

Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship*

BY EDIT KAJTÁR**

Abstract. The growing popularity of social networking sites such as Facebook or Twitter has made a strong impact on the workplace. This essay provides insight into the nature of these relatively new, digital channels of communication as well as the socio-legal environment they function in. How does the presence of social media shape the dynamics of the employment relationship? Can a routine pre-interview Google search lead to discriminatory selection practice? Can negative comments posted online about the management serve as grounds for disciplinary action, including termination? We follow the parties to the employment relationship as they use or abuse the opportunities offered to them by social networking sites; and examine how the employees' right to privacy and equal treatment is balanced against the employers' lawful rights and interests. In search of key patterns as well as potential answers, cases from different countries in and outside of the European Union are studied.

Keywords: social networking sites; employment; privacy; data protection; discrimination

1. PRIVACY AT THE WORKPLACE

“Privacy 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.”¹ The thoughts of Robert C. Post capture perfectly the slight confusion one experiences when confronted with the concept of privacy. Different disciplines ranging from law to philosophy have made abundant attempts to capture the essence and define the meaning of this composite concept. Privacy connects with equally intricate notions such as freedom and dignity; its advocates the view of the “right to be left alone” as a structural element of social interactions; invasion of what offends the human spirit², and claim that a society without privacy, would be a society deprived of meaningful social relations.³ The legal notion (i.e. the right to privacy) has been enshrined in numerous international treaties. Being a very complex umbrella concept, its fine tuning is left to different branches of the law.

Privacy is always context dependent, in our case it has to be viewed against the employment background. This specific scenery however will further increase the level of our confusion. On the one hand, we have to take into account the purpose of the employment relationship, that is provision of work for remuneration under terms and conditions defined by, at least typically and mainly, the employer. Again usually, for a certain period of time and in a certain space and manner the employee's physical and mental capacities are at the disposal of the employer. On the other hand, the most relevant characteristic of the employment relationship is the presence of power imbalance between the parties. This implies that to protect the employee, i.e. the party with less power, additional safeguards will be needed if privacy is to be effectively protected. Although the default position is that

* This essay was written with the support of OTKA, PD 996246 grant.

** Ph.D., assistant professor, WU Wien. E-mail: edit.kajtar@wu.ac.at

¹ Post (2000–2001) 2087.

² Warren and Brandeis (1890) 193, 197.

³ Roessler and Mokrosinska (2013) 771, 779.

the employee enjoys the right to privacy, this right is not absolute. Employment law acknowledges the employer's right to monitor. There is extensive academic literature on the use of camera, alcohol and drug tests, on the monitoring of emails and traditional letters addressed to the workplace etc.⁴ While the "classic" inspection activity takes place within working hours and at the workplace, the monitoring of SNSs expands outside this time frame and goes beyond the physical workplace.

The boundaries between work and private life are becoming increasingly fuzzy. With the advancement of IT and the spreading of atypical work arrangements this tendency is intensified. Often the same equipment (e.g. laptop, computer, smart phone) is used for both work and personal purposes, making it difficult to say what can and what cannot be monitored. Also, private life flows over into the working one and vice versa. The same employee who updates his status on Facebook within working hours might convert his living room into a "workplace" when he uploads a project report from his private laptop at midnight, just before the final deadline expires. While the employee is required to dedicate his energy and time to his work, the workplace is by no means a "completely privacy free zone". Craig refers to private matters such as making a phone call to a sick child or arranging medical appointments and also points out the different nature of personal time (lunch and coffee breaks).⁵ Certain rights and obligations arising from the employment relationship are not only active within working hours either; we have to bear in mind that certain duties such as to act in line with the principle of loyalty or not to harm reputation do not end with the working day.

2. SOCIAL NETWORKING SITES

The arrival of social networking sites (SNSs) is perhaps one of the biggest changes in the workplace over the last decade. These sites are typical examples of the Web 2.0 sites that enable users to interact with each other in an online community. The idea behind these sites is to connect people for instance friends or alumni with one another on an informal basis and make communication more effective. Users of SNSs step outside their immediate family circle and enter the realm of virtual social interactions; they introduce themselves by sharing information; connect and communicate with other each other. SNSs differ from physical places in many respects: they are mediated, and potentially global, searchable, and the interactions may be recorded or copied and also these sites may have invisible audiences or audiences not present at the time of the conversation.⁶

SNSs are products of what the Spanish sociologist and cybernetic culture theoretician Manuel Castells calls "global network society". Castells argues that today's societal changes are shaped by the globalised flow of information. The power is based on extensive networks and the possession of information. He points out that in contrast to real time the network society is seeking to compress time and to eliminate the traditional sequencing of time into one hypertext ("timeless time") and the societal functions no longer rest on physical encounters but on exchanges between electronic circuits ("space of flows"). The guiding principle is "being online".⁷ The popularity of these sites lies in their social functions.

⁴ For an overview in Hungarian see e.g. Hegedűs and Kerekes (2010); Arany Tóth (2008); Hajdú (2005).

⁵ Craig (1999) 20.

⁶ Boyd and Ellison (2008) 210.

⁷ Castells (2010) 406.

By giving users a forum in which they can create social identities, build relationships and accumulate social capital, Facebook and other SNSs fulfil basic human needs.⁸ This explains why in many cases employees and job candidates themselves contribute to the invasion of their privacy by oversharing.

The placement of SNSs on a “from private to public” spectrum proves to be difficult. In my opinion, because of their distinctive features, the objectives they serve and the environment they operate in SNSs have public, semi-public and private aspects at the same time. Images in academic literature attempting to capture posts with relevance to the employment relationship include “new water cooler” and “notice board of the staff canteen”. In the UK even if SNS profiles are set to private, there can generally be no expectation of privacy, the posts will be deemed to be public. In other countries the size of the intended audience plays a relevant role. However, even if SNSs posts are intended to be accessible to a limited audience, case law on “Facebook firings” from in and outside the European Union shows that privacy is of relative value. The semi-public aspect is also supported by the fact that these sites operate in a virtual space, thus whatever is put on the platform is relatively easy to search and share. The more limited the audience, the closer the information shared is to being considered private. One-to-one functions such as mail or chat should be treated as private and enjoy legal protection accordingly.

3. PRIVACY CONCERNS

Due to their inherent characteristics, SNSs pose a challenge to traditional privacy regulations, which are typically concerned with protection of citizens against unfair or non-proportional processing of personal data by the public administration, and businesses, and offer only very few rules governing the publication of personal data at the initiative of private individuals.⁹

Within the European context, the legal assessment of a pre-employment Google search and monitoring of SNSs during the employment relationship is shaped by the principles of data protection enshrined in documents such as: Directive 95/46/EC¹⁰; the OECD Guidelines on the Protection of Privacy (hereinafter: OECD Guidelines); the UN Guidelines¹¹; the Council of Europe’s Convention No. 108 (hereinafter: CoE Convention) as well as the national data protection, employment and criminal law etc. provisions. In Hungary the main law sources are Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information (DPA) and Act I of 2012 on the Labour Code. A growing interest is detectable among the scientific community towards the employment law implications of SNSs.¹² For the time being, due to the absence of consistent

⁸ Grimmelman (2009) 1137, 1206.

⁹ International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services (43rd meeting, 3-4 March 2008, Rome Italy) 1 <https://cbpweb.nl/sites/default/files/downloads/int/opinie_social_network_services.pdf > accessed 27 January 2015.

¹⁰ 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 of 23.11.1995.

¹¹ Guidelines for the Regulation of Computerized Personal Data Files, as adopted by General Assembly resolution 45/95 of 14 December 1990.

¹² See for instance Pók (2012) 10; Horváth and Gelányi (2011) 60; Németh (2013) 96; Szöke (2012).

jurisprudence the problem is mainly approached on a hypothetical level. For this reason it is beneficial to examine the external legal sources and draw from the practice of other countries.

The application of the following most important principles are examined below: fair and lawful processing (as an overarching principle); data reduction and data economy; permission; purpose; direct collection; access; accuracy and limitation.

The overarching twin principles of fairness and lawfulness are the number one principle of the UN Guidelines, it is also enshrined in Art. 5(a) of the CoE Convention; in Art. 6(1)(a) of Directive 95/46/EC. It is a crucial requirement, one that is embodied in numerous specific sub-requirements. It covers but it is not limited to existence of a fair and legal grounds. Art. 7 of Directive 95/46/EC lists six potential options where personal data can only be processed:

- a) based on the data subject's unambiguous consent or processing is necessary for:
- b) performance of a contract with the data subject;
- c) compliance with a legal obligation imposed on the controller;
- d) protection of the vital interests of the data subject;
- e) performance of a task carried out in the public interest; or
- f) legitimate interests pursued by the controller, subject to an additional balancing test against the data subject's rights and interests.

Naturally, irrespective of the existence of a legal ground, data processing must always comply with all the other general principles. Out of the six grounds, those listed in (a), (b) and (f) appear to be reasonable candidates for justifying a search on SNSs. Relying on Art. 7(a) is very shaky ground as the genuine nature of consent is always questionable due to the power imbalances of the parties. Though in itself it is – in my opinion – an insufficient justification, attaining consent complies with other data protection principles such as transparency. Art. 7(b) provides a legal ground in situations where “processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”. This article covers pre-contractual relations, provided that steps are taken at the request of the data subject, rather than at the initiative of the controller or any third party. However, detailed online background checks are unlikely to be considered as necessary steps made at the request of the data subject. This is also true within the employment context.

The employer may also try to rely on Art. 7(f). At the pre-employment stage it is a legitimate interest to want to select the best possible candidate. To avoid vicarious liability and “negligent hiring” claims the future employer has to take reasonable action to examine the candidate's background, to gain relevant information, verify documentations etc. Later on, with relation to the ongoing employment relationship, the employer has various interests to protect as well (effective functioning of the work for example). In both cases the employer's interests have to be balanced against the candidate's rights and interests (to express him- or herself freely, right to private life, etc.). The employer is obliged to look for the least intrusive measures available. For instance to check the validity of the statements of the candidate, the employer may (with the consent of the candidate) ask for a reference about the former employee or search public databases (classified directory for example). During the lifetime of the employment relationship less intrusive measures include blocking the use of SNSs on company computers during working time.

According to the principle of data reduction and data economy (also called as principle of necessity, non-excessiveness or proportionality by the various data protection instruments) data processing systems must be designed and selected to collect, process and

use as little personal data as possible (see e.g. Art. 6(1)(c) and Art. 7 of Directive 95/46/EC, Art. 5(c) of the CoE Convention). This principle is infringed as Facebook reveals a multitude of mostly non-work related information.

In line with the principle of purpose, the purposes for which data is processed or used must be defined at the time of collection and personal data can only be processed and used in accordance with this purpose (See para 9 of the OECD Guidelines; Principle 3 of the UN Guidelines; Art. 5(b) of the CoE Convention and Art 6(1)(b) of Directive 95/46/EC). In our case the purpose is most likely the selection of the best possible candidate and verification of facts stated in the CV.

According to the principle of direct collection, personal data must be collected from the data subject, unless an exemption applies by law, or the collection from the data subject would require disproportionate effort and the justified interests of the data subject are not affected. Personal data in our case is not collected from the candidate/employee, and as the collection from the data subject would not require disproportionate effort, the exception rule does not apply either, consequently this principle is violated.

Candidates and employees have the right to know what information is collected about them, for what reason, for how long and how it will be used. The principle of access and openness is violated, because the data subject may not access the information that is stored concerning him or her after the Google search. The principle of accuracy (data quality and correctness) is enshrined in para 8 of the OECD Guidelines; Art. 5(d) of the CoE Convention and Art 6(1)(d) of Directive 95/46/EC. Assessing someone's potential employability based on an online profile may produce false results. Profiles do not necessarily provide an accurate and up to date picture of the individual. As it is demonstrated in the French test case cited later on, pre-employment screens are often superficial and thus are very likely to lead to speculative conclusions. The principle of accuracy would require correction of incorrect personal data, however, as the candidate/employee is unaware of the search let alone its result, he or she clearly cannot demand the employer to correct inappropriate data. Finally, the principle of limitation would require the employer to erase the personal data collected from the Internet once it is no longer necessary for the purpose for which it has been collected (i.e. the job is filled). This is generally unlikely to happen in practice.

4. PRE-EMPLOYMENT GOOGLE SEARCH

4.1. Multitude of Information Only A Few Clicks Away

It is not a surprise that a Google search is part of the recruitment process in many workplaces. It is a fast, easy, cost effective and overall, a very convenient way to find information about the job applicants. With a few clicks of the mouse the employer may not only check the candidates' background and verify some of the facts stated in the CV (professional experience, qualifications etc.) but also acquires his first impressions of the future employee.¹³ Given the wide spread use of social networking sites (SNSs), the Google search will probably lead to a profile such as Facebook or Twitter.¹⁴ Very often it is this stage where the important decision whether a candidate will evolve to employee is made. Profiles are tale-telling. Posts full of spelling mistakes speak volumes about the lack of

¹³ Brown and Vaughn (2011) 219.

¹⁴ It remains to be seen to what extent will the famous 'right to be forgotten' ruling of the CJEU (C-131/12) moderate this tendency.

written communication skills and most certainly ruin the effect of even the most impressive motivation letter. No matter how nice the recommendations attached to the application are, pictures suggesting drug abuse or extensive use of alcohol, or offensive comments about former company and colleagues will get the application shipwrecked. The employers most certainly look for red flags when they type the applicants name in the Google browser, however, the information they encounter (most cases without the authorisation or even previous knowledge of the owner of the profile) is more than warning signs. The posts, comments, pictures, even the music shared reveal a multitude of information on the lifestyle, political and spiritual views, family status or sexual orientation of the candidate. As we can see these data are not work related, on the contrary, they concern the candidate's personal life, often the most private aspects of it.

4.2. Pre-employment Google Search as Potential Discrimination Case

In spite of all its advantages, a pre-employment Google search is not without its dangers. It does not only raise privacy concerns, but may also lead to discriminatory practices. According to EU regulations as well as national employment and data protection laws employers are only permitted to ask for personal information about the applicant's if the information is relevant to the specific job. The main problem with a Google search is that the employer also collects information that he or she would not have the right to obtain during for instance a job interview. In addition, this happens without the candidate's knowledge. Googling may very well lead to discrimination and unethical practices; applicants can be eliminated because the content they post online is considered to be inappropriate. A huge body of academic literature is dedicated to protection against discrimination including prohibition of discriminatory hiring (job advertisements and interviews infringing the principle of equal treatment etc.), yet the potential danger of a Google search from the perspective of discrimination is under-researched.

To highlight the relevance of the issue I would like to speak of a recent field study conducted by academics of Université Paris Sud. During one year from March 2012 to March 2013 the researchers handed in more than 800 applications for real accountant job offers in the greater Paris area. They adjusted the content of Facebook accounts of the candidates to manipulate the perceived origins of applicants (home town and language spoken). The twist of the experiment was that they only manipulated the Facebook profiles, not the application material, this way they could see the impact of pre-employment screening on the number of call-backs received from employers. The test applicant received a third fewer call-backs compared to the control applicant. During the course of the experiment they modified the profiles so that the language spoken by the applicants could only be reached by clicking on a tab. The results were surprising. In subsequent months, the gap between the two applicant types shrank and virtually disappeared suggesting that the future employers based their hiring decision on a search that only concerned the very surface of the profiles.¹⁵

The push toward the emergence of legal parameters to control the privacy aspects of SNSs in the employment context is a visible trend in the US. Lawyers warn of increasing numbers of "failure to hire" lawsuits if it can be proved that employers are using SNSs to gather information on the candidate's protected characteristics (such as marital status, religion, race, sexual identity, political opinion or national origin) as a basis for hiring

¹⁵ Manant, Pajak and Soulié (2014).

decisions.¹⁶ To give an example: In 2007 the University of Kentucky was looking for a founding director for the university's astronomical observatory. C. Martin Gaskell applied for the position and being the best candidate by far, he stood a high chance of getting hired. Yet, at a certain point along the selection procedure the hiring committee found his blog that discussed astronomy and the Bible from a creationist viewpoint. The same committee that had previously noted that Gaskell was "clearly the most experienced" candidate and had "already done everything [the hiring committee] could possibly want the observatory director to do," recommended another candidate for the position. Gaskell sued for religious discrimination.¹⁷

4.3. Possible Responses

The assessment of a pre-employment google search depends on the privacy awareness of the given country. In Finland the Data Protection Ombudsman explicitly stated that employers cannot use Internet search engines such as Google to collect background information on job candidates.¹⁸ He said: "According to the Privacy in Working Life Act, employers can only view personal data provided by their employees, and this includes data about job applicants". The response was a lot milder for instance in the UK. The Employment Practices Code published by the UK Information Commissioner's Office simply advised employers to "[e]nsure there is a clear statement on the application form or surrounding documents, explaining what information will be sought and from whom" and "explain the nature of and sources from which information might be obtained about the applicant in addition to the information supplied directly by the applicant"¹⁹.

The above mentioned reactions came from expert bodies; however, we can also find hard law responses. A draft bill on "Arbeitnehmerdatenschutz" was produced on 25 August 2010 in Germany. The draft prohibited employers from using personal SNSs to screen applicants, but allowed the use of business-focused networks when conducting background checks. The Explanations by the Home Office on Internet searches of the employer highlighted that the employer may, in principle, gather information on an applicant from all publicly available sources (e.g. newspapers or Internet). Regarding online social networks, as far as they serve private use (e.g. Facebook, schülerVZ, StudiVZ or StayFriends), the employer may not use them to get information. Despite this, the employer may benefit from searching those SNSs that are intended to represent its members professionally (e.g. Xing, LinkedIn).²⁰ Due to lack of consensus the draft was rejected in 2013.

¹⁶ Waring and Buchanan (2010) 14, 19.

¹⁷ *Gaskell v. Univ. of Kentucky*, No CIV.A. 09 -244-KSF, 2010 WL 4867630 (E D Ky Nov. 23, 2010) Cited by Carlson (2014) 484. The case was later settled.

¹⁸ McGeeveran (2006).

¹⁹ Information Commissioner's Office Data Protection. The Employment Practices Code [2011] <https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf> accessed 28 January 2015.

²⁰ See § 32 Absatz 6 BDSG <<http://www.arbeitnehmerdatenschutz.de/Gesetz/32-BDSG-Datenerhebung-vor-Beschaefigungsverhaeltnis.html>> Accessed 29 January 2015.

5. MONITORING SNS DURING THE EMPLOYMENT RELATIONSHIP

5.1. Cases

Below I will give some typical examples where the employees “overstepped the line” and show the balancing exercise undertaken by the courts. In the Dutch *Blokker* case the employee of *Blokker* a supermarket chain posted a critical remark about his employer on his Facebook page. The warning of the employer did not stop him from repeating this behaviour, and from posting an insulting comment²¹ within less than three weeks. Though the post was intended to a limited audience (it could be read only by the “friends” of the employee), a colleague “friend” informed the employer who dismissed the employee. The Arnhem sub district court held that free speech is limited by the duty of care towards the employer, and that the insulting Facebook post was not covered by it but they rather qualified as gross insults. The court also pointed out the relativity of the private nature of Facebook.²² Commenting on this case Van Heck argues that posting an insulting remark about the employer on Facebook (irrespective of the limited circle of addresses) is similar to pinning an unfounded and inflammatory notice on the notice board of the staff canteen where all employees as well as visitors can read it. The right to free speech has to be weighed against the duty to refrain from activities that may harm the lawful economic interest of the employer, such as posting comments online that damage the reputation of the company. The right balance depends on the degree of harm, the potential size of the audience, the method of communication and finally the relationship between the employee and the audience. SNS posts are special in many respects. The content is transmitted immediately; the audience irrespective of the user’s intentions (and privacy settings) is unlimited, the post is almost unerasable.²³

In Germany, the legal reasoning of the courts in *Blokker*-like cases is similar to that of the Dutch courts. Due to the permanent nature of online posts, defamation on Facebook weighs heavier than insulting someone verbally. In a case in front of the Higher Labour Court Hamm²⁴ an apprentice wrote “oppressor” and “exploiter” on his personal Facebook profile under the section “employer”. The Court qualified these remarks as a relevant offence and emphasised that the use of Facebook made the comment available to the public. A shift of focus is detectable in the case law. The judgments are moving away from the protection of the employee’s privacy and right to self-determination regarding personal data toward the employer’s rights of ownership (as to their company IT).²⁵

In the United Kingdom employees increasingly rely on a breach of the Human Rights Act and the European Convention on Human Rights (breach of Article 8 or Article 10 ECHR) in addition to claiming unfair dismissal, especially if they have been dismissed for using social media sites outside of working hours. The courts undertake a balancing act between the harm caused and the employer’s actions.²⁶ In *Teggart v TeleTech UK limited*

²¹ He called *Blokker* a ‘bastard company’ and the management, ‘incompetent bastards’.

²² 800536 HA VERZ 12-1038 available at <www.rechtspraak.nl>; See also LJV BV 9483 <<http://leidenlawblog.nl/articles/think-before-you-post>> accessed 26 September 2014).

²³ Facebook Posting Not Covered by Right to Free Speech (NL) [2012] 55 EELC 21-22.

²⁴ Verdict by the Higher Labour Court Hamm from October 10, 2012 (3 Sa 644/12) cited by Fülbier (2012).

²⁵ Verdict by the Higher Labour Court Hamm from October 10, 2012 (3 Sa 644/12)

²⁶ Action on Misuse of Social Media by employees (Kemp Little Social Media Seminar Section 3) <http://www.kemplittle.com/cms/document/Social_Media_Seminar_Action_on_Misuse.pdf> accessed 26 September 2014.

NIIT²⁷ the employee, Mr Teggart posted an obscene comment about the alleged promiscuity of a female colleague on his Facebook page. The post was made off working hours, from his home, from his own computer. The employer was informed by a “friend” of Mr Teggart. The outcome was dismissal for harassment on the basis that “he [had] made multiple postings on a social media site regarding a fellow employee, one of which made reference to TeleTech”. The company stressed that it considered that Mr Teggart had harassed his co-worker and, in mentioning TeleTech, had brought the company into disrepute. Mr Teggart claimed unfair dismissal and breach of his rights to privacy, freedom of belief and freedom of expression under the ECHR. The tribunal dismissed Mr Teggart’s claim for unfair dismissal.

Interestingly the court cited a famous American case, National Labor Relations Board v American Medical Response of Connecticut. It is worth devoting some lines to the case of Ms Dawnmarie Souza, because it demonstrates effectively the different approach of the American court and also because it highlights how important the content of the comment is. Ms Dawnmarie Souza had been dismissed because of the remarks she made on Facebook about her supervisor, similarly to the UK case, in her own time and from her own computer. “Looks like I’m getting some time off. Love how the company allows a 17 to be a supervisor” – read the post referring to the professional jargon for a psychiatric patient. Lafe Solomon, the board’s acting general counsel classified the case as a fairly straightforward one under the National Labor Relations Act; and stated that irrespective of the place of action “whether it takes place on Facebook or at the water cooler, it was employees talking jointly about working conditions, in this case about their supervisor, and they have a right to do that.”²⁸ The key difference between the two cases (and also between the two legal approaches) is that in the United States if an employee posts critical remarks on his employer on a social networking site with the intention to raise common concern or advance the position of the employees, his action qualifies as concerted activity and generally enjoys protection (see later in details). The case was settled. Under the settlement the respondent agreed to revise its rules to ensure that they did not improperly restrict employees from discussing their wages, hours and working conditions with co-worker’s while not at work. The respondent also pledged it would not discipline workers or discharge them for engaging in such discussions.²⁹

Going back to Mr. Teggart in the UK, his lawsuit had an opposite ending. The Industrial Tribunal found that the harassment was sufficient to justify a dismissal of the claimant for gross misconduct. Despite the limited circle of intended audience (for instance the female colleague could not view the comment) the Industrial Tribunal found that when Mr Teggart put his comments on his Facebook page he had abandoned any right to consider his comments as being “private” and that the right of freedom of expression must be exercised responsibly and did not entitle employees to make comments which harm another colleague’s reputation and infringed her right not to suffer harassment.³⁰

²⁷ Teggart v TeleTech UK limited NIIT 00704/11.

²⁸ Neal (2012) 1715.

²⁹ There was also a separate, private agreement between Ms Souza and the respondent regarding her dismissal which was not disclosed.

³⁰ Action on Misuse of Social Media by employees (Kemp Little Social Media Seminar Section 3) <http://www.kemplittle.com/cms/document/Social_Media_Seminar_Action_on_Misuse.pdf> accessed 26 September 2014; regarding the belief argument the Court made reference to academic literature Allen, Beale and Crasnow (2007) and pointed out that ‘belief’ does not extend to a belief

5.2. From Complete Ban to Hand-Crafted Code of Conduct

As we can see the employees can indeed infringe their employment-related obligations on SNSs. To ban the use of SNSs entirely is obviously not a legal solution as it constitutes an unlawful and excessive restriction on freedom of expression. The employer has no right to prohibit the use of social media per se. In many jurisdictions, the degree to which an employer can discipline an employee or terminate his/her employment relationship on account of the employee's use (or misuse) of technology will depend on the policies that are already in place.³¹ In my opinion the use of social media sites during working time in itself may only serve as ground for dismissal if the employer previously explicitly notified the employee that these activities are prohibited and the nature of the work as well as the content of the action justifies such prohibition. A written document can help the company to protect itself against liability for the actions of its workers; gives clear guidelines for employees on what they can and cannot say about the company; helps managers to manage performance effectively and employees to draw a line between their private and professional lives. It also aids compliance with the law on discrimination, data protection and protecting the health of employees.³²

The employer's social media policy needs to be clearly worded if the employer wishes to be able to rely on a breach of it, and a regular audit will enhance compliance.³³ It is useful to apply the guidelines offered by the ACAS (Advisory, Conciliation and Arbitration Service). The main suggestions are as follows: Employers should give clear examples of what will be regarded as gross misconduct (e.g. posting derogatory or offensive comments on the Internet about the company or a work colleague) and provide information about the possible consequences. The policy should specify the following areas: definition and purpose of policy; who it applies to; responsibilities; reference and links to other policies; responsible use of social media (including defining what is considered as acceptable and "normal" use and acceptable behaviour making reference to bullying and harassment policy; how breaches will be dealt with/complaints procedure and regulation on review and update. As social networking can be used internally to promote levels of employee engagement and externally to help promote the organisational brand and reputation the policy may also include business objectives as well.³⁴ There is no one size fits all. The position of the employee within the workplace hierarchy as well as the tasks assigned to him is likely to influence the level of autonomy in relation to internet use (to what extent is he allowed to use Internet for private purposes during working time, how frequently is the internet use monitored).

When the employer drafts its policy employee involvement and continuous dialogue with the social partners are equally important. The German, French and Dutch systems present fine examples.

about the promiscuity of another person and stated that the limits to the concept lie in a requirement of a serious ideology, having some cogency and cohesion ...'.

³¹ Collins and Horne (2014) 14, 18.

³² See also ACAS Advice A-Z 'Promoting Employment Relations and HR Excellence' <<http://www.acas.org.uk/index.aspx?articleid=3375>> accessed 28 January 2015.

³³ Szőke (2014) 14.

³⁴ ACAS (n 32).

6. A DOUBLE-EDGED SWORD. WHERE DO WE STAND NOW?

The rapid spreading of social networking sites undoubtedly poses new challenges. The employers' rights and interests collide with the applicants' and the employee's right to respect for their private life, freedom of expression as well as their right not to be discriminated. In many respects, these new channels of communication are double-edged swords, with both beneficial and adverse effects. On the bright side, it is undeniable that SNSs provide new, effective forums for people (and workers) to communicate about different issues; they shape identity and create new cultures. Let us also not forget that SNSs may very well serve the interest of the employer. Many firms advertise their products or services on their Facebook profile and even encourage their employees to support them in forms of likes and comments. SNSs may act as a new channel for HR strategy as well; employers may place job advertisements on Facebook or communicate with present employees. In addition SNSs may provide an informal forum of discussion between management and labour; and an effective way to keep employees informed about the latest developments and receive feedbacks.

Clearly, SNSs have a dark side as well. As these channels of communication make information relatively easy to access (even with strict privacy settings) they provide the employer additional opportunities to monitor and inspect the employees' conduct, on occasion even the most private aspects of it. Some scholars even argue that the birth of social media heralded "the beginning of the end of privacy".³⁵ Monitoring the SNSs may lead to unethical and/discriminatory practices. Obviously, the coin has two sides. The most common threats posed for the employers include misuse of confidential information, misrepresentation of the views of the business, inappropriate non-business use, disparaging remarks about the business or co-workers and harassment.³⁶

Regarding pre-employment, a clear-cut solution would be to avoid a pre-employment Google search in general (see the Finnish example above). On a theoretical level, such a system can be backed up by referring to the very nature of SNSs: these sites operate without pre-edition, or any kind of previous control. They therefore enable expression of very diverse and unfiltered opinions. The possibility of background checks may have a destructive impact on the quality of online human interaction, in the long run they may force users to create duplicate profiles, and censor their online activities for fear of being judged by their future employer. The acceptance of unregulated monitoring practice may render a widespread and otherwise useful communication medium dangerous for people to use.³⁷ Yet, I think imposing a complete ban on pre-employment screens is not feasible mostly because the invisibility of the search and the benefits it offers for the employer (it is a fast, cheap and easy way to gain many information including red flags). The solution the UK Information Commissioner's Office advocates, that is to notify the candidates about the background checks and document data which is collected, is more realistic. A written policy that specifies what information or sites will be consulted before the decision is made, who will conduct the review, and what records will be maintained helps to prevent possible lawsuits. Before hitting "search" it is also advisable that the employer ask him- or herself if

³⁵ Sanders (2012) 243.

³⁶ Proskauer Rose, LLP, Social Media in the Workplace Around the World 3.0. [2014] 2 <<http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf>> accessed 28 January 2015.

³⁷ Clark and Roberts (2010) 507.

the search fulfils the general requirements of processing data or not. Is it reasonable? Are there other, less intrusive measures available? For the time being the candidates (and later on the employees) may protect themselves against invasion into their privacy mainly by being cautious about what information they share online and by choosing their privacy settings wisely. This of course presupposes a certain awareness of one's digital footprint.

As to the adverse effects, the biggest concern is the issue of how to provide evidence. Even though in discrimination cases the burden of proof is reversed, employment discrimination can often be difficult to prove. Though, unfortunately candidates are seldom in the position to present a *prima facie* case for discrimination, successful cases such as the one concerning the job at University of Kentucky cited above give rise for optimism.

Regarding the employment stage here again, unreasonable and extensive restriction is likely to motivate the employees to create two profiles, one official with their real name and an anonymous one, and air their critiques through the alias. SNSs are by no means a no-man's land where anything goes. As we can see in the cases discussed earlier, neither the online environment nor the privacy expectations of the employee provide a shield against actions such as harassment or harming legitimate business interests. These actions may result in disciplinary action including termination just like they would in "real life". The employment consequences depend on classic factors (such as degree of harm) but also factors specific to SNSs (e.g. privacy settings).

Regarding both stages the current, typical practice (i.e. unregulated and boundless monitoring) goes against the most basic principles of lawful data processing, it is unlikely to change because of two main reasons. Firstly, the employers are tempted too much by the already-mentioned benefits. Secondly, while users do not intend their (future) employers to see their posts and pictures on Facebook or Twitter, it is them who make it possible for the public, including employers to access information on their profile. The desire of self-expression, information sharing, networking, etc. is dominant when the profiles are shaped. The opposite desire, for a clear separation of work and private life, the wish for solitude surfaces later or too late. Employment related search on social networking sites remains in the grey zone of law. For the benefit of all concerned, reasonableness and adoption of a clear policy on SNSs appears to be the best solution.

LITERATURE

- Allen QC, R., Crasnow, R. and Beale, A., *Employment Law and Human Rights* (2nd edn, Oxford UP 2007)
- Arany Tóth, M., *A munkavállalók személyes adatainak védelme a magyar munkajogban* (Bába K. 2008)
- Boyd, D. and Ellison, N., 'Social Network Sites: Definition, History, and Scholarship' (2008) 13 *Journal of Computer-Mediated Communication* 210.
- Brown, R. B. and Vaughn, E. D., 'The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions' (2011) 26 *Journal of Business and Psychology* 219-225.
- Carlson, K., 'Social Media and the Workplace: How I Learned to Stop Worrying and Love Privacy Settings and the NLRB' (2014) 66 *Florida Law Review* 479-509.
- Castells, M., *The Rise of the Network Society: The Information Age: Economy, Society and Culture* (vol 1, 2nd edn, Wiley Blackwell 2010)
- Clark, L. A. and Roberts, S. J., 'Employer's Use of Social Networking Sites: A Socially Irresponsible Practice' (2010) 95 *Journal of Business Ethics* 507-525.
- Collins, E. and Horne, S., 'Social Media and International Employment' in Erika Collins (ed), *The Employment Law Review* (5th edn, Law Business Research Ltd. 2014)

- Craig, J. D.R., *Privacy and Employment Law* (Hart 1999)
- Fülbier, U., 'Labor Courts in Germany extend Employer's Rights to Monitor and Control Employee IT Device' ORRICK (2012) <<http://blogs.orrick.com/employment/2012/10/30/labor-courts-in-germany-extend-employers-rights-to-monitor-and-control-employee-it-devices/>> accessed 26 September 2014
- Grimmelman, J., 'Saving Facebook' (2009) 94 Iowa Law Review 1137–1206.
- Hajdú, J., *A munkavállalók személyiségi jogainak védelme. Az adatvédelem alapkérdései* (Pólay Elemér Alapítvány 2005)
- Hegedűs, B. and Kerekes, Zs. (eds), *Adatvédelem és információszabadság* (CompLex 2010)
- Horváth, L., and Gelányi, A., 'Lájkolni vagy nem lájkolni? A közösségi oldalak használatának munkajogi kérdései' (2011) 43/8 Infokommunikáció és Jog 60–66.
- Manant, M., Pajak, S. and Soulié, N., 'Online Social Networks and Hiring: A Field Experiment on the French Labor Market', *Social Science Research Network* <<http://dx.doi.org/10.2139/ssrn.2458468>> accessed 9 August 2014.
- McGeeveran, W., 'Finnish Employers Cannot Google Applicants', *Information Law* (15 November 2006) <<http://blogs.law.harvard.edu/infolaw/2006/11/15/finnish-employers-cannot-google-applicants/#more-187>> accessed 9 August 2014
- Neal, L. K., 'The Virtual Water Cooler and the NLRB. Concerted Activity in the Age of Facebook' (2012) 69 Wash. & Lee L. Rev. 1715–1758.
- Németh, J., 'Az internet nem felejt – közösségi média-használatra alapított munkáltatói és munkavállalói felmondások' (2013) 55/10 Infokommunikáció és jog 96–98.
- Pók, L., 'A közösség hálójában – Közösségi oldalak munkajogi vonatkozásai' (2012) 48/9 Infokommunikáció és Jog 10–17.
- Post, R. C., 'Three Concepts of Privacy' (2000–01) 89 Georgetown Law Journal 2087–2098.
- Roessler, B. and Mokrosinska, D., 'Privacy and Social Interaction' (2013) 39 Philosophy & Social Criticism 771–791.
- Proskauer Rose LLP, *Social Media in the Workplace Around the World 3.0* (2014) 2 <<http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf>> accessed 28 January 2015.
- Sanders, S. D., 'Privacy is Dead: The Birth of Social Media Background Checks' (2012) 39 S U L REV 243–257.
- Szőke, G. L., 'Az önszabályozás, audit és tanúsítás lehetőségei és korlátai az adatvédelem területén' (2014) 11 Infokommunikáció és Jog 14–20.
- Szőke, G. L. (ed), *Privacy in the Workplace: Data Protection Law and Self-regulation in Germany and Hungary* (HVG-ORAC 2012)
- Waring, R. L. and Buchanan, F. R., 'Social Networking Web Sites: The Legal and Ethical Aspects of Pre-Employment Screening and Employee Surveillance' (2010) 4 Journal of Human Resources Education, 14–23.
- Warren, S. and Brandeis, L., 'The Right to Privacy' (1890) 4 Harvard Law Review 193–220.