugyek/facebook-szabalyzat-beleszolhat-a-munkaltato/ (Accessed: 15 November 2018)

[1995] Byrnside 2008. p. 473.

[1996] See the transcript of the hearing at: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.2547f6e741d5 (Accessed: 15 October 2018)

[1997] Pottecher – Bakhtiari 2016. p. 234.

[1998] CA Pau, chambre sociale, 6 septembre 2018, n° 17/01648

As there exists no one-size-fits-all solution, the *employer's* role is of particular importance within the workplace: the employer is the person who – taking into account the specificities of the workplace – can determine what exactly the rules to be followed are. It is recommended that these rules are laid down in internal social media policies, providing detailed guidance for employees and raising awareness among them regarding the use of SNSs and its possible (legal) consequences. Such policies can be means to adopt the general provisions laid down in the FLC and the HLC to the specific requirements of the given workplace.

At a more general level, raising awareness amongst the individuals has key importance, as it can influence or even make them more conscious while engaging in SNSs. The *state* itself can play a huge part by drawing attention to the data protection challenges through its different institutions. Also, the state might even "interfere" earlier through integrating the use of SNSs (and challenges relating to it) into public education courses, from a young age. It is also important that *SNS providers* develop technical features making it possible to effectively enhance privacy/data protection – therefore they determine the whole framework which is later going to be used by individuals. Also, they can play a role by providing general information to the public. Last but not least, the *individual's* role must be taken into account: in the first place, it is the individual who should engage in a responsible use of SNSs. Individuals have the greatest impact on the functioning of SNSs as they fuel these services with their personal data. They choose the content that they post, like or share, decide whether to use the privacy settings – thus are central actors in influencing the possible labour law consequences of their online behaviour.

CONCLUSIONS

Protecting employees' rights, and more precisely their right to privacy and right to data protection is not a new phenomenon: its main rules were already established through addressing the different technological means enabling to monitor employees, such as through applying CCTV surveillance or monitoring the use of the Internet/computer/e-mail/telephone, etc. The detailed rules of such monitoring are already elaborated both at the international[1999] and at the national level.[2000] It was established that employees are entitled to enjoy these rights not only outside, but also inside the workplace – but at the same time, originating from their status of employee, certain obligations continue to impose limits on their behaviour even outside the workplace, beyond working hours.

Neither the right to privacy, nor the right to data protection is an absolute right. As opposed to them, the employer has various rights which can justify their restriction; e.g. right to property, right to reputation, right to the protection of legitimate economic interests – notably manifested in the employer's right to control and right to monitor employees' activities. In the phase of recruitment he/she is entitled to choose with whom he/she would like to contract – in order to assess the capacities of the applicant he/she is entitled to obtain information on the applicant. If privacy and data protection requirements are respected, this can include SNSs as well. In the case of *SNS use at the expense of working hours*, it follows from the obligations and rights of the parties that the employee is obliged to spend working hours performing work, while the employer is legally entitled to expect him/her to do so. In addition, as the person responsible for the organisation of work, the employer has the right to give instructions, define the use of workplace equipment and monitor compliance. When it comes to *off-duty* use of SNSs, the employees' presence on SNSs (through expressing their opinion or engaging in other conducts) can collide with the employer's right to reputation, the protection of business secrets, or with the rules relating to competition.

The real novelty brought by SNSs was that they put the collision of rights into a new perspective, through intensifying it. 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.

[1999] See, for example, the WP29 or the EDPS.

[2000] Notably through the practice of the data protection supervisory authorities; and in France also through courts' case law.

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 behaviour on SNSs), taking relevant international and national regulations into account.

First, it had to be examined: *can the employer control and monitor employees' use of SNSs*? Regarding *monitoring*, the answer is easy: yes, he/she can process publicly available data, but must do it respecting the right to data protection. It means that a legitimate legal ground, a legal purpose must be present, with the respect of data protection principles, etc. The *control* of the use of SNSs did not emerge in the *pre-employment phase*, as in this phase the employer has no right to instruct prospective employees and to determine (or prohibit) the rules on how they can engage in SNSs. *During working hours*, it was established that the employer can regulate the use of SNSs as the employees are contractually obliged to spend their working hours performing work. However, although employees do not have a right to use SNSs in the workplace, they have the right not to be completely cut off from the outside world (e.g. to have the possibility to notify family members or friends in case of an emergency, etc.). Despite this legal possibility, it was recommended that, if possible, the use of SNSs should not be completely prohibited but rather allowed to a determined extent. As regards *employees' activities on SNSs*, it was held that the employer can also impose limitations on their use.

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 boundaries 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.[2001] In contrast, data protection requirements apply regardless the public or private nature of such content. However, due to the invisibility of SNS background checks the enforcement of these requirements is substantially challenged – raising the *raison d'être* of more flexible regulation, instead of a prohibitive one.

It was also discussed whether it should be prohibited to conduct pre-employment SNS background searches in order to better protect applicants' personal lives.[2002] After having examined the existing viewpoints, the monograph adopts the position that due to the the invisibility of such searches, their prohibition would be unreasonable: instead, they should be tolerated and regulated regarding how exactly they should be conducted in order

---

[2001] 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.

[2002] This was the matter where differences were found between the French and Hungarian approach: the NAIH argued that it would not be reasonable to ban the employer from looking at publicly available data on SNSs (even on personal SNSs), while the CNIL argued that the screening of personal SNSs should be prohibited.

to effectively protect applicants' rights. Respecting the data protection requirements[2003] primarily has the purpose of enforcing applicants' rights, but secondarily it also serves the interests of the employer, as non-compliance with these requirements would provide the employer with unreliable data, which may result in sorting out an otherwise perfect applicant and being counterproductive in relation to the aim of finding the best applicant. As a solution, instead of *ad hoc* searches, employers should understand how to screen properly, in order to avoid screening in an inefficient or illegal way.

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 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*. SNS use at the expense of working hours is in most regards similar to the personal use of the Internet and e-mail,[2004] thus raising fewer substantially new questions compared to the other examined fields.

However, SNSs have certain characteristics that must be taken into consideration in contrast to the Internet and e-mail. *First*, as a main rule, the use of SNSs supposes personal activity: as opposed to the Internet and e-mails, which both could serve as a working tool as well as personal entertainment, making it possible to create confusion when distinguishing personal and professional use. However, when a job comes with the use of SNSs, the confusion becomes possible again in the field of communication. *Second*, due to the proliferation of mobile devices, it is quite common that employees own their own device (e.g. smartphones), as well as a mobile Internet connection – which was not such a common phenomenon when the original rules were elaborated. However, even despite these SNS specific challenges, the already established rules are capable of adequately addressing the personal use of SNSs.

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. However,

---

[2003] Challenges related especially to the data protection principles – the most problematic areas were authenticity, accuracy and relevancy of the personal data.

[2004] It was held that SNSs combine the characteristics of the Internet and e-mail: they allow users to search and surf (e.g. looking for a page on Facebook or browsing the news feed), send messages (e.g. Facebook Messenger or Instagram Direct), not to mention that they are *web-based* services. Therefore, the rules established for the monitoring of the employees' use of the Internet and e-mail are essentially applied to SNSs as well.

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. However, the application of data protection principles gave to fewer doubts than in other phases of the employment. In relation to privacy, it must be established where the balance should be found between the protection of the employee's personal life and the employer's rights. The main question to be answered was whether these platforms constitute a private or a public forum,[2005] as although it is not contested that these conducts take place in the course of the employees' personal life, an SNS post can reach an extremely large audience, which excludes the private character of such content.

In the light of the above, different *recommendations* and *proposals* were formulated. They concerned the legal sphere and identified room for further improvement as regards the legal sphere (especially lawmakers, judges and data protection supervisory authorities), the employer (mostly aiming at the adoption of internal policies), technology (encouraging SNS providers to adopt privacy and data protection-friendly technological solutions) and finally the individual himself/herself. A complex approach should be adopted, involving all the actors concerned in order to successfully address challenges posed by SNSs in the employment context.

[2005] French courts, especially after the Social Chamber of the Court of Cassation ruled in the matter, came to the conclusion – according my opinion, correctly –, that as a main rule, SNSs are public platforms unless the user applies strict settings and considerably limits the circle of people who can access the content, both regarding their number and their relationship with each other. Even though in Hungary courts have not (yet) addressed this question, French jurisprudence can serve as an example when it comes to defining the nature of these sites.

BIBLIOGRAPHY – LIST OF LITERATURE AND SOURCES

Adam 2013 = Adam, Patrice: Vie personnelle/vie professionnelle : une distinction en voie de dissolution ? *Le Droit Ouvrier*, (780), 2013. pp. 431–444.

Adam 2015 = Adam, Patrice: SMS, vie privée et portable professionnel : histoire (courte) d'un homme "sans territoire". *Revue droit du travail Dalloz*, (3), 2015. pp. 191–194.

Alleaume 2016 = Alleaume, Christophe: *La notion de droit à la vie privée*. In: Batteur, Annick (ed.): Les grandes décisions du droit des personnes et de la famille. 2nd edn. LGDJ, Issy-les-Moulineaux, 2016. pp. 451–464.

Allix 2014 = Allix, Blandine: L'employeur, le salarié et Facebook', *Feuillet Rapide Social F Lefebvre*. 2014

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

Andriantsimbazovina 2017 = Andriantsimbazovina, Joêl: L'encadrement stricte du contrôle par l'employeur de l'usage de la messagerie électronique du salarié ; Note sous Cour Européenne des Droits de l'Homme, grande Chambre, 5 septembre 2017, Barbulescu c/ Roumanie, numéro 61496/08. *La Gazette du Palais*, (41), 2017. pp. 22–23.

Antonmattei 2002 = Antonmattei, Paul-Henri: NTIC et vie personnelle au travail. *Droit social*, (1), 2002. pp. 37–41.

Antonmattei 2012 = Antonmattei, Paul-Henri: Le licenciement pour trouble objectif. *Droit social*, (1), 2012. pp. 10–13.

Arany-Tóth 2008 = Arany Tóth, Mariann: Gondolatok a munkavállalók személyiségi jogainak védelméről a magyar munkajogban. *Jogtudományi közlöny*, 63(3), 2008. pp. 129–139.

Arany-Tóth 2008a = Arany-Tóth, Mariann: *A munkavállalók személyes adatainak védelme a magyar munkajogban*. Szeged: Bába Kiadó, 2008

Arany-Tóth 2011 = Arany Tóth, Mariann: A munkavállaló emberi méltóságának védelme a munkaviszonyban. *Miskolci jogi szemle*, 6(1), 2011. pp. 135–153.

Arany-Tóth 2016 = Arany-Tóth, Mariann: *Személyes adatok kezelése a munkaviszonyban*. Wolters Kluwer, Budapest, 2016

Arany-Tóth 2019 = Arany Tóth, Mariann: A magánélet védelméhez való jog újraszabályozásának hatása a munkaviszonyban a magánélet védelméről szóló törvény alapján (2. rész). *Munkajog*, (3), 2019. pp. 27–34.

Aubert-Monpeyssen 2007 = Aubert-Monpeyssen, Thérèse: "Trouble objectif dans l'entreprise" et libertés collectives du salarié. *Revue droit du travail Dalloz*, (10), 2007. pp. 586–587.

Ba Sene 2015 = Ba Sene, Fatou: *La protection constitutionnelle de la vie privée et familiale sur les réseaux sociaux en France*. In: Ndior, Valère (ed.): *Droit et réseaux sociaux*. Lextenso (Collection LEJEP), Issy-les-Moulineaux, 2015. pp. 91–100.

Bailleul – Jourdan 2011 = Bailleul, Camille – Jourdan, Dominique: *Contrat de travail: du recrutement à la rupture*. 8th edn. Delmas, Paris, 2011

Balogh et al. 2012 = Balogh, Zsolt György *et al*.: Munkahelyi adatvédelem a gyakorlatban, *Infokommunikáció és Jog*, 9(3), 2012. pp. 95–104.

Balogh et al. 2012a = Balogh, Zsolt György *et al*.: *Privacy in the Workplace*. In: Essays of Faculty of Law University of Pécs: Yearbook of 2012. University of Pécs Faculty of Law, Pécs, 2012. pp. 9–40.

Bankó – Berke – Kiss 2017 = Bankó, Zoltán – Berke, Gyula – Kiss, György: *Kommentár a munka törvénykönyvéhez*. Wolters Kluwer, Budapest, 2017

Bankó – Szőke 2016 = Bankó, Zoltán – Szőke, Gergely László: *Issues of the digital workplace – The situation in Hungary*. JurInfo, Pécs, 2016

Bányai 2016 = Bányai, Edit: *Közösségi média. Közösség vagy média*? Pécsi Tudományegyetem Közgazdaságtudományi Kar, Pécs, 2016

Barbé 2018 = Barbé, Vanessa: *Essentiel du Droit des libertés fondamentales*. Gualino, Issy-les-Moulineaux, 2018

Baugard 2010 = Baugard, Dirk: L'utilité de la Convention européenne des droits de l'homme en droit du travail. *Droit et Patrimoine*, (195), 2010. pp. 34–46.

Baugard 2015 = Baugard, Dirk: *L'usage par les salariés des réseaux sociaux*. In: Ndior, Valère (ed.): Droit et réseaux sociaux. Lextenso (Collection LEJEP), Issy-les-Moulineaux, 2015. pp. 75–89.

Baumhart 2015 = Baumhart, Peter B.: Social Media and the Job Market: How to Reconcile Applicant Privacy with Employer Needs. *University of Michigan Journal of Law Reform*, 48(2), 2015. pp. 503–533.

Befort 1997 = Befort, Stephen F.: Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place. *Hofstra Labor and Employment Law Journal*, 14(2), 1997. pp. 365–422.

Bello 2012 = Bello, Ahmed: Le licenciement pour motif tiré de Facebook : un changement ... dans la continuité. *JCP S (édition sociale)*, (26), 2012. pp. 12–16.

Benalcázar 2003 = Benalcázar, Isabelle: *Droit du travail et nouvelles technologies : collecte des données, Internet, cybersurveillance, télétravail*. Gualino, Paris, Montchrestien, 2003

Berke – Kiss 2014 = Berke, Gyula – Kiss, György (eds): *Kommentár a munka törvénykönyvéhez: kommentár a munka törvénykönyvéről szóló 2012. évi I. törvényhez*. Wolters Kluwer, Budapest, 2014

Berki et al. 2008 = Berki, Katalin *et al*.: *A munka törvénykönyve magyarázata*. 2nd edn. Complex, Budapest, 2008

Beyneix – Rovinski 2016 = Beyneix, Isabelle – Rovinski, Jean: L'emprise de la vie professionnelle sur la vie personnelle. *JCP S (édition sociale)*, (37), 2016. pp. 35–39.

Bibby 2016 = Bibby, Andrew: *You're being followed Electronic Monitoring and surveillance in the workplace*. UNI/GS/06-2006/0035/EN. UNI Global Union. 2016

Bidet – Porta 2016 = Bidet, Alexandra – Porta, Jérôme: Le travail à l'épreuve du numérique. *Revue droit du travail Dalloz*, (5), 2016. pp. 328–334.

Bioy 2016 = Bioy, Xavier: *Droits fondamentaux et libertés publiques*. 4e édition. LGDJ-Lextenso éditions (Collection Cours), Issy-les-Moulineaux, 2016

Birnhack 2008 = Birnhack, Michael D.: The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Review*, 24(6), 2008. pp. 508–520.

Bitan 2011 = Bitan, Florence: Fasc. 4740 : Courrier électronique. *JurisClasseur Communication, 2011*

Blanpain 2002 = Blanpain, Roger: *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. Kluwer Law International, The Hague, 2002. pp. 35–44.

Bloustein 1964 = Bloustein, Edward J.: Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser. *New York University Law Review*, 39(6), 1964. pp. 962–1007.

Bokor et al. 2007 = Bokor, Attila *et al.*: *Emberi erőforrás menedzsment*. Aula Kiadó, Budapest, 2007

Bölcskei 2019 = Bölcskei, Krisztián: *GDPR Kézikönyv 2.0*. Vezinfó Kiadó és Tanácsadó Kft., Budapest, 2019

Bolton 2014 = Bolton, Robert Lee: The Right to Be Forgotten: Forced Amnesia in a Technological Age. *The John Marshall Journal of Information Technology & Privacy Law*, 31(2), 2014. pp. 133–144.

Bond 2018 = Bond, Martyn: *Une introduction à la Convention européenne des droits de l'homme*. Conseil de l'Europe, Strasbourg, 2018

Boucher 1974 = Boucher, Philippe: « Safari » ou la chasse aux Français, *Le Monde*, 21 March, 1974. pp. 9–9.

Bouchet 2004 = Bouchet, Hubert: *La cybersurveillance sur les lieux de travail*. Documentation française: Commission nationale de l'informatique et des libertés, Paris, 2004

Bounedjoum 2016 = Bounedjoum, Amira: Réforme européenne des données personnelles : les nouveautés pour les droits des personnes. *JCP E Semaine Juridique*, (22), 2016. pp. 44–47.

Bourgeois – Touranchet – Alas-Luquetas 2017 = Bourgeois, Marie-Bénédicte – Touranchet, Loïc – Alas-Luquetas, Xavier: Le droit à la déconnexion. *JCP S (Édition sociale)*, (24), 2017. pp. 15–18.

Bourgeois 2017 = Bourgeois, Matthieu: *Droit de la donnée : principes théoriques et approche pratique*. LexisNexis, Paris, 2017

Boyd – Ellison 2008 = Boyd, Danah M. – Ellison, Nicole B: Social Network Sites: Definition, History and Scholarship. *Journal of Computer Mediated Communication*, 13(1), 2008. pp. 210–230.

Bozarth 2010 = Bozarth, Jane: *Social media for trainers: techniques for enhancing and extending learning*. Pfeiffer, San Francisco, 2010

Breznay 2002 = Breznay, Tibor: *A munka törvénykönyve egységes szerkezetben állásfoglalásokkal és magyarázatokkal*. Bővített kiadás. Kompkonzult, Budapest, 2002

Breznay 2006 = Breznay, Tibor: *A munkajog nagy kézikönyve*. Complex Kiadó, Budapest, 2006

Brown – Vaughn 2011 = Brown, Victoria R. – Vaughn, E. Daly: The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions. *Journal of Business and Psychology*, 26(2), 2011. pp. 219–225.

Bruguière 2017 = Bruguière, Jean-Michel *et al.*: Actualité du droit de l'internet (février – octobre 2016). *Revue Lamy Droit civil*, (144), 2017

Buitelaar 2012 = Buitelaar, J. C.: Privacy: Back to the Roots. *German Law Journal*, 13(3), 2012. pp. 171–202.

Burgorgue-Larson 2005 = Burgorgue-Larson, Laurence: *L'appréhensionconstitutionnelle de la vie privée en Europe : Analyse croisée des systèmes constitutionnels allemand, espagnol et français*. In: Sudre, Frédéric (ed.): Le droit à la vie privée au sens de la Convention européenne des droits de l'homme. Bruylant, Bruxelles, 2005. pp. 69–115.

Buttarelli 2009 = Buttarelli, Giovanni: *Do you have a private life at your workplace? Privacy in the workplace in EC institutions and bodies*. 31st International Conference of Data Protection and Privacy, Madrid, 4–6 November, 2009

Buttarelli 2010 = Buttarelli, Giovanni: *Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation*. T-PD-BUR(2010)11. The Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 2010

Bygrave 2004 = Bygrave, Lee A.: Privacy Protection in a Global Context – A Comparative Overview. *Scandinavian Studies in Law*, 47, 2004. pp. 319–348.

Bylund et al. = Bylund, Markus *et al.*: *PRIMA – Privacy Research through the Perspective of a Multidisciplinary Mash up*. Available at: http://soda.swedish-ict.se/4046/1/PRIMA_final_DOC_17.pdf (Accessed: 12 March 2018)

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

Cailleteau 2018 = Cailleteau, Clément: Temps de travail et droit à la déconnexion. *Lexbase Hebdo – Edition Sociale*, (750), 2018

Cantero – Coupez 2014 = Cantero, Isabelle – Coupez, François: L'utilisation des réseaux sociaux par l'entreprise : des risques maîtrisés ? *Revue Banque*, (769), 2014. p. 39.

Caprioli 2012 = Caprioli, Éric A.: Les propos tenus par une salarié sur Facebook peuvent justifier son licenciement. *Communication Commerce Électronique*, (4), 2012. pp. 37–40.

Caprioli 2018 = Caprioli, Éric A.: Licenciement : obtention loyale de la preuve sur le réseau social Facebook afin de caractériser une faute grave. *Communication Commerce Électronique*, (6), 2018. pp. 43–43.

Carbonnier 1971 = Carbonnier, Jean: *Droit civil. 1, Introduction. Les Personnes*. 9th edn. Presses universitaires de France, Paris, 1971

Cariat 2017 = Cariat, Nicolas: *Respect de la vie privée et familiale*. In: Charte des droits fondamentaux de l'Union européenne. Bruylant, Bruxelles, 2017. pp. 161–183.

Carlson 2014 = Carlson, Kathleen: Social Media and the Workplace: How I Learned to Stop Worrying and Love Privacy Settings and the NLRB. *Florida Law Review*, 66(1), 2014. pp. 479–509.

Caron 2018 = Caron, Mathilde: Les limites à la liberté d'expression d'un salarié sur Facebook. *Les Cahiers Sociaux*, (305), 2018. pp. 131–133.

Casaux-Labrunée 2012 = Casaux-Labrunée, Lise: Vie privée des salariés et vie de l'entreprise. *Droit social*, (4), 2012. pp. 331–345.

Cassart 2013 = Cassart, Alexandre: L'extension de la notion de communauté d'intérêts aux réseaux sociaux. *Revue du Droit des Technologies de l'Information*, (52), 2013. pp. 101–106.

Castets-Renard 2011 = Castets-Renard, Céline: Vie privée du salarié et TIC : attention à la violation de la charte informatique ! *Revue Lamy droit de l'immatériel*, (69), 2011. pp. 33–35.

Clark – Roberts 2010 = Clark, Leigh A. – Roberts, Sherry J.: Employer's Use of Social Networking Sites. A Socially Irresponsible Practice. *Journal of Business Ethics*, 95(4), 2010. pp. 507–525.

Clarke 2014 = Clarke, Roger: Privacy and Social Media: An Analytical Framework. *Journal of Law, Information and Science*, 23(1), 2014. pp. 169–191.

Collomp 2010 = Collomp, Evelyne: La vie personnelle au travail. Dernières évolutions jurisprudentielles. *Droit social*, (1), 2010. pp. 40–43.

Colonna – Renaux-Personnic 2017 = Colonna, Joël – Renaux-Personnic, Virginie: Vie privée et surveillance des communications du salarié : la position de la Cour européenne des droits de l'Homme ; Note sous Cour Européenne des Droits de l'Homme, grande Chambre, 5 septembre 2017, arrêt numéro 61496/08. *La Gazette du Palais*, (43), 2017. pp. 43–45.

Combrexelle 2010 = Combrexelle, Jean-Denis: Vie professionnelle et vie personnelle. *Droit social*, (1), 2010. pp. 12–13.

Contamine 2013 = Contamine, Alexis: La surveillance du salarié. *Revue Le Lamy de la Concurrence*, (37), 2013. pp. 155–162.

Cornesse 2011 = Cornesse, Isabelle: Quand la CNIL vient au secours des salariés. *Revue Lamy Droit des affaires*, 58, 2011. pp. 52–53.

Corrignan-Carsin 2009 = Corrignan-Carsin, Danielle: La Chambre sociale fixe les limites du pouvoir disciplinaire de l'employeur. *JCP E Semaine Juridique (édition entreprise)*, (40), 2009. pp. 44–47.

Corrignan-Carsin 2011 = Corrignan-Carsin, Danielle: Vie personnelle – vie professionnelle : la cloison est-elle étanche ? *JCP S (édition sociale)*, (26), 2011. pp. 38–41.

Corrignan-Carsin 2018 = Corrignan-Carsin, Danielle: Tenir des propos injurieux sur Facebook au sein d'un groupe fermé ne justifie pas un licenciement. *JCP G Semaine Juridique (édition générale)*, (40), 2018. pp. 1762–1762.

Costa – Poullet 2012 = Costa, Luiz – Poullet, Yves: Privacy and the regulation of 2012. *Computer Law and Security Review*, 28(3), 2012. pp. 254–262.

Costes 2011 = Costes, Lionel: Réseaux sociaux : nouveaux enjeux et nouveaux défis pour les entreprises. *Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique*, (74), 2011. pp. 131–138.

Costes 2017 = Costes, Lionel: CEDH : surveillance des courriels d'un employé à son insu constitutive d'une violation du droit au respect de la vie privée et de la correspondance. *Revue Lamy droit de l'immatériel*, (140), 2017. pp. 35–35.

Crouzatier-Durand 2013 = Crouzatier-Durand, Florence: *Fiches de libertés publiques et droits fondamentaux*. 2nd edn. Ellipses, Paris, 2013

Cséffán 2016/2018/2019 = Cséffán József: *A Munka Törvénykönyve és magyarázata*. Szegedi Rendezvényszervező Kft., Szeged, 2016/2018/2019

Cseh 2013 = Cseh, Gergely: A közösségi portálok árnyoldalai. *Infokommunikáció és jog*, (2), 2013. pp. 90–95.

Dabosville 2012 = Dabosville, Benjamin: Les contours de l'abus d'expression du salarié. *Revue droit du travail Dalloz*, (5), 2012. pp. 275–282.

De Hert – Gutwirth 2009 = De Hert, Paul – Gutwirth, Serge: *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*. In: Gutwirth, Serge et al. (eds): Reinventing Data Protection? Springer, 2009. pp. 3–44.

De Hert – Lammerant 2013 = De Hert, Paul – Lammerant, Hans: *Protection of Personal Data in Work-related Relations*. Study PE 474.440. Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs. Civil Liberties, Justice and Home Affairs, 2013

De Hert – Papakonstantinou 2012 = De Hert, Paul – Papakonstantinou, Vagelis: The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law and Security Review*, 28(2), 2012. pp. 130–142.

De Hert 2008 = De Hert, Paul: Identity management of e-ID, privacy and security in Europe. A human rights view. *Information Security Technical Report*, 13(2), 2008. pp. 71–75.

De Terwangne – Rosier – Losdyck 2016 = De Terwangne, Cécile – Rosier, Karen – Losdyck, Bénédicte: Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel. *Revue du droit des technologies de l'information*, (62), 2016. pp. 5–56.

Del Riego – Sánchez Abril – Levin 2012 = Del Riego, Alissa – Sánchez Abril, Patricia – Levin, Avner: Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy. *Journal of Internet Law*, 16(3), 2012– pp. 1., 18–26.

Denier 2003 = Denier, Jean-Louis: L'utilisation privative des NTIC d'entreprise. *Les cahiers du DRH*, (89), 2003. pp. 31–34.

Denizeau 2017 = Denizeau, Charlotte: *Droit des libertés fondamentales*. 6th edn. Vuibert, Paris, 2017

Despax 1963 = Despax, Michel: La vie extra-professionnelle du salarié et son incidence sur le contrat de travail. *Juris-Classeur Périodique. La Semaine Juridique. éd. G.*, (1776), 1963

Détraigne – Escoffier 2009 = Détraigne, Yves – Escoffier, Anne-Marie: *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*. Rapport d'information 441. Sénat. 2009

Dockès 2004 = Dockès, Emmanuel: Le pouvoir dans les rapports de travail: essor juridique d'une nuisance économique. *Droit social*, (6), 2004. pp. 620–628.

Duez-Ruff 2012 = Duez-Ruff, Valérie: Impact des nouvelles technologies sur le droit du travail : un salarié appartient-il virtuellement à son employeur ? *Lexbase Hebdo – Edition Sociale*, (498), 2012

Dupuis 2001 = Dupuis, Michel: La vie privée à l'épreuve de l'Internet : quelques aspects nouveaux. *Revue Juridique Personnes et Famille*, (12), 2001. pp. 6–9.

Dupuis 2013 = Dupuis, Michel: La vie privée à l'épreuve des réseaux sociaux. *Revue Lamy Droit Civil*, (102), 2013. pp. 39–46.

Duquesne 2003 = Duquesne, François: *Droit du travail*. 2nd edn. Gualino, Paris, 2003

Durand – Jaussaud 1947 = Durand, Paul – Jaussaud, R.: *Traité de droit du travail. Tome I*. Dalloz, Paris, 1947

Ebnet 2012 = Ebnet, Nathan J.: It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act. *Minnesota Law Review*, 97(1), 2012. pp. 306–336.

El Badawi 2014 = El Badawi, Lamia: La place des réseaux sociaux dans l'entreprise. *Revue Lamy droit de l'immatériel*, (103), 2014. pp. 108–119.

El Wafi 2016 = El Wafi, Wafa: *Perméabilité des frontières vies « personnelle et professionnelle » et usage des TIC : modèles d'articulation*. Université de Lorraine, 2016

Ellickson – Atkinson 2013 = Ellickson, Denis – Atkinson, Meg: *When Can Your Employer "Unlike" You? Just Cause for Dismissal and Social Media*. In: The Law Society of Upper Canada: Employment Law and the New Workplace in the Social Media Age. Irwin Law, Toronto, 2013. pp. 259–280.

Ember 2012 = Ember, Alex: Meddig terjedhet a munkáltató ellenőrzési joga: avagy a munkavállaló munkáltató általi kamerás megfigyelésének aggályai. *Humánpolitikai szemle*, (9), 2012. pp. 30–36.

Ember 2015 = Ember, Alex: *A munkáltató jogos gazdasági érdekének a védelme*. In: Lajkó, Dóra – Varga, Norbert (eds): Alapelvek és alapjogok. Szegedi Tudományegyetem Állam- és Jogtudományi Doktori Iskola, Szeged, 2015. pp. 113–124.

Engler – Tanoury 2007 = Engler, Peter – Tanoury, Peter: *Employers Use of Facebook in Recruiting*. In: McIntosh, Dan *et al*. (eds): The Ethical Imperative in the Context of Evolving Technologies. University of Colorado Leeds School of Business, 2007. pp. 61–74. Available at: http://www.ethicapublishing.com/ethicalimperative.pdf (Accessed: 13 July 2016)

Eriksson 2006 = Eriksson, Maja: *Article 7. Respect for private and family life*. In: EU Network of Independent Experts on Fundamental Rights: Commentary of the Charter of Fundamental Rights of the European Union, 2006. pp. 78–89.

Falque-Pierrotin 2012 = Falque-Pierrotin, Isabelle: La Constitution et l'Internet. *Les nouveaux cahiers du Conseil constitutionnel*, 36, 2012. pp. 31–44.

Favennec-Héry – Verkindt 2016 = Favennec-Héry, Françoise – Verkindt, Pierre-Yves: *Droit du travail*. 5th edn. LGDJ Lextenso éditions, Issy-les-Moulineaux, 2016

Favoreu et al. 2015 = Favoreu, Louis *et al.*: *Droit des libertés fondamentales*. 7th edn. Dalloz, Paris, 2015

Fel – Sordet 2010 = Fel, Caroline – Sordet, Emmanuel: L'utilisation des réseaux sociaux par l'entreprise et ses collaborateurs. *JCP S (édition sociale)*, (29), 2010. pp. 19–24.

Féral-Schuhl 2010/2018 = Féral-Schuhl, Christiane: *Cyberdroit: le droit à l'épreuve de l'internet*. Dalloz, Paris, 2010/2018

Ferenczy 2010 = Ferenczy, Endre: Az adatvédelem külföldi szabályozása. *Tudományos közlemények*, (23), 2010. pp. 47–67.

Fézer 2014 = Fézer, Tamás: *Harmadik rész: személyiségi jogok*. In: Osztovits, András. (ed.): A Polgári Törvénykönyvről szóló 2013. évi V. törvény és a kapcsolódó jogszabályok nagykommentárja. I. kötet. Opten Informatikai Kft., Budapest, 2014. pp. 249–355.

Fialová 2014 = Fialová, Eva: Data Portability and Informational Self-determination. *Masaryk University Journal of Law and Technology*, 8(1), 2014. pp. 45–55.

Finn et al. 2013 = Finn, Rachel L. *et al.*: *Seven Types of Privacy*. In: Gutwirth, Serge (ed.): European Data Protection: Coming of Age. Springer, Dordrecht, 2013. pp. 3–32.

Flaherty – Whitmore 2013 = Flaherty, Patrick – Whitmore, Sarah: *Privacy Protection in the Digital Workplace*. In: Law Society of Upper Canada: Employment Law and the New Workplace in the Social Media Age. Irwin Law, Toronto, 2013. pp. 9–29.

Flint 2009 = Flint, David: Law shaping technology: Technology shaping the law. *International Review of Law, Computers & Technology*, 23(1–2), 2009. pp. 5–11.

Flynn 2012 = Flynn, Nancy: *The Social Media Handbook. Policies and Best Practices to Effectively Manage Your Organization's Social Media Presence, Posts, and Potential Risks*. Pfeiffer, San Francisco, 2012

Fried 1968 = Fried, Charles: Privacy. *The Yale Law Journal*, 77(3), 1968. pp. 475–493.

Fritsch 2015 = Fritsch, Clara: *Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite*. In: Gutwirth, Serge – Leenes, Ronald – de Hert, Paul (eds.): Reforming European Data Protection Law. Springer, Dordrecht, Heidelberg, New York, London, 2015. pp. 147–167.

Funk 2011 = Funk, Tom: *Social Media Playbook for Business. Reaching Your Online Community with Twitter, Facebook, LinkedIn, and More*. Praeger, Santa Barbara, Denver, Oxford, 2011

Gaïa 2004 = Gaïa, Patrick: La Charte des droits fondamentaux de l'Union européenne. *Revue française de droit constitutionnel*, (2), 2004. pp. 227–246.

Galántai 2003 = Galántai, Zoltán: *E-privacy olvasókönyv. Dialógusok a privacyről és az internetről – meg a cyberpornóról, a megfigyelésekről és egyebekről*. 2003. Available at: https://mek.oszk.hu/04100/04134/html/ (Accessed: 18 November 2019)

Gautier 2001 = Gautier, Pierre-Yves: La preuve hors la loi ou comment, grâce aux nouvelles technologies, progresse "la vie privée" des salariés. *Recueil Dalloz Sirey*, (39), 2001. pp. 3148–3153.

Gavison 1980 = Gavison, Ruth: Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 1980. pp. 421–471.

Geffray 2014 = Geffray, Edouard: La protection des données personnelles, élément clé à l'ère numérique. *Légipresse*, (320), 2014. pp. 515–516.

Gellert – Gutwirth 2013 = Gellert, Raphaël – Gutwirth, Serge: The legal construction of privacy and data protection. *Computer Law and Security Review*, 29(5), 2013. pp. 522–530.

Gerety 1977 = Gerety, Tom: Redefining Privacy. *Harvard Civil Rights-Civil Liberties Law Review*, 12(2), 1977. pp. 233–296.

Gheorghe 2017 = Gheorghe, Monica: Considerations on the conditions under which the employer may monitor their employees at the workplace. *Juridical Tribune*, 7(2), 2017. pp. 62–69.

Ghoshray 2013 = Ghoshray, Saby: The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up. *The John Marshall Review of Intellectual Property Law*, 12(3), 2013. pp. 551–582.

Gillier 2009 = Gillier, Hadrien: Vie personnelle et licenciement disciplinaire. *Bulletin du travail (ancien nom Cahiers sociaux du barreau de Paris)*, (213), 2009. pp. 213–214.

González Fuster – Gutwirth 2013 = González Fuster, Gloria – Gutwirth, Serge: Opening up personal data protection: A conceptual controversy. *Computer Law and Security Review*, 29(5), 2013. pp. 531–539.

Gormley 1992 = Gormley, Ken: One Hundred Years of Privacy. *Wisconsin Law Review*, (5), 1992. pp. 1335–1441.

Görög 2016 = Görög, Márta: *A magánélethez való jog mint a személyiségi jog újabb, magánjogi kódexben nevesített vonatkozása*. In: Balogh, Elemér (ed.): Számadás az Alaptörvényről: tanulmányok a Szegedi Tudományegyetem Állam- és Jogtudományi Kar oktatóinak tollából. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2016. pp. 51–63.

Grabarczyk 2011 = Grabarczyk, Katarzyna: Vie privée et nouvelles technologies. *Revue des droits et libertés fondamentaux*, (7), 2011

Grandguillot 2016 = Grandguillot, Dominique: *L'essentiel du Droit du travail*. 16th edn. Gualino: Lextenso Éditions, Issy-les-Moulinaux, 2016

Grangé – Froger 2003 = Grangé, Joël – Froger, Caroline: Cyber-Monitoring in the French Workplace. *International Business Lawyer*, 31(5), 2003. pp. 213–217.

Grégoire 2018 = Grégoire, Frédéric: L'usage immodéré de Facebook peut conduire directement à Pôle emploi. *JCP G Semaine Juridique (édition générale)*, (9), 2018. pp. 437–437.

Griguer – Schwartz 2017 = Griguer, Merav – Schwartz, Julie: Les risques liés à l'implémentation du droit à la déconnexion dans l'entreprise. *Cahiers de droit de l'entreprise*, (2), 2017. pp. 50–52.

Griguer 2010 = Griguer, Merav: Les réseaux sociaux sous le contrôle des DSI. *Cahiers de droit de l'entreprise*, (6), 2010. pp. 62–64.

Griguer 2013 = Griguer, Merav: Protection des données personnelles : conformité et bonnes pratiques des entreprises. *Cahiers de droit de l'entreprise*, (1), 2013. pp. 73–76.

Griguer 2017 = Griguer, Merav: 3 questions: Le droit à la déconnexion. *La Semaine Juridique Entreprise et Affaires*, (30–34), 2017. pp. 30–34.

Grimmelmann 2009 = Grimmelmann, James: Saving Facebook. *Iowa Law Review*, 94(4), 2009. pp. 1137–1206.

Gross – Acquisti 2005 = Gross, Ralph – Acquisti, Alessandro: *Information Revelation and Privacy in Online Social Networks*. Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005

Gross 1967 = Gross, Hyman: The Concept of Privacy. *New York University Law Review*, 42(1), 1967. pp. 34–54.

Grynbaum – Le Goffic – Morlet-Haïdara 2014 = Grynbaum, Luc – Le Goffic, Caroline – Morlet-Haïdara, Lydia: *Droit des activités numériques*. 1st edn. Dalloz, Paris, 2014

Gutwirth 2002 = Gutwirth, Serge: *Privacy and the Information Age*. Rowman & Littlefield Publishers Inc., Lanham, 2002

Gyulavári – Kun 2013 = Gyulavári, Tamás – Kun, Attila: A munkáltatói szabályzat az új Munka Törvénykönyvében. *Magyar jog*, 60(9), 2013. pp. 556–566.

Gyulavári 2012/2013/2017 = Gyulavári, Tamás (ed.): Munkajog. ELTE Eötvös Kiadó, Budapest, 2012/2013/2017

Hajdú – Kun 2012 = Hajdú, József – Kun, Attila (eds): *Munkajog I.* Patrocinium, Budapest, 2012

Hajdú – Kun 2014 = Hajdú, József – Kun, Attila (eds): Munkajog. Patrocinium, Budapest, 2014

Hajdú 2004 = Hajdú, József: '*Habilitációs tézisek*'. Szegedi Tudományegyetem, 2004

Hajdú 2005 = Hajdú, József: *A munkavállalók személyiségi jogainak védelme*. Pólay Elemér Alapítvány, Szeged, 2005

Halmos – Petrovics 2014 = Halmos, Szilvia – Petrovics, Zoltán: *Munkajog*. Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kar, Budapest, 2014

Hardouin 2011 = Hardouin, Ronan: Facebook ou l'établissement de la frontière entre espace public et sphère privée. *Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique*, (67), 2011. pp. 54–55.

Hartzog 2013 = Hartzog, Woodrow: *Privacy and Terms of Use*. In: Stewart, Daxton R. (ed.): Social Media and the Law. A Guidebook for Communication Students and Professionals. Routledge, New York, London, 2013. pp. 50–74.

Hauser 2002 = Hauser, Jean: Vie privée du salarié : E-mail, domicile, sacs, bermudas et survêtement. *RTD Civ.*, (1), 2002. pp. 72.

Hegedűs 2005 = Hegedűs, Bulcsú: A munkahelyi elektronikus levelezés ellenőrzésének nemzetközi gyakorlata. *Infokommunikáció és jog*, 2(10), 2005. pp. 185–190.

Hegedűs 2006 = Hegedűs, Bulcsú: A munkahelyi hagyományos és elektronikus levelezés ellenőrzése. *Munkaügyi szemle*, 50(6), 2006. pp. 47–49.

Henderson 2013 = Henderson, Jennifer: *The Boundaries of Free Speech in Social Media*. In: Stewart, Daxton R. (ed.): Social Media and the Law. A Guidebook for Communication Students and Professionals. Routledge, New York, London, 2013. pp. 1–22.

Hendrickx 2000 = Hendrickx, Frank: *Data protection and codes of conduct: self-regulation versus legislative intervention*. In: Blanpain, Roger (ed.): Multinational Enterprises and the Social Challenges of the XXIst Century: the ILO Declaration on Fundamental Principles at Work, Public and Private Corporate Codes of Conduct. Bulletin of Comparative Labour Relations, 37, 2000. pp. 253–267.

Hendrickx 2001 = Hendrickx, Frank: *Electronic Monitoring and Employment Privacy*. In: Blanpain, Roger (ed.): The Evolving Employment Relationship and the New Economy. Kluwer Law International, The Hague/London/New York, 2001. pp. 247–250.

Hendrickx 2002 = Hendrickx, Frank: *Protection of workers' personal data in the European Union, Two studies*. EC, 2002

Hendrickx 2002a = Hendrickx, Frank: *Privacy and Employment Law: General Principles and Application to Electronic Monitoring*. In: Blanpain, Roger. (ed.): On-line Rights for Employees in the Information Society. Use and Monitoring of E-mail and Internet at Work. Kluwer Law International, The Hague, 2002. pp. 45–64.

Hennette-Vauchez – Roman 2017 = Hennette-Vauchez, Stéphanie – Roman, Diane: *Droits de l'homme et libertés fondamentales*. 3rd edn. Dalloz, Paris, 2017

Herbert 2011 = Herbert, William A.: Workplace Consequences of Electronic Exhibition and Voyeurism. *IEEE Technology and Society Magazine*, 30(3), 2011. pp. 25–33.

Hess-Fallon – Maillard – Simon 2015 = Hess-Fallon, Brigitte – Maillard, Sandrine – Simon, Anne-Marie: *Droit du travail*. 24th edn. Sirey-Dalloz, Paris, 2015

Hiselius 2010 = Hiselius, Patrik: ICT/Internet and the Right to Privacy. Scandinavian *Studies in Law*, 56, 2010. pp. 201–208.

Horinka 2018 = Horinka, Éva: *A munkavállaló és a munkáltató személyiségi jogainak védelme a munkaviszonyban*. In: Mailáth György Tudományos Pályázat 2017. Díjazott dolgozatok. Országos Bírósági Hivatal, Budapest, 2018. pp. 593–664.

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

Horváth – Gelányi 2011 = Horváth, Linda – Gelányi, Anikó: Lájkolni vagy nem lájkolni? A közösségi oldalak használatának munkajogi kérdései. *Infokommunikáció és jog*, (2), 2011. pp. 60–66.

Hughes 2015 = Hughes, R. L. David: Two concepts of privacy. *Computer Law and Security Review*, 31(4), 2015. pp. 527–537.

Icard 2014 = Icard, Julien: De l'incidence de la source d'une communication d'un salarié sur sa nature et sur son régime. *Cahiers sociaux du Barreau de Paris*, (304), 2018. pp. 84–85.

Icard 2014 = Icard, Julien: Faits commis en dehors des temps et lieu de travail mais rattachés à la vie de l'entreprise. *Bulletin du travail (ancien nom Cahiers sociaux du barreau de Paris)*, (268), 2014. pp. 642–642.

Inforeg 2015 = Inforeg: Pouvoir disciplinaire : vie personnelle, vie professionnelle et Facebook', *Cahiers de droit de l'entreprise*, (6), 2015. pp. 67–69.

Inforeg 2017 = Inforeg: De la difficulté d'appliquer le droit à la déconnexion à tous les salariés. *Cahiers de droit de l'entreprise*, (3), 2017. pp. 71–73.

Jacquelet 2008 = Jacquelet, Cédric: *La vie privée du salarié à l'épreuve des relations de travail*. Presses universitaires d'Aix-Marseille, Aix-en-Provence, 2008

Jónás 2010 = Jónás, Tünde: Véleménynyilvánítási szabadság a munkaviszonyban. *Pécsi Munkajogi Közlemények*, 3(2), 2010. pp. 23–47.

Jones – Schuckman – Watson 2007 = Jones, Michael – Schuckman, Adam –Watson, Kelly: *The Ethics of Pre-Employment Screening Through the Use of the Internet*. In: McIntosh, Dan *et al*. (eds): The Ethical Imperative in the Context of Evolving Technologies. University of Colorado Leeds School of Business, 2007

Jóri – Hegedűs – Kerekes 2010 = Jóri, András – Hegedűs, Bilcsú – Kerekes, Zsuzsanna (eds): *Adatvédelem és információszabadság a gyakorlatban*. Complex, Budapest, 2010

Jóri – Soós 2016 = Jóri, András – Soós, Andrea Klára: *Adatvédelmi jog: magyar és európai szabályozás*. HVG–ORAC, Budapest, 2016

Jóri 2005 = Jóri, András: *Adatvédelmi kézikönyv*. Osiris Kiadó, Budapest, 2005

Jóri 2009 = Jóri, András: *A magánszférajogok*. In: Jakab, András (ed.): Az Alkotmány kommentárja II. Századvég Kiadó, Budapest, 2009. pp. 2167–2193.

Jóri et al. 2018 = Jóri, András *et al.*: *A GDPR magyarázata*. HVG–ORAC, Budapest, 2018

Jourard 1966 = Jourard, Sidney M.: Some Psychological Aspects of Privacy. *Law and Contemporary Problems*, 31(2), 1966. pp. 307–318.

Jue – Marr – Kassotakis 2010 = Jue, Arthur L. – Marr, Jackia Alcade – Kassotakis, Mary Ellen: *Social Media at Work. How Networking Tools Propel Organizational Performance*. Jossey-Bass, San Francisco, 2010

Julien – Mazuyer 2018 = Julien, Mathilde – Mazuyer, Emmanuel: Le droit du travail à l'épreuve des plateformes numériques. *Revue droit du travail Dalloz*, (3), 2018. pp. 189–198.

Kajtár – Mestre 2016 = Kajtár, Edit – Mestre, Bruno: Social networks and employees' right to privacy in the pre-employment stage: some comparative remarks and interrogations. *Hungarian Labour Law E-journal*, (1), 2016. pp. 22–39.

Kajtár 2014 = Kajtár, Edit: A munkáltatói utasítás helye a 21. század munkajogában. *Jura*, 20(2), 2014. pp. 214–224.

Kajtár 2015 = Kajtár, Edit: *Európai ügyek a Facebook sötét oldaláról – A munkavállalók közösségi oldalakon tanúsított kötelezettségszegő magatartása*. In: Horváth, István (ed.): Tisztelgés: ünnepi tanulmányok Dr. Hágelmayer Istvánné születésnapjára. ELTE Eötvös Kiadó, Budapest, 2015. pp. 199–213.

Kajtár 2015a = Kajtár, Edit: *Think it over! Pre-employment search on social network sites*. In: Vinković, Mario (ed.): New Developments in EU Labour, Equality and Human Rights Law. Proceedings from the International Jean Monnet Conference "New Developments in EU Labour, Equality and Human Rights Law", Osijek 21 and 22 May 2015. Josip Juraj Strossmayer University of Osijek Faculty of Law, Osijek, 2015. pp. 97–106.

Kajtár 2015b = Kajtár, Edit: Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship. *Acta Juridica Hungarica*, 56(4), 2015. pp. 268–280.

Kajtár 2016 = Kajtár, Edit: *Dignity at Work: Employee's Personality Rights in the 21st Century*. University of Pécs, Faculty of Law (PMJK Monographs 6), Pécs, 2016

Kállai 2017 = Kállai, Péter: Bărbulescu România elleni ügye. *Fundamentum*, 21(3–4), 2017. pp. 99–101.

Kalven 1966 = Kalven, Harry Jr.: Privacy in Tort Law – Were Warren and Brandeis Wrong?. *Law and Contemporary Problems*, 31(2), 1966. pp. 326–341.

Kambellari 2013 = Kambellari, Evisa: Employee email monitoring and workplace privacy in the European perspective. *Iustinianus Primus Law Review*, 8. 2013

Kang 1998 = Kang, Jerry: Information Privacy in Cyberspace Transactions. *Stanford Law Review*, 50(4), 1998. pp. 1193–1294.

Kaplan – Haenlein 2010 = Kaplan, Andreas M. – Haenlein, Michael: Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), 2010. pp. 59–68.

Kardkovács 2012/2016: Kardkovács, Kolos (ed.): *A Munka Törvénykönyvének magyarázata*. HVG–ORAC Lap- és Könyvkiadó, Budapest, 2012/2016

Kártyás – Kozma-Fecske 2016 = Kártyás, Gábor – Kozma-Fecske, Ivett: Szerelmes levelek a munkahelyi postafiókban. *HR & Munkajog*, 7(3), 2016. pp. 14–17.

Kártyás – Répáczki – Takács 2016 = Kártyás, Gábor – Répáczki, Rita – Takács, Gábor: *A munkajog digitalizálása. A munkajog hozzáalkalmazása a digitális munkakörnyezethez és a változó munkavállalói kompetenciákhoz*. Kutatási zárótanulmány, Budapest, 2016

Kayser 1995 = Kayser, Pierre: *La protection de la vie privée par le droit : protection du secret de la vie privée*. 3rd edn.Presses universitaires d'Aix-Marseille; Economica, Aix-en-Provence; Paris, 1995

Kéfer – Cornélis 2009 = Kéfer, Fabienne – Cornélis, Sabine: L'arrêt "Copland" ou l'espérance légitime du travailleur quant au caractère privé de ses communications. *Revue Trimestrielle des Droits de l'Homme*, (79), 2009. pp. 779–793.

Kennedy – Macko 2007 = Kennedy, Nicole – Macko, Matt: *Social Networking Privacy and Its Effects on Employment Opportunities*. In: Larsen, Kai R. – Voronovich, Zoya. A. (eds): Convenient Or Invasive: The Information Age. Ethica Publishing, 2007

Kindt 2015 = Kindt, Els: *Privacy and Data Protection Law: An Introduction*. IC1206 Training School: De-identification for privacy protection in multimedia content 07–11 October 2015, Limassol, Cyprus, 11 October 2015

Kiss 2002 = Kiss, György: *A szerződéses szabadság átalakulása a munkajogban az alapjogok tükrében*. In: Czúcz, Ottó – Szabó, István (eds): Ünnepi tanulmányok. Munkaügyi igazgatás, munkaügyi bíráskodás: Radnay József 75. születésnapjára. Bíbor Kiadó, Miskolc, 2002. pp. 259–276.

Kiss 2003 = Kiss, György: A munkajog jogforrási rendszere és az alapjogok I. *Jura*, 9(1), 2003. pp. 79–95.

Kiss 2005 = Kiss, György: Munkajog. 2nd edn. Osiris Kiadó, Budapest, 2005

Kiss 2010 = Kiss, György: *Alapjogok kollíziója a munkajogban*. Justis Tanácsadó Betéti Társaság, Pécs, 2010

Kiss 2015 = Kiss, György: *Opportunities and limits of application principles and Civil Code rules in Hungarian labour law Crisis management with means of civil law*. ELLN Working Paper No. 4. 2015

Kiss 2017 = Kiss, György: A munkajog szabályozásának dilemmái. *Miskolci Jogi Szemle*, XII(2), 2017. pp. 267–277.

Klausz 2013 = Klausz, Melinda: *Megosztok, tehát vagyok: A közösségi média és az Internet szép új világa*. Magánkiadás, Veszprém, 2013

Klausz 2016 = Klausz, Melinda: *A közösségi média nagykönyve: hogyan vidd sikerre céged és önmagad*. Athenaeum, Budapest, 2016

Knight – Saxby 2014 = Knight, Alison – Saxby, Steve: Global challenges of identity protection in a networked world. *Computer Law and Security Review*, 30(6), 2014. pp. 617–632.

Kocher 2013 = Kocher, Marguerite: La protection des données des salariés : que reste-t-il de l'arrêt Nikon ? *Legicom*, (1), 2013. pp. 129–140.

Kokott – Sobotta 2013 = Kokott, Juliane – Sobotta, Christoph: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), 2013. pp. 222–228.

Kommers – Miller 2012 = Kommers, Donald P. – Miller, Russell A.: *The constitutional jurisprudence of the Federal Republic of Germany*. 3rd edn. Duke University Press, Durham and London, 2012

Konvitz 1966 = Konvitz, Milton R.: Privacy and the Law: a Philosophical Prelude. *Law and Contemporary Problems*, 31(2), 1966. pp. 272–280.

Könyves Tóth 1990 = Könyves Tóth, Pál: Adatvédelem és információszabadság. *Világosság*, 31(8–9), 1990. pp. 621–629.

Könyves Tóth 2010 = Könyves Tóth, Pál: Az adatvédelmi törvény metamorfózisai. *Fundamentum*, (2), 2010. pp. 53–61.

Koops et al. 2017 = Koops, Bert-Jaap *et al.*: A Typology of Privacy. *U. Pa. J. Int'l L.*, 38(2), 2017. pp. 483–577.

Kozma 2013 = Kozma, Anna: Mire köteles a munkavállaló? *HR & Munkajog*, 4(10) 2013. pp. 8–14.

Krishnamurthy – Wills 2008 = Krishnamurthy, Balachander – Wills, Craig E: *Characterizing Privacy in Online Social Networks*. Proceedings of the first workshop on Online social networks, Seattle, WA, USA, 2008

Kubicek et al. 2019 = Kubicek, Bettina *et al.*: *Working conditions and workers' health*. Publications Office of the European Union, Luxembourg: Eurofound, 2019

Kun 2013 = Kun, Attila: Közösségi média és munkajog – avagy „online" munkaidőben és azon túl. *Munkaügyi Szemle*, (3), 2013. pp. 12–19.

Kun 2018 = Kun, Attila: *A digitalizáció kihívásai a munkajogban*. In: Homicskó, Árpád Olivér (ed.): Egyes modern technológiák etikai, jogi és szabályozási kihívásai. Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar (Acta Caroliensia Conventorum Scientiarum Iuridico-Politicarum, XXII), Budapest , 2018. pp. 119–138.

Kuner 2009 = Kuner, Christopher: An international legal framework for data protection: Issues and prospects. *Computer Law and Security Review*, 25(4), 2009. pp. 307–317.

La Rédaction D.O. 2013 = La Rédaction D.O.: Diffusion des bonnes pratiques en matière de protection des données personnelles des salariés. *JCP S (édition sociale)*, (7), 2013. pp. 3–7.

Lábady 1995 = Lábady, Tamás: A magánélet alkotmányos védelme (A házasság és a család védelme, a magánszférához való jog). *Acta Humana: Emberi jogi közlemények*, (18–19), 1995. pp. 74–86.

Lahalle 2016 = Lahalle, Thibault: *Droits et obligations des parties*. JurisClasseur Travail Traité Fasc. 18–1, 2016

Lambert – Rigaux 1993 = Lambert, Pierre – Rigaux, François: Perquisition au cabinet d'un avocat et droit au respect de la vie privée, de la correspondance et du domicile. *Revue Trimestrielle des Droits de l'Homme*, (15), 1993. pp. 467–481.

Lambert 2014 = Lambert, Paul: *International Handbook of Social Media Laws*. Bloomsbury, Haywards Heath, 2014

La Rue 2011 = La Rue, Frank: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. UN General Assembly Sixty-sixth session. Promotion and protection of human rights. A/66/290. United Nations, 2011

Lauth 2009 = Lauth, Mechtild: *Thematic Legal Study on assessment of data protection measures and relevant institutions. Report on Germany*. FRA. 2009. Available at: https://fra.europa.eu/sites/default/files/role-data-protection-authorities-2009-de.pdf.

Le Clainche 2012 = Le Clainche, Julien: Expression des salariés sur internet : attention aux « faux amis ». *Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique*, (81), 2012. pp. 45–50.

Le Cohu 2018 = Le Cohu, Pierre: Un salarié peut-il critiquer son employeur sans être sanctionné ? *La Gazette du Palais*, (10), 2018. pp. 58–59.

Le Lamy Droit Du Numérique 2014 = Le Lamy Droit Du Numérique: (Guide), 2014 – Section 1 – Gestion Du Personnel Par Le Biais de L'informatique et Des Nouvelles Technologies de L'information

Le Lamy social 2019 = Le Lamy social: *150. Définition du contrat de travail*. 2019. Available at: shorturl.at/adoty (Accessed: 12 August 2019)

Lehoczkyné Kollonay 1997 = Lehoczkyné Kollonay, Csilla (ed.): *A magyar munkajog I.* Kulturtrade Kiadó, Budapest, 1997

Lepage 2000 = Lepage, Agathe: Pas d'échelle de responsabilité sur Internet en matière de diffamation. *Communication Commerce Électronique*, (2), 2000. pp. 24–26.

Lepage 2006 = Lepage, Agathe: La vie privée du salarié, une notion civiliste en droit du travail', *Droit social*, (4), 2006. pp. 364–377.

Levin – Sánchez Abril 2009 = Levin, Avner – Sánchez Abril, Patricia: Two Notions of Privacy Online. *Vanderbilt Journal of Entertainment and Technology Law*, 11(4), 2009. pp. 1001–1051.

Lhernould 2015 = Lhernould, Jean-Philippe: Les SMS du salarié à la libre disposition de l'employeur ? *Jurisprudence sociale Lamy*, (385), 2015. pp. 9–11.

Lhernould 2016 = Lhernould, Jean-Philippe: Statut des courriels provenant de la messagerie personnelle du salarié. *Jurisprudence sociale Lamy*, (405), 2016. pp. 10–12.

Lock 2019 = Lock, Tobias: *Article 7 CFR. Respect for private and family life*. In: Kellerbauer, Manuel – Klamert, Marcus – Tomkin, Jonathan (eds): Commentary on the EU Treaties and the Charter of Fundamental Rights. Oxford University Press, United Kingdom, 2019. p. 2115–2120.

Loiseau 2011 = Loiseau, Grégoire: Vie personnelle et licenciement disciplinaire. *Recueil Dalloz Sirey*, (23), 2011. pp. 1568–1569.

Loiseau 2014 = Loiseau, Grégoire: Le liberté d'expression du salarié. *Revue droit du travail Dalloz*, (6), 2014. pp. 396–402.

Loiseau 2017 = Loiseau, Grégoire: La déconnexion-Observations sur la régulation du travail dans le nouvel espace-temps des entreprises connectées. *Droit social*, (5), 2017. pp. 463–470.

Loiseau 2018 = Loiseau, Grégoire: La CEDH valide la jurisprudence de la Chambre sociale. *La Semaine Juridique Social*, (12), 2018. pp. 30–37.

Loiseau 2018a = Loiseau, Grégoire: Réseaux sociaux et abus de la liberté d'expression : l'exception de cercle privé. *La Semaine Juridique Social*, (41), 2018. pp. 22–25.

Lory 2010 = Lory, Beth E. H.: Using Facebook to Assess Candidates During the Recruiting Process: Ethical Implications. *NACE Journal*, 71(1), 2010. pp. 37–40.

Lynskey 2014 = Lynskey, Orla: Deconstructing Data Protection: the "Added-Value" of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly*, 63(3), 2014. pp. 569–597.

Lynskey 2015 = Lynskey, Orla: *The Foundations of EU Data Protection Law*. Oxford University Press, Oxford, 2015

Lyon-Caen 1992 = Lyon-Caen, Gérard: *Les libertés publiques et l'emploi*. La Documentation française (Collection des rapports officiels), Paris, 1992

Lyon-Caen 2001 = Lyon-Caen, Gérard: Débat autour de l'arrêt Nikon France. *Semaine sociale Lamy*, (1046), 2001. pp. 8–11.

Lyon-Caen 2014 = Lyon-Caen, Antoine: Libertés et contrôle dans l'entreprise. 20 ans après. *Revue droit du travail Dalloz*, (6), 2014. pp. 386–390.

Madden 2012 = Madden, Mary: *Privacy management on social media sites*. Pew Research Center. 2012. Available at:http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf (Accessed: 21 May 2018)

Majtényi 2006 = Majtényi, László: *Az információs szabadságok: adatvédelem és a közérdekű adatok nyilvánossága*. Complex, Budapest, 2006

Majtényi 2008 = Majtényi, László: *Az információs jogok*. In: Halmai, Gábor – Tóth, Gábor Attila (eds): Emberi jogok. Osiris Kiadó, Budapest, 2008. pp. 577–610.

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

Mandl – Biletta 2018 = Mandl, Irene – Biletta, Isabella: *Overview of new forms of employment – 2018 update*. Publications Office of the European Union, Luxembourg: Eurofound, 2018

Mandl et al. 2015 = Mandl, Irene *et al*.: *New forms of employment*. Publications Office of the European Union, Luxembourg: Eurofound, 2015

Marchadier 2018 = Marchadier, Fabien: La protection des données informatiques stockées sur l'ordinateur professionnel du salarié à titre du droit au respect de la vie privée. *JCP G Semaine Juridique (édition générale)*, (15), 2018. pp. 59–63.

Marguénaud – Mouly 2017 = Marguénaud, Jean-Pierre – Mouly, Jean: De l'accès des salariés à Internet à la rationalisation de l'influence de la Cour EDH sur les relations individuelles du travail. *La Semaine Juridique – Édition Générale*, (44–45), 2017. pp. 1992–1996.

Mayaud 1998 = Mayaud, Yves: De la mise en cause diffamatoire d'une gestion municipale : l'enjeu de publicité. *Revue de science criminelle et de droit pénal comparé*, (1), 1998. pp. 104–105.

Mayer-Schönberger 1997 = Mayer-Schönberger, Viktor: *Generational Development of Data Protection in Europe*. In: Agre, Philip E. – Rotenberg, Marc (eds): Technology and Privacy: The New Landscape. MIT Press, Cambridge, 1997. pp. 219–241.

Mayer-Schönberger 2011 = Mayer-Schönberger, Viktor: *Delete – The Virtue of Forgetting in the Digital Age*. Princeton University Press, Princeton and Oxford, 2011

Mayoux 2018 = Mayoux, Sébastien: Licéité de la preuve recuillie sur Facebook par l'employeur. *Jurisprudence sociale Lamy*, (449), 2018. pp. 23–26.

Mazeaud 2015 = Mazeaud, Vincent: La constitutionnalisation du droit au respect de la vie privée. *Les Nouveaux Cahiers du Conseil constitutionnel*, (48) 2015. pp. 7–20.

Mazeaud 2014/2016 = Mazeaud Antoine: *Droit du travail*. LGDJ-Lextenso éditions (Domat Droit privé), Issy-les-Moulineaux, 2014/2016

McCullagh 2008 = McCullagh, Karen: Blogging: self presentation and privacy. *Information & Communications Technology Law*, 17(1), 2008. pp. 3–23.

Mélypataki – Rácz 2018 = Mélypataki, Gábor – Rácz, Zoltán: *A személyiségi jogok védelmének ütközése a munkajogban*. In: Auer, Ádám *et al*. (eds): Ünnepi kötet a 65 éves Kiss György tiszteletére – Liber Amicorum in honorem Georgii Kiss aetatis suae LXV. Dialóg Campus Kiadó, Budapest, 2018. pp. 677–684.

Mendel et al. 2013 = Mendel, Toby *et al.*: *Étude mondiale sur le respect de la vie privée sur l'Internet et la liberté d'expression*. Éditions Unesco (Collection Unesco sur la liberté de l'Internet), Paris, 2013

Mettling 2015 = Mettling, Bruno: *Transformation numérique et vie au travail*. 2015

Mgrditchian 2015 = Mgrditchian, Greg: Employment and Social Media Privacy: Employer Justifications for Access to "Private" Material. *Rutgers Computer & Technology Law Journal*, 41(1), 2015. pp. 108–133.

Michel 2016 = Michel, Alejandra: L'utilisation des contenus postés sur les réseaux sociaux comme éléments de preuve d'un dommage. *Revue du droit des technologies de l'information*, (65), 2016. pp. 94–112.

Michel 2018 = Michel, Stéphane: TIC et protection de la vie privée du salarié. *Bulletin Joly Travail*, (2), 2018. pp. 149–152.

Miholics 2015 = Miholics, Tivadar: Általános magatartási követelmények a munkaviszonyban. *Magyar jog*, 62(4), 2015. pp. 245–249.

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

Mills 2015 = Mills, Jon L.: *Privacy in the New Media Age*. University Press of Florida, Gainesville, 2015

Moderne 2012 = Moderne, Franck: *La Convention européenne des Droits de l'Homme*. 3rd edn. Dalloz, Paris, 2012

Molfessis 2004 = Molfessis, Nicolas: Vie professionnelle, vie personnelle et responsabilité des commettants du fait de leurs préposés. *Droit social*, (1), 2004. pp. 31–39.

Mooney 2010 = Mooney, Daniel E.: Employer on the Web Wire: Balancing the Legal Pros and Cons of Online Employee Screening *Idaho Law Review*, 46(3), 2010. pp. 733–761.

Moreira 2013 = Moreira, Teresa Coelho: The Digital To Be or Not To Be: Privacy of Employees and the Use of Online Social Networks in the Recruitment Process. *GSTF International Journal of Law and Social Sciences (JLSS)*, 2(2), 2013. pp. 76–80.

Moreira 2016 = Moreira, Teresa Coelho: The Electronic Control of the Employer in Portugal. *Labour & Law Issues*, 2(1), 2016. pp. 1–27.

Morgenroth 2016 = Morgenroth, Thomas: *La vie privée en droit du travail*. Doctoral dissertation. Université Lille 2 – Droit et Santé. 2016

Mouly 2012 = Mouly, Jean: *Droit du travail*. 6e édition. Bréal (Lexifac Droit), Rosny-sous-Bois, 2012

Nasom-Tissandier 2018 = Nasom-Tissandier, Hélène: L'importance de la charte informatique dans la justification de mesures de surveillance des salariés. *Jurisprudence sociale Lamy*, (451), 2018. pp. 12–14.

Ndior 2015 = Ndior, Valère: *Le réseau social : essai d'identification et de qualification*. In: Ndior, Valère (ed.): Droit et réseaux sociaux. Lextenso (Collection LEJEP), Issy-les-Moulineaux, 2015. pp. 7–37.

Németh 2013 = Németh, Janka: Az internet nem felejt – közösségi media-használatra alapított munkáltatói és munkavállalói felmondások. *Infokommunikáció és jog*, (2), 2013. pp. 96–98.

Németh 2013a = Németh, Janka: Internet és közösségi háló mint munkaeszköz. *Infokommunikáció és jog*, (1), 2013. pp. 37–41.

Netter 2015 = Netter, Emmanuel: *La liberté d'expression sur les réseaux sociaux en droit français.*, In: Ndior, Valère (ed.): Droit et réseaux sociaux. Lextenso (Collection LEJEP), Issy-les-Moulineaux, 2015. pp. 39–63.

Newell 2011 = Newell, Bryce Clayton: Rethinking Reasonable Expectations of Privacy in Online Social Networks. *Richmond Journal of Law and Technology*, 17(4), 2011. pp. 1–62.

Niel 2007 = Niel, Sylvain: Elaborer une charte informatique. *Les cahiers du DRH*, (130), 2007. pp. 37–45.

Nissenbaum 1998 = Nissenbaum, Helen: Protecting Privacy in an Information Age: the Problem of Privacy in Public. *Law and Philosophy*, 17(5–6), 1998. pp. 559–596.

Nivelles 2014 = Nivelles, Vanessa: Les entreprises à l'épreuve des réseaux sociaux. *Jurisprudence Sociale Lamy*, (377–378), 2014. pp. 9–13.

North 2010 = North, Evan E.: Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites. *Kansas Law Review*, 58(5), 2010. pp. 1279–1309.

Nyman-Metcalf 2014 = Nyman-Metcalf, Katrin: *The Future of Universality of Rights*. In: Kerikmäe, Tanel (ed.): Protecting Human Rights in the EU. Controversies and Challenges of the Charter of Fundamental Rights. Springer, Heidelberg, 2014. pp. 21–36.

Otto 2016 = Otto, Marta: *The Right to Privacy in Employment: a Comparative Analysis*. Hart Publishing, Oxford, Portland, 2016

Ouaissi 2017 = Ouaissi, Haïba: *Droit du travail : de l'individuel au collectif*. 2nd edn. Bruylant, Bruxelles, 2017

Pailler 2012 = Pailler, Ludovic: *Les réseaux sociaux sur internet et le droit au respect de la vie privée*. Larcier, Bruxelles, 2012

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

Parker 1974 = Parker, Richard B.: A Definition of Privacy. *Rutgers Law Review*, 27(2), 1974. pp. 275–297.

Péano 1995 = Péano, Marie-Annick: L'intuitus personae dans le contrat de travail. *Droit social*, (2), 1995. pp. 129–138.

Peck 2012 = Peck, Stephanie: *Social media, monitoring and surveillance at work – a practical guide for trade unionists*. LRD Publ. (Labour Research Department Booklets), London, 2012

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

Péronne – Daoud 2018 = Péronne, Géraldine – Daoud, Emmanuel: Accès par l'employeur au compte Facebook du salarié et droit à la vie privée. *Dalloz IP/IT*, (5), 2018. pp. 315–316.

Perraki 2015 = Perraki, Panagiota: *La protection de la vie personnelle du salarié en droit comparé et européen : étude comparative des droits français, hellénique, britannique et européen*. L'Harmattan, Paris, 2015

Persson – Hansson 2003 = Persson, Anders J. – Hansson, Sven Ove: Privacy at Work – Ethical Criteria. *Journal of Business Ethics*, 42(1), 2003. pp. 59–70.

Peskine – Wolmark 2016 = Peskine, Elsa – Wolmark, Cyril: *Droit du travail*. 11th edn. Dalloz (Hypercours Dalloz cours & travaux dirigés), Paris, 2016

Pete 2018 = Pete, Éva: *A munkavállaló és a munkáltató személyiségi jogainak védelme a munkaviszonyban*. In: Mailáth György Tudományos Pályázat 2017. Díjazott dolgozatok. Országos Bírósági Hivatal, Budapest, 2018. pp. 768–807.

Péterfalvi – Révész – Buzás 2018 = Péterfalvi, Attila – Révész, Balázs – Buzás, Péter (eds): *Magyarázat a GDPR-ról*. Wolters Kluwer Hungary, Budapest, 2018

Péterfalvi 2012 = Péterfalvi, Attila (ed.): *Adatvédelem és információszabadság a mindennapokban*. HVG–ORAC, Budapest, 2012

Péterfalvi 2014 = Péterfalvi, Attila: Személyiségi jogok – adatvédelem – információszabadság. *Magyar jog*, 61(9), 2014. pp. 486–489.

Petit 2011 = Petit, Franck: *Droits des contrats de travail*. Gualino, Paris, 2011

Petrik 2014 = Petrik, Ferenc: *Személyiségi jogok*. In: Wellmann, György (ed.): Polgári jog: Bevezető és záró rendelkezések. Az ember mint jogalany. Öröklési jog. 2nd edn. HVG–ORAC Lap- és Könyvkiadó, 2014. pp. 166–211.

Pettiti – Decaux – Imbert 1995 = Pettiti, Louis-Edmond – Decaux, Emmanuel – Imbert, Pierre-Henri (eds): *La Convention Européenne des Droits de l'Homme, commentaire article par article*. Economica, Paris, 1995

Peyronnet 2017 = Peyronnet, Marie: CEDH : la protection réaffirmée de la vie privée du salarié sur internet. CEDH 5 sept. 2017, Bărbulescu c. Roumanie, req. n° 61496/08. *Dalloz actualité*, 2017

Picq 2011 = Picq, Marielle: Facebook et les salariés : vie privée, liberté d'expression et humour. *Revue des droits et libertés fondamentaux*, (11) 2011

Pierroux 2015 = Pierroux, Emmanuèle: Facebook, Twitter et autres résaux sociaux: petites injures entres “amis”. *La Gazette du Palais*, (336–337), 2015. pp. 4–8.

Pizzio-Delaporte 2001 = Pizzio-Delaporte, Corinne: Libertés fondamentales et droits du salarié le rôle du juge. *Droit Social*, (4), 2001. pp. 404–412.

Plasschaert 2017 = Plasschaert, Emmanuel: *La licéité du traitement de données personnelles du travailleur au regard du nouveau Règlement (UE) n° 2016/679 sur la protection des données*. In: Ragheno, Natalie (ed.): Data protection & privacy: le GDPR dans la pratique. Anthemis, Limal, 2017. pp. 105–118.

Pók 2012 = Pók, László: A közösség hálójában – Közösségi oldalak munkajogi vonatkozásai. *Infokommunikáció és jog*, (1), 2012. pp. 10–17.

Pók 2012a = Pók, László: Lájkolni szabad? Munkavállalói véleménynyilvánítás az új Munka Törvénykönyve tükrében. *Infokommunikáció és jog*, (4), 2012. pp. 160–165.

Polefkó 2011 = Polefkó, Patrik: Barátok és bizonytalanságok közt (5. rész) : avagy a közösségi oldalakról adatvédelmi szemszögből. *Infokommunikáció és jog*, (44), 2011. pp. 109–110.

Porta et al. 2018 = Porta, Jérôme *et al.*: Libertés fondamentales, égalité de traitement et discrimination. *Bulletin d’information de la Cour de Cassation*, (887), 2018. pp. 15–18.

Posner 1978 = Posner, Richard. A.: The Right of Privacy. *Georgia Law Review*, 12(3), 1978. pp. 393–422.

Post 2001 = Post, Robert C.: Three Concepts of Privacy. *Georgetown Law Journal*, 89(6), 2001. pp. 2087–2098.

Pottecher – Bakhtiari 2016 = Pottecher, Marie-Claire – Bakhtiari, Zartoshte: Travailler ou tweeter, le salarié n’a pas (forcément) à choisir. *Cahiers sociaux du Barreau de Paris*, (285), 2016. pp. 233–234.

Poullet 2005 = Poullet, Yves: Pour une troisième génération de réglementations de protection des données. *Jusletter*. 2005. Available at: http://www.crid.be/pdf/public/5188.pdf (Accessed: 24 February 2018)

Proskauer Rose LLP 2014 = Proskauer Rose LLP: *Social Media in the Workplace Around the World 3.0. 2013/14 Survey*. 2014. Available at: http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf (Accessed: 3 February 2017)

Prosser 1960 = Prosser, William L.: Privacy. *California Law Review*, 48(3), 1960. pp. 383–423.

Prugberger 2011 = Prugberger, Tamás: A munkaszerződés és a munkaviszonyból származó alapvető jogok és kötelezettségek a Munka Törvénykönyvének rekodifikációs tervezetében. *Gazdasági élet és társadalom*, (1–2), 2011. pp. 269–288.

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

Qi – Edgar-Nevill 2011 = Qi, Man – Edgar-Nevill, Denis: Social networking searching and privacy issues. *Information Security Technical Report*, 16(2), 2011. pp. 74–78.

Rácz 2015 = Rácz, Ildikó: *A közösségi média használatának árnyoldalai a munkaviszonyban*. In: Deres, Petronella – Grad-Gyenge, Anikó (eds): Acta Iuvenum Caroliensia VII. Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest, 2015. pp. 279–305.

Radé 2002 = Radé, Christophe: *Droit du travail*. 2nd edn. Montchrestien, Paris, 2002

Radnay 2003/2008 = Radnay, József: *Munkajog*. Szent István Társulat, Budapest, 2003/2008

Rátkai 2019 = Rátkai, Ildikó: Új adatvédelmi szabályok a munkaviszonnyal összefüggésben. *Munkajog*, (2), 2019. pp. 69–75. Available at: https://munkajogilap.hu/uj-adatvedelmi-szabalyok-a-munkaviszonnyal-osszefuggesben/ (Accessed: 12 August 2019)

Ray – Bouchet 2010 = Ray, Jean-Emmanuel – Bouchet, J.-P.: Vie professionnelle, vie personnelle et technologies d'information et de communication. *Droit social*, (1), 2010. pp. 44–55.

Ray 1992 = Ray, Jean-Emmanuel: Nouvelles technologies et nouvelles formes de subordination. *Droit social*, (6), 1992, pp. 525–537.

Ray 1993 = Ray, Jean-Emmanuel: Une loi macédonienne ? Étude critique du V de la loi du 31 décembre 1992. « Dispositions relatives au recrutement et aux libertés individuelles ». *Droit social*, (2), 1993. pp. 103–114.

Ray 2001 = Ray, Jean-Emmanuel: *Le droit du travail à l'épreuve des NTIC*. Liaisons, Rueil-Malmaison, 2001

Ray 2001a = Ray, Jean-Emmanuel: *Le droit du travail à l'épreuve des NTIC*. 2nd edn. Liaisons, Rueil-Malmaison, 2001

Ray 2007 = Ray, Jean-Emmanuel: Actualités des TIC. *Droit social*, (9–10), 2007. pp. 951–961.

Ray 2009 = Ray, Jean-Emmanuel: Actualité des TIC (II). Rapports collectifs de travail. *Droit social*, 1, 2009. pp. 22–37.

Ray 2010 = Ray, Jean-Emmanuel: D'un droit des travailleurs aux droits de la personne au travail. *Droit social*, (1), 2010. pp. 3–11.

Ray 2010a = Ray, Jean-Emmanuel: Little Brothers are watching you. *Semaine sociale Lamy*, 1470, 2010. pp. 10–13.

Ray 2011 = Ray, Jean-Emmanuel: Facebook, le salarié et l'employeur. *Droit social*, (2), 2011. pp. 128–140.

Ray 2012 = Ray, Jean-Emmanuel: A propos de la révolution numérique. Actualités des TIC (mai-septembre 2012). *Droit social*, (10), 2012. pp. 934–939.

Ray 2013 = Ray, Jean-Emmanuel: Facebook, espace public plus que privé. A propos de l'arrêt de la 1 ère Chambre civile du 10 avril 2013. *Semaine sociale Lamy*, (1599), 2013. pp. 14–19.

Ray 2015 = Ray, Jean-Emmanuel: Actualité des TIC. Tous connectés, partout, tout le temps ? *Droit social*, (6), 2015. pp. 516–527.

Ray 2017 = Ray, Jean-Emmanuel: *Droit du travail: droit vivant*. Wolters Kluwer France, Paris, 2017

Ray 2018 = Ray, Jean-Emmanuel: Des "licenciements Facebook" à la sanction d'un "Like" ?. *Semaine sociale Lamy*, (1830), 2018. pp. 10–12.

Ray 2018a = Ray, Jean-Emmanuel: *Droit du travail: droit vivant*. Wolters Kluwer France, Paris, 2018

Retzer – Lopatowska 2011 = Retzer, Karin – Lopatowska, Joanna: *How to Monitor Workplace E-Mail and Internet in Europe: The Polish Perspective*. Privacy & Security Law Report, Bureau of National Affairs. 2011

Rey 2012 = Rey, Bénédicte: *La vie privée à l'ère du numérique*. Lavoisier, Bénédicte, 2012

Rey 2013 = Rey, Bénédicte: 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), 2013. pp. 105–136.

Richard 2016 = Richard, Jacky: Le numérique et les données personnelles : quels risques, quelles potentialités ? *Revue du Droit public (RDP)*, 1, 2016. pp. 87–100.

Richard de la Tour 1999 = Richard de la Tour, Jean: *La vie personnelle du salarié. Étude sur la jurisprudence récente de la Chambre sociale de la Cour de cassation*. Cour de cassation, 1999

Rigaux 1991 = Rigaux, M. François: La liberté de la vie privée. *Revue internationale de droit comparé*, 43(3), 1991. pp. 539–563.

Rijckaert – Lambert 2012 = Rijckaert, Olivier – Lambert, Noël: *Le respect de la vie privée dans la relation de travail*. Wolters Kluwer Belgium, Waterloo, 2012

Rivero – Savatier 1978 = Rivero, Jean – Savatier, Jean: *Droit du travail*. Presses Universitaires de France, Paris, 1978

Rivero 1982 = Rivero, Jean: Les libertés publiques dans l'entreprise. *Droit social*, (5), 1982. pp. 421–424.

Rouvroy – Poullet 2009 = Rouvroy, Antoinette – Poullet, Yves: *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*. In: Gutwirth, Serge *et al*. (eds): Reinventing Data Protection? Springer, 2009. pp. 45–76.

Rózsavölgyi 2018 = Rózsavölgyi, Bálint: Mikor lehet jogszerű a munkáltató ellenőrzése? – az Emberi Jogok Európai Bírósága Nagykamarája Bărbulescu kontra Románia ügyben hozott ítéletének iránymutatásai. *Munkajog*, 2(1), 2018. pp. 43–48.

Rücker – Kugler 2018 = Rücker, Daniel – Kugler, Tobias (eds): *New European General Data Protection Regulation. A Practitioner's Guide*. C.H. Beck, Hart, Nomos, München, Oxford, Baden-Baden, 2018

Rustad – Paulsson 2005 = Rustad, Michael L. – Paulsson, Sandra R.: Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe. *U. Pa. Journal of Labor and Employment Law*, 7(4), 2005. pp. 829–904.

Saint-Pau 2016 = Saint-Pau, Jean-Christophe: *Art. 9 – Fasc. 10 : Jouissance des droits civils. – Droit au respect de la vie privée. – Définition conceptuelle du droit subjectif*. JurisClasseur Civil Code, 2016

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

Sanders 2013 = Sanders, Amy Kristin: *Obscenity, Sexting, and Cyberbullying*. In: Stewart, Daxton R. (ed.): Social Media and the Law. A Guidebook for Communication Students and professionals. Routledge, New York, London, 2013. pp. 156–174.

Sári – Somody 2008 = Sári, János – Somody, Bernadette: *Alapjogok*. Osiris Kiadó, Budapest, 2008

Savatier 1992 = Savatier, Jean: La protection de la vie privée des salariés. *Droit social*, (4), 1992. pp. 329–336.

Schabas 2015 = Schabas, William A.: *The European Convention on Human Rights: a Commentary*. Oxford University Press, Oxford, 2015

Schoeman 2007 = Schoeman, Ferdinand D.: *Privacy: philosophical dimensions of the literature*. In: Schoeman, Ferdinand D. (ed.): Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, Cambridge, 2007. pp. 1–33.

Schultis 2017 = Schultis, Catherine: Le traitement de données dans le cadre des relations de travail dans le règlement sur la protection des données personnelles. *Dalloz IP/IT*, (5), 2017. pp. 265–267.

Schwartz 1989 = Schwartz, Paul: The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. *The American Journal of Comparative Law*, 37(4), 1989. pp. 675–701.

Shapiro 1985 = Shapiro, Fred R.: The Most-Cited Law Review Articles. *California Law Review*, 73(5), 1985. pp. 1540–1554.

Shih 2011 = Shih, Clara: *A Facebook kora*. Kiskapu Kiadó, Budapest, 2011

Simitis 1995 = Simitis, Spiros: From the Market to the Polis: The EU Directive on the Protection of Personal Data. *Iowa Law Review*, 80(3), 1995. pp. 445–470.

Simitis 1998 = Simitis, Spiros: From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union. *Comparative Labor Law and Policy Journal*, 19(3), 1998. pp. 351–372.

Simitis 1999 = Simitis, Spiros: Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data. *European Law Journal*, 5(1), 1999. pp. 45–62.

Simitis 2010 = Simitis, Spiros: Privacy – An Endless Debate. *California Law Review*, 98(6), 2010. pp. 1989–2006.

Simms 1994 = Simms, Michele: Defining Privacy in Employee Health Screening Cases: Ethical Ramifications Concerning the Employee/Employer Relationship. *Journal of Business Ethics*, 13(5), 1994. pp. 315–325.

Simon 2005 = Simon, Éva: Egy XIX. századi tanulmány margójára. *Információs Társadalom*, (2), 2005. pp. 32–43.

Sipka – Zaccaria 2018 = Sipka, Péter – Zaccaria, Márton Leó: A munkáltató ellenőrzési joga a munkavállaló munkahelyi számítógépén tárolt magánadatai fölött. *Munkajog*, 2(2), 2018. pp. 45–49.

Síthigh 2008 = Síthigh, Daithí Mac: The mass age of internet law. *Information & Communications Technology Law*, 17(2), 2008. pp. 79–94.

Smith-Butler 2009 = Smith-Butler, Lisa: Workplace Privacy: We'll Be Watching You. *Ohio Northern University Law Review*, 35(1), 2009. pp. 53–81.

Solomon 2012 = Solomon, Lafe E.: *Memorandum OM 12-59*. Office of the General Counsel Division of Operations-Management. 2012. Available at: http://www.rc.com/documents/OM1259ActingGeneralCounselReportConcerningSocialMediaCases.pdf (Accessed: 30 November 2018)

Solove 2002 = Solove, Daniel J.: Conceptualizing Privacy. *California Law Review*, 90(4), 2002. pp. 1087–1156.

Solove 2007 = Solove, Daniel J.: *The Future of Reputation. Gossip, Rumor, and Privacy on the Internet*. Yale University Press, New Haven and London, 2007

Solove 2011 = Solove, Daniel J.: *Nothing to hide: the false tradeoff between privacy and security*. Yale University Press, New Haven & London, 2011

Solove 2013 = Solove, Daniel J.: Introduction: Privacy-Self Management and the Consent Dilemma. *Harward Law Review*, 126(7), 2013. pp. 1880–1903.

Sólyom 1983 = Sólyom, László: *A személyiségi jogok elmélete*. Közgazdasági és Jogi Könyvkiadó, Budapest, 1983

Sólyom 1988 = Sólyom, László: Adatvédelem és személyiségi jog. *Világosság*, 29(1), 1988. pp. 53–60.

Sólyom 2001 = Sólyom, László *Az alkotmánybíráskodás kezdetei Magyarországon*. Osiris Kiadó, Budapest, 2001

Sordet 2010 = Sordet, Emmanuel: Facebook, néfaste pour la vie privée (des salariés) ? *JCP G Semaine Juridique (édition générale)*, (48), 2010. pp. 2228–2228.

Sprague 2008 = Sprague, Robert: Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees. *The John Marshall Law Review*, 42(1), 2008. pp. 83–135.

Sprague 2008a = Sprague, Robert: Rethinking Information Privacy in an Age of Online Transparency. *Hofstra Labor & Employment Law Journal*, 25(2), 2008. pp. 395–417.

Sprague 2011 = Sprague, Robert: Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship. *University of Louisville Law Review*, 50(1), 2011. pp. 1–34.

Stroud 2008 = Stroud, Dick: Social networking: An age-neutral commodity — Social networking becomes a mature web application. *Journal of Direct, Data and Digital Marketing Practice*, 9(3), 2008. pp. 278–292.

Suder 2014 = Suder, Seili: Pre-Employment Background Checks on Social Networking Sites – May Your Boss Be Watching? *Masaryk University Journal of Law and Technology*, 8(1), 2014. pp. 123–136.

Sudre 2015 = Sudre, Frédéric: *La Convention européenne des droits de l'homme*. 10th edn. Presses Universitaires de France, Paris

Sudre 2018 = Sudre, Frédéric: La « vie privée » dans un contexte professionnel. *La Semaine Juridique Edition Générale*, (41), 2018. pp. 1054–1055.

Sulyok 2017 = Sulyok, Márton: *Magánszféravédelem a tisztességes eljárásban – Az alapjogsértő bizonyítás összehasonlító alkotmányjogi vizsgálata*. Doctoral dissertation. Szegedi Tudományegyetem, 2017

Supiot 2000 = Supiot, Alain: Les nouveaux visages de la subordination. *Droit social*, (2), 2000. pp. 131–145.

Supiot 2002 = Supiot, Alain: *Critique du droit du travail*. Presses universitaires de France, Paris, 2002

Szabó – Székely 2005 = Szabó, Máté Dániel – Székely, Iván: *A privacy védelme a munkahelyen*. In: Szabó, Máté Dániel – Székely, Iván (eds): Szabad adatok, védett adatok. BME GTK ITM, Budapest, 2005. pp. 115–48.

Szabó 2004 = Szabó, Máté Dániel: „Erős jogvédő szemlélettel, de a törvényi felhatalmazás keretein belül kell dolgoznunk." Péterfalvi Attila adatvédelmi biztossal Szabó Máté Dániel beszélget. *Fundamentum*, VIII(4), 2004. pp. 37–43.

Szabó 2005 = Szabó, Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. *Információs Társadalom*, (2), 2005. pp. 44–54.

Szabó 2008 = Szabó, Máté Dániel: *Nyilvános magánszféra – Hol a határ*? In: Dezső, Márta – Kukorelli, István (eds): Ünnepi kötet Sári János egyetemi tanár 70. születésnapja tiszteletére. Rejtjel Kiadó, Budapest, 2008. pp. 329–341.

Szabó 2010 = Szabó, Endre Győző: *A személyes adatok védelmének kérdései a virtuális világban*. In: Talyigás, Judit (ed.): Az internet a kockázatok és a mellékhatások tekintetében. Scolar Kiadó, Budapest, 2010. pp. 43–65.

Székely 2010 = Székely, Iván: *Kukkoló társadalom – avagy van-e még függöny virtuális ablakunkon?* In: Talyigás, Judit (ed.): Az internet a kockázatok és a mellékhatások tekintetében. Scolar Kiadó, Budapest, 2010. pp. 93–120.

Szekfü 2007 = Szekfü, András: *Kommunikáció, nyilvánosság, esélyegyenlőség Magyarországon: a távírótól a Web 2.0-ig*. Gondolat, MTA–ELTE Kommunikációelméleti Kutatócsoport, Budapest, 2007

Szőke 2012 = Szőke, Gergely László (ed.): *Privacy in the workplace. Data protection law and self-regulation in Germany and in Hungary*. HVG–ORAC Lap- és Könyvkiadó, Budapest, 2012

Szőke 2013 = Szőke, Gergely László: Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*, (3), 2013. pp. 107–112.

Szőke 2015 = Szőke, Gergely László: *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*. HVG–ORAC, Budapest, 2015

Szőke et al. 2012 = Szőke, Gergely László *et al.*: *Munkahelyi adatvédelem. Nemzeti jelentés – Magyarország*. 2012. Available at: http://pawproject.eu/en/sites/default/files/page/web_national_report_hungary_hu.pdf (Accessed: 21 October 2016)

Szűcs 2013 = Szűcs, Péter: *A munka törvénykönyve, 2012–1992*. CompLex, Budapest, 2013

Szüts – Karsai – Mándi 2006 = Szüts, Korinna – Karsai, Dániel – Mándi, Gábor: *Az Alkotmánybíróság egyes határozatainak ismertetése*. Rejtjel Kiadó, Budapest, 2006

Szűts 2015 = Szűts, Zoltán: A munka világának online kommunikációs kérdései. *Opus et Educatio*, 2(2), 2015. pp. 26–30.

Tene 2011 = Tene, Omar: Privacy: The new generations. *International Data Privacy Law*, 1(1), 2011. pp. 15–27.

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

Teyssié 1988 = Teyssié, Bernard: Personnes, entreprises et relations de travail. *Droit social*, (5), 1988. pp. 374–383.

Thompson 2007 = Thompson, Bill: The Breaking Wave: New Law for a Wired World? *International Review of Law, Computers & Technology*, 21(3), 2007. pp. 221–223.

Thornthwaite 2016 = Thornthwaite, Louise: Chilling times: social media policies, labour law and employment relations. *Asia Pacific Journal of Human Resources*, 54(3), 2016. pp. 332–351.

Tissot 1995 = Tissot, Olivier: La protection de la vie privée du salarié. *Droit social*, (3), 1995. pp. 222–230.

Tobok 2013 = Tobok, Daniel: *Social Network Recruiting: Implications of this New Hiring Model*. In: Law Society of Upper Canada: Employment law and the new workplace in the social media age. Irwin Law, Toronto, 2013. pp. 95–99.

Towner 2016 = Towner, Nathalie: *Social media at work. A practical guide for trade union reps*. LRD Publications (Labour Research Department Booklets), London, 2016

Tricoit 2013 = Tricoit, Jean-Philippe: Recrutement, rupture du contrat de travail et TIC. *La Semaine Juridique Social*, (40), 2013. pp. 9–14.

Tshilembe 2015 = Tshilembe, Anne-Sophie: *Vie privée – protection des données personnelles du travailleur: la question de l'embauche*. In: Martin, Denis – Morsa, Marc – Gosseries, Philippe (eds): Droit du travail européen : questions spéciales. Éditions Larcier, Bruxelles, 2015. pp. 645–702.

Türk 2011 = Türk, Alex: *La vie privée en péril: des citoyens sous contrôle*. OJacob, Paris, 2011

Vallet 2012 = Vallet, Caroline: Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs. *Droit et société*, (1), 2012. pp. 163–188.

Van Eecke – Truyens 2010 = Van Eecke, Patrick – Truyens, Maarten: Privacy and social networks. *Computer Law and Security Review*, 26(5), 2010. pp. 535–546.

Vékás 2013 = Vékás, Lajos (ed.): *A Polgári Törvénykönyv magyarázatokkal*. Complex, Budapest, 2013

Velu – Ergec 2014 = Velu, Rusen – Ergec, Jacques: *Convention européenne des droits de l'homme*. Bruylant, Bruxelles, 2014

Verkindt 2010 = Verkindt, Pierre-Yves: Les "amis" de nos "amis"…*JCP S (édition sociale)*. (48), 2010. pp. 3–5.

Vickery – Wunsch-Vincent 2007 = Vickery, Graham – Wunsch-Vincent, Sacha: *Participative Web and User-Created Content. Web 2.0, Wikis and Social Networking*. OECD Publishing, 2007

Vigneau 2002 = Vigneau, Christophe: Information Technology and Workers' Privacy: the French Law. *Comparative Labor Law & Policy Journal*, 23(2), 2002. pp. 351–376.

Vigneau 2006 = Vigneau, Christophe: *Protection of personal data (Article 8)*. In: Bercusson, Brian (ed.): European Labour Law and the EU Charter of Fundamental Rights. Nomos, Baden-Baden, 2006, pp. 115–131.

Vissy 2015 = Vissy, Beatrix: *Az információs önrendelkezési jog*. In: Pozsár-Szentmiklósy, Zoltán – Somody, Bernadette (eds): Alkotmányos alapok. 2nd edn. HVG–ORAC Lap- és Könyvkiadó, Budapest, pp. 200–207.

Voigt – von dem Bussche 2017 = Voigt, Paul – von dem Bussche, Axel: *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Springer, 2017

Waquet – Struillou – Pécaut-Rivolier 2014 = Waquet, Philippe – Struillou, Yves – Pécaut-Rivolier, Laurence: *Pouvoirs du chef d'entreprise et libertés du salarié: du salarié-citoyen au citoyen-salarié*. ÉdLiaisons, Rueil-Malmaison, 2014

Waquet 1994 = Waquet, Philippe: Vie professionnelle et vie personnelle du salarié. *Cahier Sociaux du Barreau de Paris*, (64), 1994. pp. 289–292.

Waquet 2001 = Waquet, Philippe: *La vie personnelle du salarié*. In: Droit syndical et droits de l'homme à l'aube du XXIe siècle : mélanges en l'honneur de Jean-Maurice Verdier. Dalloz, Paris, 2001. pp. 513–524.

Waquet 2002 = Waquet, Philippe: Retour sur l'arrêt Nikon. *Semaine sociale Lamy*, (1065), 2002. pp. 5–10.

Waquet 2003 = Waquet, Philippe: *L'entreprise et les libertés du salarié*. Editions Liaisons, Paris, 2003

Waquet 2004 = Waquet, Philippe : La vie personnelle du salarié. *Droit social*, (1), 2004. pp. 23–30.

Waquet 2006 = Waquet, Philippe: Le "trouble objectif dans l'entreprise" : une notion à redéfinir. *Revue droit du travail Dalloz*, (5), 2006. pp. 304–310.

Warren – Brandeis 1890 = Warren, Samuel D. – Brandeis, Louis D.: The Right to Privacy. *Harvard Law Review*, 4(5), 1890. pp. 193–220.

Warren – Pedowitz 2011 = Warren, Marisa – Pedowitz, Arnie: (Social Media, Trade Secrets, Duties of Loyalty, Restrictive Covenants and Yes, the Sky is Falling. *Hofstra Labor and Employment Law Journal*, 29(1), 2011. pp. 99–114.

Weir – Toolan – Smeed 2011 = Weir, George R.S. – Toolan, Fergus – Smeed, Duncan: The threats of social networking: Old wine in new bottles? *Information Security Technical Report*, 16(2), 2011. pp. 38–43.

Westin 2003 = Westin, Alan F.: Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 2003. pp. 431–453.

Wilkens et al. 2018 = Wilkens, Mathijn *et al.*: *Striking a balance: Reconciling work and life in the EU*. Publications Office of the European Union, Luxembourg: Eurofound, 2018

Wolton – Pompey 2013 = Wolton, Elise – Pompey, Sébastien: Données à caractère personnel et droit du travail. *Revue de Jurisprudence Sociale (RJS)*, (4), 2013. pp. 215–220.

Wong 2012 = Wong, Rebecca: The Data Protection Directive 95/46/EC: Idealisms and realisms. *International Review of Law, Computers & Technology*, 26(2–3), 2012. pp. 229–244.

Zaccaria 2016 = Zaccaria, Márton Leó: Munkavállalók a világhálón – "Megosztani ér?" *HR & Munkajog*, 7(10), 2016. pp. 14–17.

Online (press) articles, blog entries, statistics

http://arsboni.hu/kozossegi-media-es-munkajog-kereszttuzeben/ (27 February 2018)

http://hvg.hu/tudomany/20041203interhist (22 September 2017)

http://munkajogportal.hu/felmondhatunk-a-munkavallalonak-egy-facebook-bejegyzes-miatt/ (27 May 2017)

http://munkajogportal.hu/mik-azok-a-munkajogi-alapelvek-es-mire-valok/ (6 September 2018)

http://rabble.ca/columnists/2012/10/employees-beware-perils-posting-facebook (11 May 2018)

http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (28 February 2018)

http://www.cbc.ca/news/canada/british-columbia/delta-hockey-coach-christopher-sandau-fired-over-nazi-posts-on-facebook-1.2825623 (3 May 2018)

http://www.cbc.ca/news/canada/montreal/depressed-woman-loses-benefits-over-facebook-photos-1.861843 (3 May 2018)

http://www.cil.cnrs.fr/CIL/spip.php?article1954 (1 October 2018)

http://www.dailymail.co.uk/news/article-4950268/Even-teenagers-growing-tired-social-media.html (10 November 2017)

http://www.danah.org/papers/talks/2011/PDF2011.html (28 February 2017)

http://www.e-marketing.fr/Definitions-Glossaire/ATAWAD-240581.htm ; (11 May 2018)

http://www.huffingtonpost.com/fauzia-burke/social-media-vs-social-ne_b_4017305.html%202017%2002%2027 (22 September 2017)

http://www.ilo.org/global/about-the-ilo/how-the-ilo-works/departments-and-offices/governance/labour-law/judges/lang--en/index.htm (1 May 2018)

http://www.internetworldstats.com/emarketing.htm (16 December 2016)

http://www.nbcnews.com/id/26167371/ns/us_news-life/t/burger-king-worker-fired-bathing-sink/#.XUgxoo4zbct (5 August 2019)

http://www.pordesresidential.com/wp-content/uploads/2010/11/1-19-2011-miami-herald-biz.pdf (10 March 2017)

http://www.seesa.co.za/whistle-blowing-on-social-media/ (22 April 2018)

http://www.socialmediatoday.com/social-business/peteschauer/2015-06-28/5-biggest-differences-between-social-media-and-social (22 September 2017)

http://www.sweeneyinc.com/files/benefits_preemployment_screening.pdf (3 May 2018)

https://444.hu/2015/09/10/kirugtak-a-tanitonot-aki-ket-hitler-kep-kozott-uzent-a-tankonyvekrol-a-facebookon/ (15 November 2018)

https://ado.hu/munkaugyek/a-csak-meg-ot-perc-munkajogi-kovetkezmenyei/ (7 January 2020)

https://ado.hu/munkaugyek/a-keses-ot-szankcioja/ (7 January 2020)

https://ado.hu/munkaugyek/facebook-szabalyzat-beleszolhat-a-munkaltato/ (15 November 2018)

https://adozona.hu/munkajog/Pert_nyert_az_ugyesz_akit_harom_Facebookpos_RUXHRH (9 January 2020)

https://allpryme.com/employee-privacy-laws/employee-privacy-laws/ (14 August 2019)

https://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm (20 January 2019)

https://blogs.harvard.edu/infolaw/2006/11/15/finnish-employers-cannot-google-applicants/ (2 July 2018)

https://business.lesechos.fr/directions-ressources-humaines/ressources-humaines/recrutement/030656487193-85-des-recruteurs-font-des-recherches-en-ligne-sur-les-candidats-314060.php (20 June 2019)

https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf (20 January 2019)

https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage (4 January 2018)

https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Information_and_communication_technology_(ICT) (25 October 2019)

https://econsultancy.com/personal-versus-professional-social-networks-infographic/ (13 August 2019)

https://edition.cnn.com/travel/article/easyjet-backless-seats-scli-gbr-intl/index.html (7 August 2019)

https://edps.europa.eu/data-protection/data-protection/glossary/b_en (20 January 2019

https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf (20 January 2019)

https://getbambu.com/blog/data/downtime-to-work-marketing-report/ (20 January 2019)

https://hbr.org/2018/05/employees-who-use-social-media-for-work-are-more-engaged-but-also-more-likely-to-leave-their-jobs (27 July 2019)

https://hrdailyadvisor.blr.com/2018/07/24/6-ways-introduce-digital-detox-employees-boost-productivity/ (8 January 2020)

https://hvg.hu/itthon/20130727_blikk_kirugas (22 November 2018)

https://index.hu/belfold/2015/09/28/lemondott_devecz_miklos_a_szegedi_egyetem_kancellarja/ (3 May 2018)

https://index.hu/belfold/2016/10/15/az_allasaba_kerult_hogy_a_facebookon_azt_irta_jo_iranyba_halad_a_szeker/ (15 November 2018)

https://index.hu/belfold/2019/05/10/facebook_per_ugyesz_ugyeszseg_kirugas_itelet/ (9 January 2020)

https://index.hu/belfold/2019/12/23/jogeros_vissza_kell_venni_a_facebook-posztjai_miatt_kirugott_ugyeszt/ (9 January 2020)

https://index.hu/tech/2012/01/04/banktitkot_sertett_egy_magyar_mikroblogger/ (7 September 2018)

https://index.hu/tech/cellanaplo/2009/12/09/kirugtak_a_twitterezo_vodafonost/ (5 November 2018)

https://jogaszvilag.hu/cegvilag/mit-jelent-munkara-kepes-allapotban-lenni/ (7 January 2020)

https://jogaszvilag.hu/szakma/a-kozossegi-media-hasznalata-munkaltatoi-szemmel/ (6 September 2018)

https://money.cnn.com/2017/05/31/technology/facebook-like-defamation-switzerland/ (15 October 2018)

https://nepszava.hu/1090759_kirugtak-facebook-posztja-miatt-aczel-endret (15 November 2018)

https://newsroom.fb.com/news/2012/03/protecting-your-passwords-and-your-privacy/ (13 August 2019)

https://www.adweek.com/digital/how-social-media-actually-boosts-efficiency-in-an-office-environment/ (27 July 2019)

https://www.awesomeinventions.com/fired-posting-on-facebook/ (30 July 2019)

https://www.bozemandailychronicle.com/news/city-requires-facebook-passwords-from-job-applicants/article_a9458e22-498a-5b71-b07d-6628b487f797.html (3 May 2018)

https://www.brandwatch.com/blog/47-facebook-statistics-2016/ (7 January 2017)

https://www.businessinsider.com/17-people-who-were-fired-for-using-facebook-2014-7 (30 July 2019)

https://www.californiabusinesslitigation.com/2013/05/high_school_teacher_files_an_a.html (3 May 2018)

https://www.cnil.fr/fr/10-conseils-pour-rester-net-sur-le-web (Accessed: 19 August 2018)

https://www.cnil.fr/fr/candidats-lemploi-protegez-votre-reputation-sur-le-web (Accessed: 19 August 2018)

https://www.cnil.fr/fr/cnil-direct/question/354 (Accessed: 21 December 2019)

https://www.cnil.fr/fr/le-reputation-en-questions-0 (Accessed: 4 April 2017)

https://www.cnil.fr/fr/les-operations-de-recrutement (Accessed: 20 June 2019)

https://www.cnil.fr/fr/maitriser-les-informations-publiees-sur-les-reseaux-sociaux (Accessed: 26 February 2017)

https://www.coe.int/en/web/european-social-charter (Accessed: 12 August 2019)

https://www.definitions-marketing.com/definition/atawad/ (15 May 2018)

https://www.droit-technologie.org/actualites/perdre-emploi-a-cause-dun-jaime-cest-possible/ (15 October 2018)

https://www.emarketer.com/Article/Instagram-Snapchat-Adoption-Still-Surging-US-UK/1016369 (10 November 2017)

https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/platform-work (13 August 2019)

https://www.euromedia.fr/public/2016/12/etude-olfeo-2016-realite-utilisation-web-au-bureau.pdf (20 January 2019)

https://www.ft.com/content/f6182bc8-85e4-11dc-b00e-0000779fd2ac (9 November 2017)

https://www.hrportal.hu/c/facebook-szabalyzat-a-mentoknel-van-apropoja-20120116.html (15 November 2018)

https://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf (3 May 2018)

https://www.lexology.com/library/detail.aspx?g=b03caa90-2830-4194-a967-6cceaa561e7e (17 July 2018)

https://www.merriam-webster.com/dictionary/social%20media (22 September 2017)

https://www.merriam-webster.com/dictionary/social%20networking (22 September 2017)

https://www.michaelpage.fr/sites/michaelpage.fr/files/Charte_rxseaux_sociaux_internet_vie_privxe_et_recrutement.pdf (13 August 2019)

https://www.mirror.co.uk/news/uk-news/dvla-worker-fired-using-facebook-1903697 (25 July 2019)

https://www.nytimes.com/2004/11/16/business/fired-flight-attendant-finds-blogs-can-backfire.html (11 May 2018)

https://www.nytimes.com/2006/02/19/fashion/sundaystyles/here-i-am-taking-my-own-picture.html (20 January 2019)

https://www.nytimes.com/2009/04/16/business/media/16dominos.html (3 May 2018)

https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html (11 May 2018)

https://www.socialintel.com/ (13 August 2019)

https://www.socialmediatoday.com/content/when-your-employees-go-too-far-social-media (11 May 2018)

https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (13 August 2019)

https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (4 January 2018)

https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (20 January 2019)

https://www.taylorwessing.com/globaldatahub/article-employee-monitoring-update.html (1 May 2018).

https://www.telegraph.co.uk/news/worldnews/europe/france/12179584/French-parents-could-be-jailed-for-posting-childrens-photos-online.html (30 November 2018)

https://www.theguardian.com/business/2018/nov/07/ryanair-sacks-six-cabin-crew-after-staged-photo-sleeping-on-malaga-airport-floor (19 November 2018)

https://www.theguardian.com/news/2015/feb/26/pics-or-it-didnt-happen-mantra-instagram-era-facebook-twitter (20 January 2019)

https://www.theguardian.com/technology/2015/feb/21/internet-shaming-lindsey-stone-jon-ronson (3 May 2018)

https://www.thewindowsclub.com/list-of-countries-that-have-banned-social-media-for-its-citizens (21 October 2019)

https://www.washingtonpost.com/lifestyle/style/more-employers-using-firms-that-check-applicants-social-media-history/2011/07/12/gIQAxnJYGI_story.html?noredirect=on&utm_term=.1506923db7c6 (16 August 2018)

https://www.washingtonpost.com/local/flipping-off-president-trump-has-changed-julibriskmans-life--and-exposed-our-divisions/2017/11/07/19efab02-c3f6-11e7-afe9-4f60b5a6c4a0_story.html (14 August 2019)

https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.2547f6e741d5 (15 October 2018)

https://www.xperthr.co.uk/law-reports/in-the-employment-tribunals-august-2010/104153/#gill (20 September 2018)

https://www.youtube.com/watch?v=qd3VV8Za04g&t=316s (16 April 2018)

https://www.youtube.com/watch?v=yb0yrdDOy0g (16 April 2018)

shorturl.at/bcuwG (5 August 2019)

Social media policies

Charte d'utilisation des réseaux/médias sociaux numériques IUT de Rennes. Available at: http://partages.univ-rennes1.fr/files/partages/Services/IUT_administration/Internet/doc/IUTrennesCharteRSN.pdf (Accessed: 21 March 2017)

Global Social Media Policy. Available at: http://www.dell.com/learn/uk/en/ukcorp1/corp-comm/social-media-policy?c=uk&l=en&s=corp (Accessed: 23 March 2017)

Social Media Guidelines for Canadian Red Cross Staff and Volunteers. Available at: http://www.redcross.ca/crc/documents/What-We-Do/Violence-Bullying/partners/social-media-guidelines-2013.pdf (Accessed: 19 March 2017)

Social Media Guidelines. Available at: https://www.orange.com/sirius/smg/FR_Guides_Medias_Sociaux.pdf (Accessed: 22 March 2017)

Social Media Policy. 2010. Available at: https://edit.doi.gov/sites/doi.gov/files/migrated/notices/upload/DOI-Social-Media-Policy-Final-Redacted.pdf (Accessed: 19 March 2017)

Social Media Policy. Available at: http://www.equestrian.org.au/sites/default/files/Social%20Media%20Policy.pdf (Accessed: 19 March 2017)

Social Media Policy. Available at: http://www.nvidia.co.uk/object/social-media-guidelines-uk.html (Accessed: 23 March 2017)

Volleyball Australia Social Media Policy. 2012. Available at: http://www.volleyballaustralia.org.au/_literature_152757/Social_Media_Policy (Accessed: 19 March 2017)

Legislative documents

International

United Nations:

- *Universal Declaration of Human Rights*, 1948
- *International Covenant on Civil and Political Rights*, 1966
- *Guidelines for the Regulation of Computerized Personal Data Files*. Adopted by General Assembly resolution 45/95 of 14 December 1990

ILO:

- *Protection of workers' personal data. An ILO code of practice*. International Labour Office, Geneva, 1997
- *Recommendation concerning the employment relationship*. (No. 198.) 95th ILC session, Geneva, 2006

OECD:

- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* 1980
- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – revised*, 2013

Council of Europe:

- *European Convention on Human Rights*, 1950
- *European Social Charter*, ETS No.035, 1961
- *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No.108, 1981
- *Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*. 1989
- *European Social Charter (revised)*, ETS No.163, 1996
- *The protection of privacy and personal data on the Internet and online media*. Resolution 1843 (2011)
- *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*, 2012
- *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 2015
- *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. CM/Inf(2018)15-final, Elsinore, Denmark, 2018

European Union:

- *Treaty on the Functioning of the European Union*
- *Charter of Fundamental Rights of the European Union* (2000)
- *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*. OJ L 281, 23/11/1995, p. 31–50
- *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*. OJ L 8, 12.1.2001, p. 1–22
- *Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time*. OJ L 299, 18.11.2003, p. 9–19
- *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)*. OJ L 119, 4.5.2016, p. 1–88

Article 29 Data Protection Working Party:

- *Opinion 8/2001 on the processing of personal data in the employment context*. 5062/01/EN/Final WP 48, 2001
- *Working document on the surveillance of electronic communications in the workplace*. 5401/01/EN/Final WP 55, 2002
- *Opinion 4/2007 on the concept of personal data*. 01248/07/EN WP 136, 2007
- *Opinion 5/2009 on online social networking*. 01189/09/EN WP 163, 2009
- *Opinion 15/2011 on the definition of consent*. 01197/11/EN WP187, 2011
- *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. 844/14/EN WP 217, 2014
- *Opinion 2/2017 on data processing at work*. 17/EN WP 249, 2017

National

France

- Code du travail
- Code civil
- Code pénal
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n°82-689 du 4 août 1982 relative aux libertés des travailleurs dans l'entreprise

- Loi n° 92-1446 du 31 décembre 1992 relative à l'emploi, au développement du travail à temps partiel et à l'assurance chômage
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

Hungary

- Fundamental Law of Hungary (2011)
- Act XX of 1949 on the Constitution of the Hungarian Republic
- Act XXII of 1992 on the Labour Code
- Act XXXIII of 1992 on the Legal Status of Public Servants
- Act LXIII of 1992 on the protection of personal data and access to data of public interest
- Act XCIII of 1993 on labour safety
- Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information
- Act I of 2012 on the Labour Code
- Act C of 2012 on the Penal Code
- Act V of 2013 on the Civil Code
- Act LIII of 2018 on the protection of private life
- 50/1999. (XI. 3) decree of the Ministry of Health on the minimum health and safety requirements for work with display screen
- *T/4786. számú törvényjavaslat a Munka Törvénykönyvéről* (2011). Előadó: Dr. Matolcsy György nemzetgazdasági miniszter. Budapest
- *T/332. számú javaslat Magyarország Alaptörvényének hetedik módosítása* (2018). Előadó: Dr. Trócsányi László igazságügyi miniszter. Budapest
- *T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról* (2019). Előadó: Dr. Trócsányi László igazságügyi miniszter. Budapest
- Az Egyenlő Bánásmód Tanácsadó Testület 1/2007. TT. sz. állásfoglalása az állásinterjún feltehető munkáltatói kérdésekről

Court cases

International

Court of Justice of the European Union

- *Union de Recouvrement des Cotisations de Sécurité Sociale et d'Allocations Familiales de la Savoie (URSSAF) v Hostellerie Le Manoir SARL*, Case C-27/91, ECLI:EU:C:1991:441, 21 November 1991
- *Bodil Lindqvist*, Case C-101/01, ECLI:EU:C:2003:596, 6 November 2003

- *Rechnungshof v. Österreichischer Rundfunk*, Joined Cases C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2017:131, 20 May 2003
- *Productores de Música de España (Promusicae) v Telefónica de España SAU*, Case: C-275/06. ECLI:EU:C:2008:54, 29 January 2008
- *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, Joined cases C-92/09 and C-93/09, Opinon, ECLI:EU:C:2010:353, 9 November 2010
- *Commission v Bavarian Lager*, Case C-28/08 P, ECLI:EU:C:2010:378, 29 June
- *PPU. J. McB. v L. E.*, Case *C-400/10*, ECLI:EU:C:2010:582, 5 October 2010
- *V v. European Parliament*, Case F46/09, ECLI:EU:F:2011:101, 5 July 2011

European Court (and Commission) of Human Rights

European Court of Human Rights:

- *Niemietz v. Germany*, application no. 13710/88, 16 December 1992
- *Halford v. the United Kingdom*, application no. 20605/92, 25 June 1997
- *Amann v. Switzerland*, application no. 27798/95,16 February 2000
- *Christine Goodwin v. the United Kingdom*, application no. 28957/95, 11 July 2002
- *Pretty v. the United Kingdom*, application no. 2346/02, 29 July 2002
- *Société Colas Est and others v. France*, application no. 37971/97, 16 April 2002
- *Peck v. the United Kingdom*, application no. 44647/98, 28 January 2003
- *Copland v. the United Kingdom*, application no. 62617/00, 3 April 2007
- *Evans v. the United Kingdom*, application no. 6339/05, 10 April 2007
- *S. and Marper v. the United Kingdom*, application nos. 30562/04 and 30566/04, 4 December 2008
- *Jehovah's witnesses of Moscow and Others v. Russia*, application no. 302/02, 10 June 2010
- *Von Hannover v. Germany*, applications nos. 40660/08 and 60641/08, 7 February 2012
- *S.A.S. v. France*, application no. 43835/11, 1 July 2014
- *Bărbulescu v. Romania*, application no. 61496/08, 12 January 2016
- *Bărbulescu v. Romania*, application no. 61496/08, 5 September 2017
- *Libert v. France*, application no. 588/13, 22 February 2018

Commission of the ECtHR:

- *X v Iceland*, application no. 6825/74, 8 May 1976
- *Pierre Herbecq and the Association Ligue des droit de l'homme v. Belgium*, applications n° 32200/96 and 32201/96 (joined), 14 January 1998

Decisions of national courts and state institutions

France

Conseil constitutionnel:

- décision n° 76-75 DC du 12 janvier 1977
- décision n° 88-244 DC du 20 juillet 1988
- décision n° 94-352 DC du 18 janvier 1995
- décision n° 99-416 DC du 23 juillet 1999
- décision n° 2009-580 du 10 juin 2009

Conseil d'Etat:

- N° 06361, Section, 1 février 1980
- N° 316856, 4ème et 5ème sous-sections réunies, 15 décembre 2010
- N° 393320 (ECLI:FR:CECHR:2017:393320.20170320), 3ème – 8ème chambres réunies, 20 mars 2014

Cour de cassation:

- chambre commerciale, financière et économique, 10 février 2015, n° 13-14.779
- chambre sociale, 20 nov. 1991, n° 89-44.605
- chambre sociale, 3 déc. 2002, n° 00-44.321
- chambre sociale, 16 juin 1945
- chambre sociale, 31 mai 1956, N° 56-04323
- chambre sociale, 25 février 1988. N° 85-40821
- chambre civile 1, 23 octobre 1990, N° 89-13163
- chambre sociale, 17 avril 1991, N° 90-42636
- chambre sociale, 17 avril 1991, N° 88-40.121
- chambre sociale, 20 nov. 1991, n° 89-44.605
- chambre sociale, 20 novembre 1991, N° 88-43120
- chambre sociale, 20 novembre 1991, N° 89-4460
- chambre sociale, 22 janvier 1992, N° 90-42517
- chambre sociale, 22 mai 1995, N° 93-44078
- chambre civile 1, 6 mars 1996, N° 94-11273
- chambre sociale, 13 novembre 1996, N° 94-13187
- chambre sociale, 14 mai 1997, N° 94-45473
- chambre sociale, 16 déc. 1997, n° 95-41.326
- 16 juin 1998, n° 96-41558

- chambre sociale, 16 décembre 1998, N° 96-43540
- chambre sociale, 14 décembre 1999, N° 97-41995
- chambre sociale, 25 janvier 2000, N° 97-45044
- chambre sociale, 14 mars 2000, n° 98-42.090
- chambre sociale, 19 décembre 2000, N° 98-40.572
- chambre sociale, 10 mai 2001, N° 99-40584
- chambre sociale, 2 octobre 2001, n° 99-42.942
- chambre sociale, 21 mai 2002, 00-41.128
- chambre sociale, 10 juillet 2002, N° 00-45135
- chambre sociale, 30 octobre 2002, N° 00-40868
- chambre sociale, 25 févr. 2003, n° 00-42.031
- chambre sociale, 21 oct. 2003, n° 00-45.291
- chambre sociale, 21 octobre 2003, N° 01-43943
- chambre sociale, 2 décembre 2003, N° 01-43227
- chambre sociale, 17 février 2004, N° 01-45.889
- chambre criminelle, 19 mai 2004, N° 03-83953
- chambre sociale, 2 juin 2004, 03-45.269
- chambre sociale, 17 mai 2005, N° 03-40017
- chambre sociale, 26 avr. 2006, n° 04-43.582
- chambre mixte, 18 mai 2007, N° 05-40803
- chambre sociale, 30 mai 2007, N° 05-43102
- chambre sociale, 29 janvier 2008, N° 06-45279
- chambre sociale, 18 mars 2008, N° 06-45093
- chambre sociale, 9 juillet 2008, N° 06-45800
- chambre sociale, 18 mars 2009, N° 07-44247
- chambre sociale, 17 juin 2009, n° 08-40.274
- chambre sociale, 23 juin 2009, N° 07-45256
- chambre sociale, 9 février 2010, N° 08-45253
- chambre sociale, 17 février 2010, N° 08-45298
- chambre sociale, 26 octobre 2010, N° 09-42740
- chambre sociale, 15 décembre 2010, N° 08-42486
- chambre sociale, 3 mai 2011, N° 09-67464
- chambre sociale, 17 novembre 2011, N° 10-17950
- chambre sociale, 9 mai 2012, n° 11-13.687
- chambre sociale, 26 juin 2012, n° 11-15310

- chambre sociale, 4 juillet 2012, N° 11-12502
- chambre sociale, 4 juillet 2012, N° 11-14241
- chambre sociale, 4 juillet 2012, N° 11-30266
- chambre sociale, 11 juillet 2012, n˚ 11-22.972
- chambre sociale, 26 février 2013, N° 11-27372
- chambre civile 1, 10 avril 2013, N° 11-19.530
- chambre sociale, 16 mai 2013, N° 12-11866
- chambre sociale, 19 juin 2013, N° 12-12138
- chambre sociale, 18 décembre 2013, nº 12-17.832
- chambre sociale, 29 octobre 2014, N° 13-18173
- 26 janvier 2016, n° 14-15.360
- chambre sociale, 7 avril 2016, n° 14-27949
- chambre civile 2, 5 janvier 2017, N° 16-12394
- chambre sociale, 5 juillet 2017, N° 16-15623
- chambre sociale, 20 déc. 2017, n°16-19609
- chambre sociale, 12 sept. 2018, n°16-11.690

Courts of Appeal:

- CA Aix en Provence, 17eme chambre, arrêt au fond du 13 janvier 2015
- CA Aix-en-Provence, 17e chambre B, 4 février 2016, n° 14/13125
- CA Aix-en-Provence, 5 février 2016, n° 14/13717
- CA Aix-en-Provence, 9e chambre A, 27 mars 2015, n° 13/20847
- CA Amiens, 21 mai 2013, n° 12/01638
- CA Basse-Terre, chambre sociale, 13 octobre 2014, N° de RG: 13/01046
- CA Besançon, chambre sociale, 15 novembre 2011, n° 10/02642
- CA Bordeaux, chambre sociale, section A, 12 février 2013, n°12/01832
- CA Bordeaux, Chambre sociale, section A, Arrêt du 15 janvier 2013
- CA Caen, 1re chambre sociale, 27 janvier 2017, n° 15/04402
- CA Caen, 1re chambre sociale, 27 janvier 2017, n° 15/04417
- CA Chambéry, 25 févr. 2016, RG n°15/01264
- CA Fort-de-France, Chambre sociale, 21 décembre 2012, n° 12/00053
- CA Lyon, chambre sociale A, 13 mars 2013, n° 12/05390
- CA Lyon, chambre sociale A, 24 mars 2014, n° 13-03463
- CA Lyon, chambre sociale B, 22 novembre 2012, n° 11/05140
- CA Lyon,18 novembre 2011, n° 11/01261
- CA Montpellier, 4e chambre sociale, section A, 14 mars 2018, n°14/09173

- CA Nîmes, 2 avril 2013, n° 12/02146
- CA Orléans, 28 février 2013, N° 12/01717
- CA Paris, Pôle 6, 3ème ch., 15 novembre 2011, n˚ 09/09 398
- CA Paris, Pôle 6, 5ème ch., 19 janvier 2012, n˚ 10/04 071
- CA Paris, Pôle 6, 6ème ch., 6 février 2013, n˚ 11/03 458
- CA Paris, Pôle 6, chambre 5, 20 septembre 2018, n° 14/04515
- CA Paris, Pôle 6, chambre 8, 3 décembre 2015, n° 13/01716
- CA Paris, Pôle 6, chambre 9, 3 décembre 2015, n° 15/04533
- CA Pau, chambre sociale, 6 septembre 2018, n° 17/01648
- CA Pau, Chambre sociale, Arrêt du 13 juin 2013
- CA Reims, chambre sociale, 15 novembre 2017, n° 16/02786
- CA Reims, chambre sociale, 9 juin 2010, n° 09/03205
- CA Rennes 6 février 2003 n°02-2859
- CA Rennes, 7e chambre prud'homale, 20 novembre 2013, n° 12/03567
- CA Rennes, 8e chambre prud'homale, 2 mars 2018, n° 16/07806
- CA Rouen, Chambre sociale, 1 novembre 2011, n° 11/01827
- CA Rouen, 15 novembre 2011, N° 11/01830
- CA Rouen, 26 avril 2016, n°14/03517
- CA Rouen, chambre sociale, 10 février 2015, n° 14/03335
- CA Rouen, chambre sociale, 15 mars 2018, n° 15/06042
- CA Rouen, chambre sociale, 15 novembre 2011, N° 11/01827
- CA Rouen, chambre sociale, 15 novembre 2011, N° 11/01830
- CA Toulouse, 4e chambre sociale, 2e section, 2 février 2018, n° 16/04882
- CA Versailles, 17e chambre, 4 octobre 2017, n° 15/03872
- CA Versailles, 17e chambre, 7 février 2018, n° 15/05739

Industrial tribunals:

- CPH Boulogne-Billancourt (Section Encadrement), 19 novembre 2010, n° 09/00343

Hungary

Constitutional Court:

- Decision No. 15/1991. (IV. 13.)
- Decision No. 56/1994 (XI. 10.)
- Decision No. 35/2002. (VII. 19.)
- Decision No. 36/2005. (X. 5.)
- Decision No. 32/2013. (XI. 22.)

- Decision No.13/2014. (IV. 18.)
- Decision No. 14/2017. (VI. 30.)

Supreme Court and Curia:

- 1050/2004. számú munkaügyi elvi határozat
- 18/2018. számú munkaügyi elvi határozat
- 7001/2005. (MK 170.) FMM-PM együttes irányelv a munkavégzés alapjául szolgáló szerződések minősítése során figyelembe veendő szempontokról
- LB Pfv. IV. 21 028/2000. – BH2001/61.
- Mfv.II.10.609/2017
- Mfv. I. 10.264/2002/2.
- Mfv. 10.655/2013/6.
- Mfv. 10.469/2013/4.
- BH 1986. 384.
- BH 1991. 47.
- BH 1992.387.
- BH 1996. 286.
- BH 2000. 267.
- BH 2005. 102.
- BH 2006.201.
- BH 2006.64
- BH 2008. 132.

Lower courts:

- Fővárosi Ítélőtábla 2.Pf.20.429/2010/3
- Csongrád Megyei Bíróság 2. Mf. 20. 566/1997.
- Szegedi Munkaügyi Bíróság 4. M. 1159/1994.

Other countries

Belgium:

- Cour du travail de Liège (3e ch.) – Arrêt du 24 mars 2017 – Rôle n° 2016-AL-94
- Canada:
- Canadian National Railway Co. v. Norsk Pacific Steamship Co., [1992] 1 SCR 1021, 1992 CanLII 105 (SCC)

UK:

- Taylor v Somerfield Stores Ltd. Case no: S/107487/07, Held at Aberdeen on 24 July 2007

United States:

- Court of Appeals for the Fourth Circuit: Bland v. Roberts, No. 12-1671, Filed: September 23, 2013
- Court of Appeals for the Ninth Circuit: *Konop v. Hawaian airlines*, 236 F.3d 1035
- District court for the Eastern District of Virginia: Bland v. Roberts, 4-11cv45 (E.D. Va.; Apr. 24, 2012)
- District of New Jersey: *Pietrylo v. Hillstone Restaurant Group*, No. 06-05754, 2009
- Konop v. Hawaian airlines (United States Court of Appeals for the Ninth Circuit, 236 F.3d 1035.)
- Supreme Court of the United States: L*ester Gerard Packingham, Petitioner v. North Carolina*, June 19, 2017

Documents of the data protection supervisory authorities

France – CNIL

- *Guide pratique pour les employeurs*. Les guides de la CNIL, 2005
- *Guide pour les employeurs et les salariés*. Les guides de la CNIL, 2010
- *Rapport d'activité 2016*. La documentation française, Paris, 2017
- *L'écoute et l'enregistrement des appels*. Fiches pratiques. Travail & données personnelles, 2018
- *Le recrutement et la gestion du personnel*. Fiches pratiques. Travail & données personnelles, 2018
- *Les outils informatiques au travail*. Fiches pratiques. Travail & données personnelles, 2018
- *Délibération portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement*. Délibération n°02-017 du 21 mars 2002
- *Délibération n°2007-374 du 11 décembre 2007 sanctionnant la société X*. Délibération n°2007-374 du 11 décembre 2007
- *Délibération de la formation restreinte n°2012-475* du 03 janvier 2013

Hungary – Data Protection Commissioner and NAIH

- Data protection Commissioner:
- ABI 1012/K/2005-3

- ABI 167/A/2006-3.
- ABI 1723/P/2008
- ABI 1767/K/2006-3.
- ABI 235/K/2008
- ABI 2550/K/2007-3.
- ABI 40/K/2006
- ABI 531/A/2004
- ABI 570/A/2001
- ABI 790/A/2001
- ABI 800/K/2008
- ABI 800/K/2008-3.
- ABI 814/A/2004-8.
- ABI 866/A/2006-3.
- ABI 900/A/2006
- The Commissioner's Recommendation on job advertisements and on the activity of private recruitment agencies

NAIH:

- *A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről*. NAIH-4001-6/2012/V. Budapest, 2013
- NAIH 2016 = *A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről*. Budapest, 2016
- NAIH/2016/4386/2/V
- NAIH/2019/51/11

Other law related documents – reports, recommendations, activity reports, press releases etc.

International

United Nations

CoE 2018 = CoE: *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 10 October 2018

CoE 2019 = CoE: *Guide sur l'article 8 de la Convention européenne des droits de l'homme. Droit au respect de la vie privée et familiale*. 2019. Available at: https://www.echr.coe.int/Documents/Guide_Art_8_FRA.pdf (Accessed: 5 November 2019

CoE 2015 = CoE: *Explanatory memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 2015

ECtHR, Press Unit 2017 = ECtHR, Press Unit: *Q & A. Grand Chamber judgment in the case of Bărbulescu v. Romania (application no. 61496/08)*. 2017. Available at: https://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF (Accessed: 1 May 2018)

European Committee of Social Rights = European Committee of Social Rights: *Activity Report 2016*. Council of Europe

European Committee of Social Rights 2012 = *European Committee of Social Rights: Activity Report 2012*. Council of Europe, 2013

European Committee of Social Rights 2006 = *European Committee of Social Rights: Statements of interpretation – Article 1–2*. 2006_Ob_1-2/Ob/EN., 2006

ILO 2006 = ILO: *The employment relationship. Report V(1)*. International Labour Conference, 95th Session, 2006

ILO 2006a = ILO: *The employment relationship. Report V(2A)*. International Labour Conference, 95th Session, 2006

ILO 2007 = ILO: *The employment relationship: An annotated guide to ILO Recommendation No. 198*, 2007

ILO 2017: *The Future of Work We Want: A global dialogue*. Available at: http://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_570282.pdf (Accessed: 16 May 2018)

International Labour Office 2015 = International Labour Office: *World employment and social outlook 2015: The changing nature of jobs*. ILO, Geneva, 2015

International Labour Office, Governance and Tripartism Department – European Labour Law Network 2013 = International Labour Office, Governance and Tripartism Department – European Labour Law Network: *Regulating the employment relationship in Europe: A guide to Recommendation No. 198*. ILO, Geneva, 2013

UN 2015 = UN: *The right to privacy in the digital age*. A/HRC/28/L.27. United Nations, General Assembly, 2015

UN 2016 = UN: *Report of the Special Rapporteur on the right to privacy*. A/HRC/31/64. United Nations, General Assembly, 2016

XVIIth Meeting of European Labour Court Judges 2009 = XVIIth Meeting of European Labour Court Judges: *General and national reports. Privacy in the workplace*. ILO, 2009

EU

ENISA 2007 = ENISA: *Security Issues and Recommendations for Online Social Networks*. Position Paper, 2007

Eurofound – International Labour Office 2017: Eurofound – International Labour Office: *Working anytime, anywhere: The effects on the world of work*. Joint ILO–Eurofound report. Publications Office of the European Union, International Labour Office, Luxembourg, Geneva, 2017

European Commission 2004 = European Commission: *Second stage consultation of social partners on the protection of workers' personal data*. 2004

European Commission 2010 = European Commission: *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union*. COM(2010) 609 final. Brussels, 2010

European Commission 2010a = European Commission: *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*. JLS/2008/C4/011 – 30'CE'0219363/00'28, 2010

European Commission 2012 = European Commission: *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. Press release. 2012. Brussels. Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm (Accessed: 18 January 2019)

European Commission 2015 = European Commission: *Digital Single Market Strategy for Europe*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 192 final. Brussels, 2015

European Commission 2016 = European Commission: *A European agenda for the collaborative economy*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2016) 356 final. Brussels, 2016

European Commission 2018 = European Commission: *The GDPR: new opportunities, new obligations. What every business needs to know about the EU's General Data Protection Regulation*. Publications Office of the European Union: European Union, Luxembourg, 2018. Available at: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf (Accessed: 30 October 2019)

European Data Protection Supervisor 2015 = European Data Protection Supervisor: *Guidelines on personal data and electronic communications in the EU institutions*. 2015. Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-16_eCommunications_EN.pdf (Accessed: 12 August 2019)

European Data Protection Supervisor 2016 = European Data Protection Supervisor: *Guidelines on the protection of personal data processed through web services provided by EU institutions*. 2016. Available at: https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_web_services_en.pdf (Accessed: 12 August 2019)

European Union Agency for Fundamental Rights – Council of Europe 2018 = European Union Agency for Fundamental Rights – Council of Europe: *Handbook on European data protection law: 2018 edition*: Publications Office of the European Union, Luxembourg, 2018

Explanation on Article 7. Explanations relating to the Charter of Fundamental Rights (2007). 2007/C 303/02

Other

30th International Conference of Data Protection and Privacy Commissioners 2008 = 30th International Conference of Data Protection and Privacy Commissioners: *Resolution on Privacy Protection in Social Network Services*. Strasbourg, 2008

European Digital Rights = European Digital Rights: *Key aspects of the proposed General Data Protection Regulation explained: What are they? Why are they important? What are common misconceptions? What can be improved?* Available at: https://edri.org/files/GDPR-key-issues-explained.pdf (Accessed: 1 May 2018)

European Network of Legal Experts in the field of Labour Law 2009 = European Network of Legal Experts in the field of Labour Law: *Characteristics of the Employment Relationship. Thematic Report 2009*. Contract No. VC/2008/1211, 2009

Information Commissioner's Office 2011 = Information Commissioner's Office: *The employment practices code*. 2011. Available from: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf (Accessed 1 February 2017)

International Working Group on Data Protection in Telecommunications 2008 = International Working Group on Data Protection in Telecommunications: *Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" –*. 675.36.5. Rome, 2008

International Working Group on Data Protection in Telecommunications 2013 = International Working Group on Data Protection in Telecommunications: *Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy*. 675.46.32., 2013

National

France

Assemblé Nationale 2014 = Assemblé Nationale: *Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique*, Mercredi 26 novembre 2014, Séance de 17 heures, Compte rendu n° 08. Available at: http://www.assemblee-nationale.fr/14/cr-comnum/14-15/c1415008.asp (Accessed: 26. February 2017)

Commentaire: Conseil constitutionnel: décision n° 2012-248 QPC du 16 mai 2012

Commentaire de la décision n° 2009-580 DC – 10 juin 2009. Loi relative à la diffusion et à la protection de la création sur internet. *Les Cahiers du Conseil Constitutionnel*, (27). Available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009580DCccc_580dc.pdf (Accessed: 6 June 2018)

Conseil d'Etat 2014 = Conseil d'Etat: *Le numérique et les droits fondamentaux*. Les rapports du Conseil d'Etat, 2014

Le Défenseur des droits Le Défenseur des droits 2015 = Le Défenseur des droits Le Défenseur des droits: *Guide pratique pour les professionnels du recrutement. Recruter avec des outils numériques sans discriminer*. 2015. Available at: https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/636150490_int_valide_ft_fini_complet.pdf (Accessed: 27 June 2018)

Ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social 2015 = Ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social: *Guide pratique du droit du travail*. La Documentation française, Paris, 2015

Rapport de la Cour de Cassation 2001: A. Contrat de travail 1. Exécution.

Hungary

Kúria tájékoztatója a Kúria M.I. tanácsa által tárgyaláson kívül elbírált Mfv.I.10.098/2019. számú ügyről, 2019

A PÓLAY ELEMÉR ALAPÍTVÁNY KÖNYVTÁRA
Sorozatszerkesztő: Balogh Elemér egyetemi tanár

1. Balogh Elemér és Sarnyai Csaba Máté (szerk.): *Deák Ferenc és a polgári átalakulás Magyarországon.* Szeged, 2004.
2. Homoki-Nagy Mária (szerk.): *Mezővárosaink jogélete a 18–19. században*. Szeged, 2010.
3. Eric Blin (réd.): *Mécanisme de décisions dans une Europe élargie*. Szeged, 2004.
4. Hajdú József: *A munkavállalók személyiségi jogai*. Szeged, 2005.
5. Eike von Repgow: *A Szász tükör. Szeged*, 2005.
6. Balogh Elemér (Hg.): *Ungarn auf der Schwelle in die EU. Herausforderungen und Aufgaben für Wirtschaft und Gesellschaft*. Szeged, 2006.
7. Karsai Krisztina (szerk.): *Keresztmetszet. Tanulmányok fiatal büntetőjogászok tollából*. Szeged, 2005.
8. Papp Tekla: *A koncesszió*. Szeged, 2006.
9. Hajdú József: *A japán munkaügyi kapcsolatok sajátosságai a kezdetektől 1995-ig*. Szeged, 2006.
10. Szajbély Katalin és Traser Julianna Sára (szerk.): *Képünk az Unióról, helyünk az Unióban*. Szeged, 2006.
11. Nagy Ferenc (szerk.): *Bűnügyi mozaik. Tanulmányok Vida Mihály 70. születésnapja tiszteletére*. Szeged, 2006.
12. Rúzs Molnár Krisztina: *Mediáció a munkajogban*. Szeged, 2007.
13. Nagy Ferenc (szerk.): *Ad futuram memoriam. Tanulmányok Cséka Ervin 85. születésnapja tiszteletére*. Szeged, 2007.
14. Szondi Ildikó: *Nemzetiségi demográfiai viszonyok a déli szláv országokban*. Szeged, 2007.
15. Nagy Ferenc (szerk.): *Büntetőjog és humánum. Emlékkötet Fonyó Antal halálának 25. évfordulójára*. Szeged, 2007.
16. Nagy Tamás és Nagy Zsolt (szerk.): *Jogelmélet és önreflexió*. Szeged, 2007.
17. *Legal Transitions. Development of Law in Formerly Socialist States and the Challenges of the European Union*. Szeged, 2007.
18. Lőrincsikné Lajkó Dóra (szerk.): *Opuscula Szegediensia. A Munkajogi és Szociális Jogi Doktoranduszok és Pályakezdő Oktatók első konferenciája*. Szeged, 2007.
19. Nagy Zsolt: *A jogi oktatás fejlődése és aktuális kérdései*. Szeged, 2007.
20. Gellén Klára: *A színlelt szerződés*. Szeged, 2008.
21. Karsai Krisztina (Hg.): *Strafrechtlicher Lebensschutz in Ungarn und in Deutschland. Beiträge zur Strafrechtsvergleichung*. Szeged, 2008.
22. Görög Márta: *A kegyeleti jog és a nem vagyoni kártérítés*. Szeged, 2008.
23. Szabó Imre (szerk.): *Ius et legitimatio. Tanulmányok Szilbereky Jenő 90. születésnapja tiszteletére*. Szeged, 2008.
24. Csink Lóránt: *Az államfő jogállása Európában és Magyarországon*. Szeged, 2008.
25. Lőrincsikné Lajkó Dóra (szerk.): *Opuscula Szegediensia 2. A Munkajogi és Szociális Jogi Doktoranduszok és Pályakezdő Oktatók második konferenciája*. Szeged, 2008.
26. Both Ödön: *Reform és forradalom. Egybegyűjtött írások Magyarország alkotmány- és jogtörténetéből 1790–1849*. Szeged, 2009.
27. Soós Edit – Fejes Zsuzsanna: *Határon átnyúló együttműködések Magyarországon*. Szeged, 2009.

28. Bobvos Pál (szerk.): *Reformator iuris cooperandi. Tanulmányok Veres József 80. születésnapja tiszteletére*. Szeged, 2009.
29. Bató Szilvia: *A „büntetési rendszer" átalakításának megjelenése Kossuth Lajos Pesti Hírlapjában (1841–1844)*. Szeged, 2010.
30. Juhász Zsuzsanna: *A börtön-egészségügy „gócpontjai" és ártalomcsökkentő kezdeményezések külföldön*. Szeged, 2010.
31. Lőrincsikné Lajkó Dóra (szerk.): *Opuscula Szegediensia 3. A Munkajogi és Szociális Jogi Doktoranduszok és Pályakezdő Oktatók harmadik konferenciája Szeged*. Szeged, 2010.
32. Hegedűs Andrea: *Az élettársi kapcsolat a polgári jogi kodifikáció tükrében*. Szeged, 2010.
33. Berki Gabriella (szerk.): *Opuscula Szegediensia 4. A Munkajogi és Szociális Jogi Doktoranduszok és Pályakezdő Oktatók negyedik konferenciája Szeged*. Szeged, 2011.
34. Horesnyi Julianna Csilla: *Bérgarancia. A magyar szabályozás és annak gyakorlata*. Szeged, 2011.
35. Blazovich László és Schmidt József (közreadják): *A Sváb tükör*. Szeged, 2011.
36. Antal Tamás: *Város és népképviselet. Az 1848:XXIII. tc. és intézményei Debrecenben* (*1848–1872*). Szeged, 2011.
37. Trócsányi László (szerk.): *Dikaiosz logosz. Tanulmányok Kovács István emlékére*. Szeged, 2012.
38. Nagy Zsolt: *Metszetek a jogásztársadalomról*. Szeged, 2012.
39. Merkovity Norbert: *Bevezetés a hagyományos és az új politikai kommunikáció elméletébe*. Szeged, 2012.
40. Császár Mátyás: *Az Európai Unió intézményi jogi aktusai*. Szeged, 2013.
41. Ember Alex: *Az üzemi baleset*. Szeged, 2013.
42. Szalai Anikó: *A fegyveres összeütközések hatása a nemzetközi szerződésekre*. Szeged, 2013.
43. József Hajdú: *Social Protection of the Unemployed*. Szeged, 2013.
44. Molnár Imre: *A locatio conductio a klasszikus kori római jogban*. Szeged, 2013.
45. Molnár Imre: *Ius criminale Romanum. Tanulmányok a római jog köréből*. Szeged, 2013.
46. Jakab Éva: *Humanizmus és jogtudomány. Brissonius szerződési formulái I*. Szeged, 2013.
47. Badó Attila: *Az igazságszolgáltató hatalom függetlensége és a tisztességes eljárás*. Szeged, 2013.
48. Téglási András: *A tulajdonhoz való jog alkotmányos védelme*. Szeged, 2013.
49. Soós Edit: *A mélyülő európai integráció*. Szeged, 2013.
50. Révész Béla (szerk.): *„Most megint Európában vagyunk…" Szabó József emlékkönyv*. Szeged, 2014.
51. Bóka János: *Tradíció és modernitás a kínai jogrendszerben. A szerződési jog útja a császárkori gyökerektől a modern szintézisig*. Szeged, 2015.
52. Sulyok Tamás: *Az ügyvédi hivatás alkotmányjogi helyzete*. Szeged, 2015.
53. Juhász Krisztina: *Az Európai Unió biztonság- és védelempolitikája, az EU válságkezelési tevékenysége*. Szeged, 2015.
54. Homoki-Nagy Mária: *„A ministerium az ősiség teljes és tökéletes eltörlésének alapján a polgári törvénykönyvet ki fogja dolgozni (…) Az Osztrák Polgári Törvénykönyv hatása a magyar magánjogra*. [Előkészületben.]
55. Karsai Krisztina: *Alapelvi (r)evolúció az európai büntetőjogban*. Szeged, 2015.
56. Szomora Zsolt: *Alkotmány és anyagi büntetőjog. A büntetőjog-alkalmazás alkotmányosságának egyes kérdései*. Szeged, 2015.
57. Stipta István: *A magyar jogtörténet-tudomány kétszáz éve*. Szeged, 2015.

58. Balogh Elemér – Homoki-Nagy Mária (szerk.): *Tripartitum trium professorum. Három szegedi jogtörténész. Drei Szegediner Rechtshistoriker. Tudományos emlékülés Bónis György születésének 100., Both Ödön születésének 90. és Iványi Béla halálának 50. évfordulóján.* Szeged, 2017.
59. Gácsi Anett: *A jogellenesen megszerzett bizonyítékok értékelése a büntetőeljárásban*. Szeged, 2016.
60. Fejes Zsuzsanna (szerk): *Suum cuique. Ünnepi tanulmányok Paczolay Péter 60. születésnapja tiszteletére*. Szeged, 2016.
61. Gál Andor – Karsai Krisztina (szerk.): *Ad valorem. Ünnepi tanulmányok Vida Mihály 80. születésnapjára*. Szeged, 2016.
62. Pákozdi Zita: *A jogerő tárgyi terjedelme a polgári perben*. Szeged, 2017.
63. Juhász Andrea Erika: *A kínzás, az embertelen, a megalázó bánásmód tilalma a fogvatartottakkal szemben*. 2019.
64. Gellén Klára (szerk.): *Honori et virtuti. Ünnepi tanulmányok Bobvos Pál 65. születésnapjára*. Szeged, 2017.
65. Gellén Klára – Görög Márta: *Lege et fide. Ünnepi tanulmányok Szabó Imre 65. születésnapjára*. Szeged, 2016.
66. Pozsonyi Norbert: *Dologi hitelbiztosítékok az ügyleti gyakorlatban. Kauteláris praxis a preklasszikus és a klasszikus korszakban*. Szeged, 2017.
67. Révész Béla (szerk.): *A szegedi jogbölcseleti iskola alapítója. Horváth Barna emlékkönyv*. Szeged, 2017.
68. Görög Márta – Hegedűs Andrea (szerk): *Lege duce, comite familia. Ünnepi tanulmányok Tóthné Fábián Eszter tiszteletére, jogászi pályafutásának 60. évfordulójára*. Szeged, 2017.
69. Legeza Dénes: *A kiadói szerződés története. A reformkortól 1952-ig*. Szeged, 2018.
70. Martonyi János: *Nyitás és identitás. Geopolitika, világkereskedelem, Európa*. Szeged, 2018.
71. Görög Márta – Mezei Péter (szerk.): *A szellemi tulajdonvédelem és a szabadkereskedelem aktuális kérdései*. Szeged, 2018.
72. Deák Zoltán: *Az erőszak, a fenyegetés és a kényszer büntetőjogi fogalmai*. Szeged, 2018.
73. Dúl János: *A társasági jog és az öröklési jog kapcsolódási pontjai osztrák jogi fragmentumokkal*. Szeged, 2018.
74. Tamási Anna Éva: *A veszprémi és a székesfehérvári szentszékek törvénykezési gyakorlata házassági perekben* (*1850–1920*). [Előkészületben.]
75. Juhász Krisztina (szerk.): *Az első 25 év. A szegedi Politológiai Tanszék jubileumi tanulmánykötete*. Szeged, 2018.
76. Gál Andor: *A jogos védelem teleologikus megközelítésben*. Szeged, 2019.
77. Csatlós Erzsébet: *A konzuli védelem európai közigazgatása. Az együttműködések szervezeti és eljárásjoga az uniós polgár konzuli védelemhez való jogának tükrében*. Szeged, 2019.
78. Rokolya Gábor: *Az államosított közjegyzőség története*. Szeged. 2019.
79. Badó Attila: *A bírói függetlenség egyes garanciális elemeinek összehasonlító vizsgálata*. Szeged, 2020.
80. Görög Márta – Mezei Péter (szerk.): *Innovatív társadalom – innovatív szellemi tulajdonvédelem*. Szeged, 2020.
81. Siket Judit: *A helyi, önkormányzatok közigazgatási autonómiája Magyarországon. Az autonómia egyes tárgykörei intézménytörténeti és nemzetközi kitekintéssel, figyelemmel a Helyi Önkormányzatok Európai Chartájára*. Szeged, 2020.
82. Szakály Zsuzsa: *Az alkotmány stabilitását védő garanciák*. Szeged, 2020.

83. Varga Norbert: *A kartellfelügyelet bevezetése Magyarországon. Az 1931:XX. tc. kodifikációja és gyakorlata.* Szeged, 2020.
84. Molnár Erzsébet: *A gazdálkodó szervezet vezetőjének speciális büntetőjogi felelőssége*. Szeged, 2020.
85. Jakab Éva: *Iustitia mérlege. Polgárok és peregrinusok a helytartó bírói fóruma előtt*. Szeged, 2020.
86. *Communicative Space – Political Space. 11th Central and Eastern European Communication and Media Conference, 2018*. Szeged, 2020.
87. Harkai István: *Az internet hatása a többszörözési és a nyilvánossághoz közvetítési jogra*. Szeged, 2021.
88. Gyémánt Richárd: *A Koronák Uniójától az egyesülési törvényekig*. Szeged, 2021.
89. Tribl Norbert: *Az alkotmányos identitás funkciója és alkalmazhatósága a szupranacionális térben.* Szeged, 2021.
90. Adrienn Lukács: *Employees' Right to Privacy and Right to Data Protection on Social Network Sites, with Special Regard to France and Hungary.* Szeged, 2021.