HUNGARIAN LABOUR LAW
E - J O U R N A L

Social networks and employees' right to privacy in the pre-employment stage: some comparative remarks and interrogations[1]

Edit Kajtár[*] – Bruno Mestre[**]

1. Enunciation of the problem

Let's face it: we have all done it! Any regular user of social networks/social networking sites (hereinafter also SNSs) has at one point used them to look for someone in particular without being noticed; it may be that crush, that first college boyfriend/girlfriend, those classmates we (dis)liked, our neighbour, anyone who happens to arouse our curiosity. Herbert refers to this phenomenon as "electronic voyeurism".[2] These behaviours may be morally questionable but they are for the most part innocuous unless the person decides to use that information for a specific purpose. Alternatively, this situation takes a completely different dimension when the individual looking for information does so in the context of an employment relationship.[3]

Employment is a very important facet in everyone's life and it is perhaps the feature in which an individual holds the most important stake. If someone decides to look up for information on another individual for job related purposes, it is seldom out of sheer curiosity or for innocent reasons. Any information gathered about someone in an employment context may and will certainly be used vis-à-vis that person in the normal development of the employment relationship. This is particularly important in the pre-employment stage, in which someone is under the process of selection for a

1 This paper was written with the support of the Hungarian Scientific Research Fund – OTKA, PD 109163 grant and OTKA K 109457 grant.

* Ph.D., professor assistant at WU Wien, Welthandelsplatz 1, 1020 Wien Austria, edit.kajtar@wu.ac.at

** PhD in Labour Law by the European University Institute, Florence; formerly lecturer of Labour Law and European Law at IPCA – Instituto Politécnico do Cávado e do Ave and Universidade Lusófona do Porto; currently Judge.

2 William A. Herbert: Workplace Consequences of Electronic Exhibitionism and Voyeurism. *IEEE Technology and Society Magazine*, vol. 30, no. 3, (2011) 25–34.

3 Michael Jones – Adam Schuckman – Kelly Watson: The Ethics of Pre-Employment Screening through the Use of the Internet. In: *The Ethical Imperative in the Context of Evol.ving Technologies.* Ethica Publishing, 1996. <http://www.ethicapublishing.com/3contents.htm>.

particular job. Employment contracts are relational contracts and the adequacy of someone for a particular job can seldom be reduced to the qualifications exhibited in a CV and the personal image sold in a presentation letter; personal aspects of an individual are of paramount importance in the normal development of an employment relationship. Therefore the "temptation" to discover the "true face" of the applicant using the information freely disclosed in social networks may be overwhelming.[4]

This situation is particularly important in the US where the existence of the tort of negligent hiring has spawned a number of precautions on the part of employers in order to be assured of the true character of the applicant. The omnipresent market has even given birth to companies specialising in undertaking background checks on individuals upon request using solely the information available on the internet. Despite the potential danger of these practices, there has been very few litigation concerning them because regulators acted promptly – and perhaps precipitately – in order to bring some discipline to these practices. There has been an intense discussion on the adequacy of the regulatory framework and on an ideal regulation that could protect business interests without an excessive interference on employees' right to privacy. Similarly, there has also been a jurisprudential discussion in Brazil concerning these practices.

The purpose of this work is to present a comparative analysis on the protection of personal data in the pre-employment stage. We will compare the US, the Brazil and the EU. We also provide some thoughts on the nature of these digital channels of communication and examine the potential dangers from the angle of privacy protection and anti-discrimination.

2. Social networks and the pre-employment stage – a complex problem

As a preliminary point, it is useful to expose the reader the surrounding the use of social networks in the pre-employment stage. The issue is far more complex than it appears because, notwithstanding the undeniable right to privacy of the applicant, there may be a legitimate business interest in making a preliminary screening of the job applicant, which may even run in the interest of the applicant him/herself. This point is structured as follows: firstly, we will provide a possible definition of the concept of "social network" stressing the conflict between the intended audience of the network and the actual audience; secondly, we will provide an enunciation of the most common practices concerning the use of information of job applicants available in social networks; thirdly, we will attempt to provide some possible justifications on the use of these methods.

There is a wide variety of definitions of social networks but the majority stress three fundamental aspects: they are web-based services which (1) allow an individual do construct an individual profile identifying him/her, (2) integrate that profile within a bound system, articulating a list of users with

[4] Franz Marhold: *Datenschutz und Arbeitsrecht*. Wien, Signum-Verlag, 1986. 2. See also: Edit Kajtár: The Dark Side of Facebook: Employee Misconduct on Social Networking Sites. *Revista de Dereito Público,* 2015. (forthcoming).

whom to share connections and (3) view and cross the connections within the system. The user chooses which information is disclosed in the network and who can have access to it; some profile pages can be seen even by people not integrated in the network by means of a simple search using a normal search engine; others are available only to people who possess a similar page in the network and finally some pages are disclosed only to selected people.[5]

There is a wide variety of networks organized in accordance with its users' interests. "Facebook" is a social network intended primarily for a personal use; "LinkedIn" is a social network intended for professional use; "Instagram", "Vine", "Reddit" and "Tumblr" may be defined as thematic social networks in the sense that they allow users to share – respectively – user-edited photos, short videos and start a discussion on themes of common interest (such as sexuality related issues, depression, gender issues, divorce, marriage, baby nurturing, relationship advice, anything) with users sharing similar interests.[6]

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 are products of what the Spanish sociologist and cybernetic culture theoretician Manuel Castells calls "*global network society*", a society where the guiding principle is "*being online*".[7] SNSs differ from physical places in many respects: they are mediated and potentially global, searchable, 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.[8] The popularity of these sites lies in their social functions. 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.[9]

One of the most important aspects to have in mind when considering social networks is the distinction between the "intended audience" and the "actual audience". Users disclose information having in mind an intended audience and not necessarily the actual audience. When examining the information disclosed by college students in their individual Facebook pages, Tenenbaum refers that many students made a conscious attempt to portray a particular image and that those who posted problematic information did so to impress a particular audience, their peers;[10] the information displa-

---

5 See https://en.wikipedia.org/wiki/Social_network; also Robert Sprague: Invasion of the Social Networks. Blurring the Line between Personal Life and the Employment Relationship. *University of Louisville Law Review*, vol. 50, no. 1, (2011) 50.;. Jason M. Tenenbaum: Posting Yourself Out of a Posting: Using Social Networks to Screen Job Applicants in America and Germany. (Hofstra University School of Law) *Social Science Research Network (Blog),* March 12, 2012 <www.SSRN.com>

6 Karolin Andréewitch: Die Privatnutzung von Social Networks am Arbeitsplatz. Die Regelung der Privatnutzung von Social Networks aus arbeitsrechtlicher Perspektive sowie Kontroll- und Sanktionsmöglichkeiten des Arbeitgebers. *Arbeits- und SozialrechtsKartei*, 2015., 52–57., 54.

7 Manuel Castells: *The Information Age: Economy, Society and Culture.* Vol. 1. *The Rise of the Network Society.* Chichester, Blackwell, 2010. 406.

8 Danah M. Boyd – Nicole B. Ellison: Social Network Sites. Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, vol. 13., no. 1, (2007) 210.

9 James Grimmelman: Saving Facebook. *Iowa Law Review*, 2009. 1206. See also: Edit Kajtár: Till Facebook Do Us Part? Social Networking Sites and the Employment Relationship. *Acta Juridica Hungarica: Hungarian Journal of Legal Studies*, vol. 56., no. 4. (2015) 2.

10 Tenenbaum (2012) ibid.

yed in a personal page is seldom the same disclosed in a professional page because the *intended audience* is not the same. This is – of course – merely an extension of our own personality: we are not the same person with our friends and loved ones, at work or even alone; we have distinct dimensions of our personality which manifest themselves in distinct contexts. Social networks are simply an on-line projection of those distinct personality traits.

There is a wide variety of ways through which an employer may gain access to information on an individual applicant disclosed in a social network. This enumeration will grow from the least to the most intrusive form of interference:

a) *Screening info* – this is the least intrusive way of searching for information about a job applicant and it simply consists on "googling" the name of the applicant and analyse whatever information is there freely available to anyone;
b) *Changing privacy settings* – this second more intrusive form of searching information consists in demanding access to the personal profile of the person; the employer will demand to be "friended" or to have somehow access to the information disclosed by the applicant in that page; this is more problematic because if the information was kept private from third parties, it generally means that those third parties were not included in the intended audience;
c) *Shoulder surfing* – a third more intrusive form of searching for information consists in demanding that the applicant log into the page and then observe it as it navigates through the content displayed; this provides an idea of the information disclosed by the applicant but also of the types of social relations nurtured by the applicant;
d) *Demanding login credentials* – this final more intrusive form of interference consists in simply demanding the login credentials of the social network webpage and thoroughly examine its content.[11]

There are a number of reasons why employers choose to look for online information about their prospective employees, some of them are not necessarily against the interests of the employee. The following paragraphs will attempt to discuss the most common justifications offered for these pre-employment screening tests.

Firstly – the most obvious one – employers do so in order to get a better idea of the applicant. Employment contracts are relational contracts (meaning that the contracts are based upon a relationship of trust between the parties; the explicit terms of the contract are simply an outline of the most important aspects governing the development of the relationship between the parties to the contract)[12] and the personality of the individual is often a very important dimension in the normal

11 Susan Park: Employee Internet Privacy: A Proposed Act That Balances Legitimate Employer Rights and Employee Privacy. *American Business Law Journal*, vol. 51, no. 4, (2014) 51., 779–841.

12 Júlio Gomes: *Direito Do Trabalho.* Coimbra, 2007. 81–94; I. R. Macneil: Contracting Worlds and Essential Contract Theory. *Social and Legal Studies*, 9, (2000) 431–ff.

development of the employment relationship. The potentiality of the applicant for a job is – fortunately – seldom reducible to the formal qualifications attested by certificates and the personal image sold by the prospective employee in the presentation letter (examples of which can be easily found on the internet and are increasingly circulated in job workshops and similar activities). Considering that the information available in the personal profile of the applicant is freely disclosed by him/her, it may help to provide a perhaps more accurate idea of the person behind the CV. We say "perhaps" because the opposite may also be true, all depending on the information available and the intended audience of it. A Facebook profile whose intended audience are primarily close friends, old classmates and relatives may not necessarily provide an adequate image of the professional behaviour of the applicant.

Secondly, the personal information obtained via social networking sites may also help to combat statistical discrimination. This is a type of discrimination in which a person attempts to offset the lack of information about an individual by attributing to him/her several assumptions about the group to which that individual belongs.[13] In Europe, Roma/Gypsies are assumed to have a low educational level and originate from socially disintegrated backgrounds; the same is also assumed in the US of African-Americans and Hispanics (note: *the authors DO NOT endorse any of these views*). Although in general Roma/Gypsies, African-americans and Hispanics are historically plagued by institutional problems of social integration, education and academic achievements, the same does not necessarily hold true about individuals pertaining to these groups. The "screening process" may serve as a means of fighting this type of discrimination by allowing an individual to be evaluated by its merits rather than by the assumptions about his/her group. However the contrary may also be true and discovering elements about the individual's ethnicity may contribute to a discriminatory employment decision, the proof of which is quite hard to establish in the pre-employment stage.

Finally, in the particular case of the US, the pre-employment screening may be justified by the tort of negligent hiring. This tort may make an employer directly or vicariously liable for the tortious conduct of its employee if the employee (the tortfeasor) had a reputation or record that showed his/her propensity to misuse the kind of authority given by the employer, and this record would have been easily discoverable by the employer, had the employer exercised "due diligence"; this is particularly important in situations of sexual harassment and assault in the workplace.[14] In the European context the employer is liable for the actions of its employees irrespective of the hiring decision. The doctrine of negligent hiring does not apply, as the liability is objective. It appears perfectly reasonable to undertake background checks in order to avoid liability and guarantee a safe working environment. Nevertheless there are also two sides to the same coin: the existence of a previous situation of harassment does not

13 Lior Jacob Strahilevitz: Privacy versus Antidiscrimination. *Public Law and Legal Theory Working Paper University of Chicago Law School*, 2009.

14 Stephen F. Befort: Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place. *Hofstra Labor and Employment Law Journal*, 14, (1997) 365–ff.

mean that the situation is going to happen again; the posting of sexual content in a personal profile in a social network does not make the person a sexual harasser or a potential danger for the employees.

The former paragraphs attempted to illustrate the complexity of the situation. There is a wide variety of social networks, in accordance with the interests of the users, with distinct levels of privacy, users post different contents in those networks having in mind a certain intended audience, there are a number of forms to have access to those contents and finally there are also several reasons why employers may have a legitimate interest to have access to that content – some of which may be misused. The following lines will attempt to demonstrate the regulatory response to those practices.

3. The regulatory reaction – a comparative overview

One of the most striking features concerning these practices is the lack of litigation. This does not mean – of course – that only a few employers screen job applicants in social networking sites or that the practice of demanding access to personal profile is reduced to a number of limited incidents. Quite the contrary: Tenenbaum reports that circa 45% of American employers admitted to undertaking background checks on job applicants on social networking sites.[15] However few of these situations reached the courts; Prague even boldly affirmed that there have been no published cases on this issue.[16] There is a possible justification for this; in the context of US Law, the absence of litigation is due perhaps to the fact that state legislators acted promptly upon the situation issuing a number of statutes; this situation contrasts starkly with the Brazil, where there has been a number of cases concerning the legality of background checks of employees in public registers and there is a considerable debate on the legality of using social networks to undertake these checks; whereas in Europe with some exceptions (see below) the issue received considerably less attention. The following lines will attempt to make a brief comparative outline of the regulatory response to these issues.

Levinson reports a very interesting reaction to employers' pre-employment screening practices such as those outlined above because it is not based on employment law, data protection law or even privacy law but simple good, old contract law.[17] Levinson reports that a (famous) social media company included in its statement of rights and responsibilities that users should not share their login credentials and it warned that it would initiate legal action against third parties – in particular employers – who shared or solicited a password. In terms of contract law, this could be construed as a form of inducement to breach a contract (a.k.a tortious interference), i.e: a situation in which a third party to a contract induces one of the parties to not comply with one of the explicit terms of the

15 Tenenbaum (2012) ibid.

16 Sprague (2011) ibid.

17 Ariana R. Levinson: Social Media, Privacy, and the Employment Relationship: The American Experience. *Spanish Labour Law and Employment Relations Journal*, 2013/2. 15–31.; Ariana R. Levinson: Carpe Diem: Privacy Protection in Employment Act. *University of Louisville School of Law Research Paper Series,* 2009.

contract and share their login credentials, allowing the third party to observe both the information posted by the user as well as information posted by the friends of the user to which the user would have access.

This is a very interesting reaction because it is – at the same time – quite simple and quite complex. It is simple because it merely consists in inserting in the explicit terms of the contract a clause stating that the user should not share its login credentials with any third parties in particular when applying to a particular job; it is complex because not all jurisdictions recognise the tort of inducement to breach a contract and even in those who do so, it is still the subject of a dispute (particularly in Continental Europe).

In the United States, the main reaction appears to have been at the state level. Following the heavy publicity surrounding these employment practices, many authors report that state legislatures reacted promptly, enacting a number of statutes prohibiting these practices. Susan Park reports that by mid-term 2014, a total of 17 US states had enacted legislation prohibiting certain pre-employment screening practices and that a total of 27 other US states had introduced bills in their national legislatures in order to counter the problem.[18]

However, the same author also notes that albeit the problems may be the same, the regulatory answer is widely divergent; for example, Susan Park reports the difference of definition of "personal internet account" in the statutes of Utah and Michigan: the first legislature defines it "*as one that is created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data*"; the second legislature defines it as an "*online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer*"; the first definition is considerably wider as it covers both personal and professional accounts (such as Facebook and LinkedIn) whereas the second limits its scope to personal accounts (such as Facebook only). The same is also true to the prohibited acts: the author refers that although virtually all statutes prohibit an employer from requesting an employee's login credentials, not all statutes prohibit "shoulder surfing" or demanding access to the personal page (for instance by changing privacy settings or adding the prospective employer as a "friend" in the user's list).[19] Robert Sprague undertook a very interesting taxonomic analysis of the different statutes, enunciating in each one of them the fundamental statutory prohibitions, the definitions, the exemptions and the remedies available to affected applicants.[20]

---

18 Park (2014) ibid.

19 Park (2014) ibid.

20 Robert Sprague: No Surfing Allowed: A Review and Analysis of Legislation Prohibiting Employers from Demanding Access to Employees' and Job Applicants' Social Media Accounts. *Albany Law Journal of Science and Technology,* vol. 24, no. 3, (2014) 481–513.

In the same line, many authors report that at the federal level, US Law offers a very feeble protection to job applicants due to the fact that employees are protected by a patchwork of legislation enacted in different time periods and in different circumstances and not having directly in mind these practices. The federal legal instruments applicable may be (1) the Discrimination statutes, (2) the Stored Communications Act, (3), the Fair Credit Reporting Act, (4) the National Labor Relations Board and (6) common law privacy claims.

As regards the discrimination statutes, the applicant could find shelter mainly in Title VII of the Civil Rights Act (T.VII), the Americans with Disabilities Act (ADA), the Age Discrimination in Employment Act (ADEA), the Bankruptcy Reform Act (BRA) and the Genetic Information Non-Discrimination Act (GTIA).[21] However, the protection is fragile and fraught with difficulties. Firstly, the employee has the burden of demonstrating that he is a member of a protected class; secondly the employee has the burden of demonstrating that s/he suffered adverse treatment on the basis of that protected characteristic or that the employer's practice had a disparate impact over that protected characteristic. Considering that the majority of these practices are protected by the anonymity of the internet or are demanded equally from all applicants, the applicant may find it difficult to prove that his/her rejection was based upon a protected characteristic.

The Stored Communications Act (SCA) also provides for some protection. This act was enacted as Title II of the Electronic Communications Privacy Act of 1986 and it addresses voluntary and compelled disclosure of "*stored wire and electronic communications and transactional records*" held by third-party internet service providers (ISPs); social networks perfectly fit this description. In the ruling *Pietrylo v. Hillstone Rest. Group*[22] from the Federal District Court of New Jersey, the court held that an employer was liable for violation of the SCA when the employer demanded that two of its employees provided their login credentials for a page in a social network (named Myspace) where employees used to submit their grievances in a password protected environment accessible only to those who were in possession of those credentials. Nevertheless, the adequacy of this act for providing an adequate protection for employees has been challenged because it is outdated (it dates from 1986), complex and confusing: for instance, Susan Park reports that courts have answered differently the applicability of the act to email messages sent between employees or between employees and third parties and although it is generally agreed that it opposes the practice of requesting employees' passwords, it is subject to a debate if the legislation covers other controversial practices such as shoulder surfing or changing privacy settings.[23] On the other hand, Sanchez Abril et allii report that the protection afforded by the SCA does not apply when the employee makes the digital information

21 Since the USA lacks a coherent non-discrimination act, such as the one found in the UK or Germany, these are the main acts.

22 Pietrylo v. Hillstone Rest. Group, Case number 06-5754 (FSH); see http://www.dmlp.org/threats/hillstone-restaurant-group-v--pietrylo#description for info about the case and http://www.employerlawreport.com/files/2013/09/PIETRYLO-v-HILLSIDE-RESTAURANT.pdf for a copy of the decision (access in 21/08/2015).

23 Park (2014) ibid.

available to the general public; this could be the case of unprotected profile pages in any given social network which could be observed by any user of the network or by anyone through a simple internet search.[24]

The Fair Credit Reporting Act (FCRA) is a federal law regulating the collection, dissemination, and use of consumer information, including consumer credit information; under the FCRA, employers are required to follow specific procedures when they use consumer reporting agencies to obtain consumer reports or investigative consumer reports on employees and/or job applicants for "employment purposes"; covered reports can include credit checks, motor vehicle records and driving history and criminal background information and different types of information. In particular, §613 of the act requires that a consumer reporting agencies furnishing a consumer report for employment purposes inform the affected consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported, as well as maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date.

Tenenbaum reports that this act offers a very feeble protection because it is only applicable to consumer reporting agencies, i.e. when an employer requests a third party to compile that information; it does not apply to investigations undertaken by the employer himself or situations in which the employer requests permission to the applicant to conduct some background information.

The NLRB also offers very little protection to employees; firstly, because it only applies to concerted activity; secondly, because although the NLRB has issued a total of three reports concerning social media cases, it has yet failed to produce a report on the use of social media during the pre-employment stage; this failure to produce a report reveals that even this specialised body does not feel very secure when it concerns the hiring process, which is indicative of how sensitive this matter is.[25]

Another means of providing some relief to employees is the common law right to privacy particularly in the tort of *intrusion upon seclusion*; this tort occurs when a perpetrator intentionally intrudes, physically, electronically, or otherwise, upon the private space, solitude, or seclusion of a person, or the private affairs or concerns of a person, by use of the perpetrator's physical senses or by electronic device or devices to oversee or overhear the person's private affairs, or by some other form of investigation, examination, or observation intrude upon a person's private matters *if the intrusion would be highly offensive to a reasonable person*. However the application of this tort finds two important barriers: firstly, the expectation of privacy; secondly, the possibility of consent.

---

24 Patricia Sanchéz Abril – Avner Levin – Alissa Del Riego: Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. *American Business Law Journal*, vol. 49, no. 1, (2013) 63–124.

25 https://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media (access at 21/08/2015).

As regards the expectation of privacy, it is debatable to which extent an applicant may expect his social media profiles to remain private. For instance, Philip Gordon refers that no court has ever construed the tort of invasion of privacy by intrusion upon seclusion so broadly as to protect the activity of a user who has more than 500 "friends" on Facebook and who expects to use the privacy settings of the social networking site to protect his/her activity; that tort requires a "private fact" which can be the subject of an intrusion; the vast majority of courts have held that, if the fact that is the subject of the claim has been disclosed to even a few people not under a legal or contractual obligation of confidentiality, the fact is not private and the intrusion upon seclusion claim fails.[26] The same author refers the precedent of *Nader v. General Motors Corporation* in which the Supreme Court of the US considered that there was no violation of the applicant's right to privacy when a company interviewed the applicant's acquaintances in the process of an autonomous investigation hoping to discover some information that the applicant could have revealed to his/her acquaintances; the applicant could not expect that the right to privacy cover information freely disclosed to third parties. The same could be said about information freely disclosed to hundreds of Facebook "friends".

Brazil is a curious case because, in contrast to the US, the issue has been dealt with mainly in the courts albeit the judicature is still very much divided on the subject. Despite the fact that some situations were heavily reported in the press, the courts have yet to reach a harmonious conclusion. The Brazilian Supreme Labour Court (Tribunal Superior do Trabalho) ruled in the affair Barbosa Comercial Lta[27] that it was not discriminatory nor against the principle of human dignity enshrined in the Brazilian constitution for employers to undertake a preliminary assessment of the candidates to a certain position by consulting police records and its credit worthiness; the Brazilian Supreme Labour Court considered that since those records are publicly available and can be consulted by anyone, the applicant cannot reasonably expect privacy in relation to that data and cannot claim a moral damage because the prospective employer consulted publicly available data; the same Court added that the practice was not discriminatory because it is perfectly reasonable for a company to want to know more about the personal conduct of the employee in order to judge his adequacy to a certain position.

However this ruling is not at all pacific and it contrasts sharply with some precedents. For instance, in a previous ruling from 2008, the Brazilian Supreme Labour Court decided that employers could demand information about previous convictions by the applicants to a certain position even if that information is irrelevant to the position but that it could not demand information about applicants' credit worthiness.[28] In the same line of reasoning, the Brazilian Labour Court of Appeals decided in two previous rulings dated from 2009 and 2012 that employers could not consult information about

---

26 Philip L. Gordon – Amber M. Spataro – William J. Simmons: *Social Media Password Protection and Privacy – The Patchwork of State Laws and How It Affects Employers.* Littler Workplace Policy Institute, May 3, 2013.

27 Procedure Nº TST-RR-38100-27.2003.5.20.0005

28 ED-RR-9892100-27.2004.5.09.0014, Relator Ministro: Ives Gandra Martins Filho, Judgement date: 21/05/2008, 7ª Turma, Publication date: 30/05/2008;

applicants' credit worthiness in order to fundament their hiring decisions on grounds of violating the applicant's right to privacy.[29]

These rulings reveal that in Brazil, the issue has been discussed mainly in Courts and judges have yet to find a definitive conclusion on the employee's right to privacy in relation to publicly available data. Although there have been no reported cases concerning the use of information available in social networks during the hiring process, the precedents related above could form a basis for considering that if the information is publicly available then the employer could rely on it to fundament his/her decision. In contrast, in relation to information available in social networks during the performance of the employment contract, the courts and the legal thinking have been more active; Christiane de Mello reports and analyses a number of cases in which courts allowed employers to rely on information publicly available in social networks, i.e. with an unrestricted access; if the information is not publicly disclosed then it is protected by the employee's right to privacy. The issue is still subject to a considerable dispute.[30]

4. Europe: Practice Shaped by National, International, Regional and Union Rules[31]

Within the European context, the legal assessment of a pre-employment Google search is shaped by the principles of data protection enshrined in documents such as: Directive 95/46/EC[32]; the OECD Guidelines on the Protection of Privacy (hereinafter: OECD Guidelines); the UN Guidelines[33]; the Council of Europe's Convention No. 108 (hereinafter: CoE Convention) as well as the national employment and data protection provisions. Below application of the following most important principles are examined: fair and lawful processing (as an overarching principle); data reduction and data economy; permission; purpose; direct collection; access; accuracy and limitation.

The overarching twin principle of fairness and lawfulness is the no. 1 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; personal data shall only be processed:

a) based on the data subject's unambiguous consent or processing is necessary for:

---

29 TRT-PR-30471-2009-084-09-00-3-ACO-27089-2011 - 2A. Turma; Relator: Rosalie Michaele Bacila Batista; Published at 08-07-2011; TRT-PR-05811-2007-594-09-00-4-ACO-00278-2009 - 2A. Turma; Relator: Ana Carolina Zaina; Published at 20-01-2009.

30 Cristiane Mello: *Direito de crítica do empregado nas redes sociais e repercussão no contrato de trabalho* (São Paulo). 2014., unpublished thesis.

31 This part is largely based on Edit Kajtár: Think it Over! Pre-Employment Search on Social Networking Sites. *Pravni Vjesnik,* 2015. Forthcoming.

32 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.

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

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 the principle of necessity, proportionality, purpose limitation and all the other general requirements discussed later in this paper. Out of the six grounds, those listed in (a), (b) and (f) appear to be reasonable candidates for justifying pre-employment 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 our 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 be considered as necessary steps made at the request of the data subject. Linked-in and alike sites are exceptions, here the users are present online for professional reasons and provide job-relevant information deliberately to future customers, clients and employers. However, even in these cases the accuracy of information obtained needs to be verified.

The employer may also try to rely on Art. 7(f). To select the best possible candidate is a legitimate interest. Careful selection is also important because the employer is liable for the damage caused by actions of employees committed within the scope or course of employment. 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. However it has to be balanced against the candidate's rights and interests (to express him- or herself freely, right to private life, etc.). It is also noteworthy that less intrusive measures are available to check the validity of the statements of the candidate. The employer may (with the consent of the candidate) ask for reference about the former employee or search public databases (classified directory for example).

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.

The collection, processing and use of personal data are only admissible if either it is expressly permitted by legal provision or the data subject has expressly consented in advance. Generally no legal provision exists (except in relation to certain specific categories of workers) and the permission is also missing. In line with the principle of purpose, the purposes for which data is be 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 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 have the right to know what information is collected about them, for what reason 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 was demonstrated in the French test case cited above, 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 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.

On the national level the assessment of pre-employment Google search depends on the privacy awareness of the given country. Article 9 of the French Civil Code (Law No. 70-643, 17 July 1970) guarantees everyone a right to respect of his private life. Article L.120-2 of the Labour Code (Law No. 92-1446, 31 December 1992) allows only those restrictions on rights of persons or on their individual or collective liberties that are justified by the nature of the work and proportionate to that end. France was one of the first EU Member States to adopt a data privacy act (Act n 78-17 of 6 January 1978 on Data Processing). However, none of these acts address the employees' use of SNSs. On the other hand the access and processing of the employee's or applicant's personal information via SNSs is strictly

limited by general legal provisions. Asking applicants or employees for information unrelated to the job or their qualifications is prohibited.

For historical reasons Germany has one of the strongest data protection systems. The right to privacy is protected by the Constitution; and the Federal Data Protection Act[34] limits the employer's use of personal data to specific purposes of the employment relationship. The general rule is that collecting, using and monitoring personal data is prohibited unless the employee consents expressly in writing or the law expressly allows it. Unauthorised monitoring of private communication can be considered a criminal offense.[35] The law does not allow employers to ask employees to disclose their social media account details. According to case law the personal circumstances of an employee may be disclosed only to the extent to which a legitimate, justified and equitable interest of the employer exists in relation to the employment relationship.[36] The employer's ability to use employee data obtained from social media with respect to termination depends on the employer's policy on Internet use in the workplace.[37]

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.[38] 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"[39].

In Hungary growing interest is detectable among the scientific community towards the employment law implications of SNSs.[40] Due to the fact that there is no specific regulation, general principles

---

34 Bundesdatenschutzgesetz – BDSG.

35 Art. 206 Criminal Code, Art. 202 a Criminal Code – StGB.

36 Falk Hagedorn: *Privacy in the Workplace. National report on Germany.* June, 2011. < http://pawproject.eu/en/sites/default/files/page/web_national_report_germany_en.pdf > 33–34.; Peter Gola: Von Personalakten- und Beschäftigtendaten. *Recht der Datenverarbeitung*, vol. 27., no. 2., (2011) 66–68.; Jan Tibor Lelley – Florian Müller: Ist § 32 Abs. 6 Satz 3 BDSG-E verfassungsmäßig? *Recht der Datenverarbeitung*, vol. 27., no. 2., (2011) 59–66.

37 Erika Collins – Suzanne Horne: Social Media and International Employment. In: Erika Collins (ed.): *The Employment Law Review.* 5th ed. London, Law Business Research Ltd., 2014. 18.; Hans-Joachim Reinhard: Information Technology and Workers' Privacy: the German Law. *Comparative Labor Law & Policy Journal,* 2001-2002, no. 2. 384.

38 William McGeveran: Finnish Employers Cannot Google Applicants. *Information Law, (blog)* 15 November 2006. < http://blogs.law.harvard.edu/infolaw/2006/11/15/finnish-employers-cannot-google-applicants/#more-187 > accessed 9 August 2014.

39 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.

40 See for instance Pók, László: A közösség hálójában – Közösségi oldalak munkajogi vonatkozásai. *Infokommunikáció és Jog,* vol. 48, 2012. 10–17.; Horváth, Linda – Gelányi, Anikó: Lájkolni vagy nem lájkolni? A közösségi oldalak használatának munkajogi kérdései. *Infokommunikáció és Jog*, vol. 43, 2011. 60–66.; Németh, Janka: Az internet nem felejt – közösségi média-használatra alapított munkáltatói és munkavállalói felmondások. *Infokommunikáció és Jog,* vol. 55, 2013. 96–98., 96.; Szőke, Gergely László (szerk.): *Privacy in the Workplace: Data Protection Law and Self-regulation in Germany and Hungary.* Budapest, HVG-Orac, 2012.; Böröcz, István: A munkahelyi érdek-összeütközés rendhagyó formája: munkavállalók megfigyelése pró és kontra. *Infokommunikáció és Jog*, vol. 55, 2013. 99–101. For an overview on the national data protection law at workplace see e.g. Arany

as well as contractual rights and obligations of the parties gain relevance. The law of personal data protection in employment context is, like in other countries, lagging behind technology.

In Portugal, the situation is expressly addressed in art. 16, n. 2 and art. 17 of the Portuguese Labour Code. The first provision enshrines the employee's right to privacy and it states that the right to privacy embraces any kind of access to information on the intimate sphere of the parties, in particular related to the family life, love life and sexual life, health and religious and political ideologies; although it only refers to "employees" it may be constructed also to embark candidates to a job. The second provision is specifically addressed to applicants to a specific job and it states that the employer may demand no information on the applicant's private life save when that information is strictly necessary to evaluate the applicant's aptitude to perform the job and the employers provides a written justification. The fact that the employer needs to provide a written justification effectively eliminates the legality of any hidden searches in SNS such as the ones we have been addressing in this paper.[41]

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. However, the employer may benefit from searching those SNSs that are intended to represent its members professionally (e.g. Xing, Linked In).[42] Due to lack of consensus the draft was rejected in 2013.

Google search does not only raise privacy concerns, it may also lead to discriminatory practice. 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 Google search is that the employer also collects information that he or she would not have the right to obtain during 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 or it simply does not fit with the image of the company.

Tóth, Mariann: *A munkavállalók személyes adatainak védelme a magyar munkajogban.* Szeged, 2008.; Hajdú, József: *A munkavállalók személyiségi jogainak védelme. Az adatvédelem alapkérdései.* Szeged Pólay Elemér Alapítvány, 2005.; Jóri, András (ed.): *Adatvédelem és információszabadság a gyakorlatban*. Budapest, CompLex, 2010.

41 Julio Gomes: *Direito do Trabalho.* Coimbra, 2007. 265 ff. See also José João Abrantes: Algumas notas sobre o direito do trabalhador à reserva da vida privada. In: F. Amaral et al (ed.): *Estudos Comemorativos dos 10 anos da Faculdade de Direito da Universidade Nova de Lisboa.* Almedina, Coimbra, 2008. Vol. II, 241–248.

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

In a recent field study conducted by academics at Université de 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 (hometown and language spoken). The twist of the experiment was that they only manipulated the Facebook profiles, not the application material, in order to be able to observe 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 finding was 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.[43]

5. Comparative conclusion

The only reasonable conclusion that we may extract from the current state of things is that we are walking on an unstable ground. Nearly everyone agrees that this is a subject in dire need of regulation; however nobody knows in which direction legislators and courts should go and the disparity in approaches and legal solutions reached briefly outlined above is a clear indicator of how delicate the issue is.

In the US, the reaction has been mainly at the legislative level albeit legislatures have adopted fairly distinct approached to the problem. The push toward the emergence of legal parameters to control the privacy aspects of SNSs in the employment context is a visible trend; 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 decisions.[44]

This situation contrasts starkly with Brazil, where the reaction has occurred mainly at the courts level and where the courts are discussing to which extent the employees' right to privacy enshrined in the Brazilian Constitution and Civil Code may prevent employers from searching for publicly available information about applicants. Although there is some consensus that they may do so in cases of public sector jobs in which there is a need for the reputation of the employee to be immaculate, there is a considerable discussion to which extent other employers may invoke the same reasons.

---

43 Matthieu Manant – Serge Pajak – Nicolas Soulié: Online Social Networks and Hiring A Field Experiment on the French Labor Market. *Social Science Research Network (Blog)* October 28, 2014<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2458468> Accessed: 30. 08. 2015.

44 Renee L. Waring – F. Robert Buchanan: Social Networking Web Sites: The Legal and Ethical Aspects of Pre-Employment Screening and Employee Surveillance. *Journal of Human Resources Education,* vol. 4., no. 2. (2010) 14–23., 19.

In Europe, pre-employment search on social networking sites is common practice, yet it mostly remains in the grey zone of law. Though 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 too tempted 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, the one for 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.

Obviously, banning pre-employment Google search in general (see the Finnish example above) would provide a clear cut solution. 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, 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, on 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.[45] Yet, 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 what data 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 on "search" it is also advisable that the employer ask him- or herself if 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 against 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

[45] Leigh A. Clark – Serry J. Roberts: Employer's Use of Social Networking Sites: A Socially Irresponsible Practice. *Journal of Business Ethics*, no. 4. (2010) 507.

difficult to prove. Though, unfortunately candidates are seldom in the position to present a prima facie case for discrimination, successful cases from the US such give rise for optimism.

As a concluding sentence, one can say that although the situation in Europe varies greatly due to the diversity of national legislations allowed by the relatively broad provisions of the Directive, there is a consensus on the need for regulation and on the most important aspects to be addressed: those could be – in our opinion – (1) a general principle of prohibition of job related SNS searches, (2) followed by a set of possible justifications in form of exceptions to the general principle and (3) a mechanism of external control and to whom employees could complain to. A possible means of addressing these issues could be in the form of a "model statute" which member states could implement in their national legislations followed by a report disclosing the solutions adopted in the national territory and the justifications thereof. However this is a simple contribution to an ongoing discussion on a relatively shaky ground.