BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 10, NUMBER 2 (2017)
ISSN 2029-0454

DE GRUYTER OPEN

Cit.: *Baltic Journal of Law & Politics* 10:2 (2017): 76–106
http://www.degruyter.com/view/j/bjlp
DOI: 10.1515/bjlp-2017-0013

EMPLOYERS AS NIGHTMARE READERS: AN ANALYSIS OF ETHICAL AND LEGAL CONCERNS REGARDING EMPLOYER-EMPLOYEE PRACTICES ON SNS

Seili Suder

Doctoral Student; MA
University of Tartu, Faculty of Law (Estonia)

Contact information
Address: Näituse 20, 50409 Tartu, Estonia
Phone: +372 626 9191
E-mail address: seili.suder@sm.ee

Andra Siibak

Professor; PhD
University of Tartu, Institute of Social Studies (Estonia)

Contact information
Address: Lossi 36, 51003 Tartu, Estonia
Phone: +372 737 5188
E-mail address: andra.siibak@ut.ee

Received: August 2, 2017; reviews: 2; accepted: December 12, 2017.

ABSTRACT

The aim of this interdisciplinary paper is to study the social reality surrounding the data processing practices employers and employees engage in on social networking sites (SNS). Considering the lack of empirical studies, as well as the considerable uncertainty in the way personal data protection is implemented across the European Union (EU), the paper offers insights on the topic. Qualitative text analysis of semi-structured interviews with employers

from the service sector (N=10) and the field of media and communication (N=15), as well as employers from organisations which had experienced various problems due to things their employees had posted on social media (N=14), and employees from the financial sector (N=15) were carried out to explore whether the data protection principles, which can be viewed as the most important guidelines for employers in the EU, are actually followed in their everyday SNS data processing practices. Even though the data protection principles emphasise the need for fair, purposeful, transparent, minimal and accurate processing of personal data, our interviews with employers and employees reveal that the actual SNS processing practices rarely live up to the standards. Our findings indicate that there is a growing mismatch between the social reality and legal requirements regarding data subjects.

KEYWORDS

Data processing, employers, employees, social media, data protection principles

NOTE

The preparation of this article was supported by the research funding project PUT 44 financed by Estonian Research Council. The authors are grateful to Eva-Liis Ivask, Greete Kempel, Mari Krusten and Hendrik Urbel for carrying out and transcribing the interviews.

INTRODUCTION

Various studies and court cases[1] indicate that the processing[2] (i.e. collecting, using, storing, recording and organising) of employees' personal data on social media in general, and social networking sites (SNS) in particular, may have a considerable effect on various human resource decisions, including hiring, training, promotion and termination. Although scholars have indicated two main legal and ethical issues surrounding these practices – the right of employer access to the employee's or applicant's online information, and the permissibility of basing hiring, promotion or dismissal decisions on the discovered digital information[3] – using information found on a SNS has become a routine practice in many human resource departments. Furthermore, in the context in which an employee is considered to act as a "business card" of an organisation, employers show a growing concern for the fact that many employees are making defamatory and outspoken remarks on social media about their organisations, supervisors, co-workers and clients. All of this has led to the blurring of boundaries between the personal and professional lives of employees and applicants and has started to create both legal and ethical minefields for employers[4].

Regardless of various real life cases in the European Union (EU) and growing public concern about the legal and ethical aspects of processing employee data, academic discussion and analysis of the topic has so far mainly been carried out in the US[5]. In fact, findings of the thematic review by El Ouirdi et al[6] indicate that the lack of studies investigating the "laws regulating this usage in geographical areas other than the US" is one of the major weaknesses of this research stream. Another

[1] CareerBuilder, "Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade" (April 2016) //http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=4%2f28%2f2016&siteid=cbpr&sc_cmp1=cb_pr945_&id=pr945&ed=12%2f31%2f2016; Jennifer Bond and George Waggott, "Social Media Policies in the Workplace: Case Studies" (2017) // https://www.go2hr.ca/articles/social-media-policies-workplace-case-studies; Victoria R. Brown and E. Daly Vaughn, "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decision," *Journal of Business and Psychology* Vol. 26, No. 2 (May 2011) // DOI:10.1007/s10869-011-9221-x; Sarah L. Bicky and Linchi Kwok, "Social Media as an Employee Recruitment Tool," 16th Graduate Students Research Conference (2011), Track 2, Poster Session // http://scholarworks.umass.edu/gradconf_hospitality/2011/Poster/94/; Louisa Peacock, "Employers watch Facebook usage," *Employers Law* (2008): 4.

[2] In this article, we use the term "processing" as it is defined in the General Data Protection Regulation Art. 4 Sec. 2: "processing" is any operation or set of operations which is(are) performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[3] Patricia Sánchez Abril, Avner Levin, and Alissa Del Riego, "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee," *American Business Law Journal* Vol 49, No. 1. (January 2012) // DOI: 10.1111/j.1744-1714.2011.01127.x.

[4] Kathleen Elliott Vinson, "The blurred boundaries of Social Networking in the Legal Field: Just 'Face' it," *University of Memphis Law Review* Vol 41 (2010).

[5] Asma El Ouirdi, Mariam El Ouirdi, Jesse Segers, and Erik Henderickx, "Employees' use of social media technologies: a methodological and thematic review," *Behaviour & Information Technology* Vol. 34, No. 5 (May 2015) // DOI: 10.1080/0144929X.2015.1004647.

[6] *Ibid*.: 458.

major weakness of literature on the topic that El Ouirdi et al point out is the lack of empirical work on employees' social media use.

1. THE BACKGROUND OF THE PRESENT STUDY

This interdisciplinary article aims to begin to fill the above-mentioned gaps in the literature. We make use of empirical data gathered during several small case studies carried out among Estonian employers working in the field of media and communication, and in the service sector, as well as employees from the financial sector, so as to study the social reality surrounding the data processing practices employers and employees engage in on public networks. Furthermore, we also rely on the findings of semi-structured interviews with the representatives of organisations which had experienced various problems due to things their employees had posted on social media so as to explore whether there is the mismatch between the social reality of data subjects and the legal reality of data protection in the EU that scholars[7] have referred to.

We believe that empirical research on the topic is crucial as there is considerable fragmentation and legal uncertainty in the way personal data protection is implemented across the Union. EU member states have a wide range of different rules regarding processing employees' personal data and there are large differences in the implementation, interpretation and enforcement of these rules[8]. In fact, EU member states not only have a wide range of different rules regarding processing employees' personal data, but according to the widespread public perception there are also significant risks associated notably with online activity.[9] Furthermore, regardless of the fact that the processing of personal data has grown exponentially with SNS,[10] the ethical and legal aspects of employers' right to availably search for or use information from SNS are rarely addressed at the national and EU levels. In reality, there is not a lot of guidance for employers who process data from employees' SNS.

[7] Norberto Nuno Gomes de Andrade and Shara Monteleone, "Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications": 129; in: Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet, eds., *European Data Protection: Coming of Age* (Dordrecht and Heidelberg, New York, London: Springer, 2013).
[8] *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Eur-Lex (COM/2012/011 final – 2012/0011 (COD)), 103.
[9] Special Eurobarometer, "Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union" (June 2011) // http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.
[10] European Commission, "Questions and Answers - Data protection reform" (December 2015) // http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm.

Today the legal framework for privacy and data protection in the EU is based upon the Data Protection Directive (DPD),[11] adopted in 1995. However, EU institutions have reached agreement on a new data protection regulation, establishing a modern and harmonised data protection framework across the EU. The primary aim of this regulation – The General Data Protection Regulation (GDPR)[12] – is to set forth rules to make sure people's right to personal data protection remains effective in the digital age.[13] The intent of the regulation is to strengthen and unify data protection for all individuals within the EU. The GDPR will replace the DPD and will go into effect on 25 May 2018, after a two-year transition period. Unlike a directive, it does not require that any enabling legislation be passed by national governments.

Irrespective of the changes in the EU framework, employers must still be aware that any collection, use or storage of personal data on employees by electronic means due to professional or commercial activity will fall within the scope of the EU data protection legislation[14]. However, the DPD and the GDPR are quite ambiguous concerning employers' right to process information from employees' social media accounts. In fact, the main source of legal guidance for employers comes from the data protection principles. These principles – lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability – have been enacted in the GDPR and derive from the DPD.

The principles have formed the basis for EU privacy legislation. Nevertheless, substantial doubts have been expressed as to whether the attempt to enforce the data protection principles through legislation has actually protected privacy.[15] Scholars have identified issues that should be resolved in order to accommodate privacy principles in different environments[16] and they argue that these principles have increasingly been reduced to narrow, legalistic principles that place the burden of protection on the individual rather than on society and its institutions.[17] However,

[11] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal of the European Union (L 281, 23.11.1995, 31–50).
[12] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Official Journal of the European Union (L 119, 4.5.2016, 1–88).
[13] European Commission, *supra* note 10.
[14] *General Data Protection Regulation*, *supra* note 12, art. 2, sec. 1.
[15] William Bonner and Mike Chiasson, "If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy," *Information and Organization* Vol. 15 No. 4 (October 2005) // DOI: 10.1016/j.infoandorg.2005.03.001.
[16] Maria Karyda, Stefanos Gritzalis, Jong Hyuk Park, and Spyros Kokolakis, "Privacy and fair information practices in ubiquitous environments: Research challenges and future directions," *Internet Research* Vol. 19, No. 2 (April 2009) // DOI: 10.1108/10662240910952346.
[17] Fred H. Cate, "The Failure of Fair Information Practice Principles": 341-378; in: Jane K. Winn, ed., *Consumer Protection in the Age of the 'Information Economy'* (Routledge, 2006).

in its opinion from 2017 on the future of privacy, the Article 29 Data Protection Working Party[18] confirmed that the principles of data protection are still valid and even more important than before due to development of new technologies and new methods of data processing.[19] Nevertheless, the earlier opinions of this working party have also acknowledged the need for better application of these principles in practice.[20]

The lack of application of data protection principles in Europe was under scrutiny in the recent case of Bărbulescu v Romania in the European Court of Human Rights (ECHR). In this case Mr Bărbulescu was dismissed after creating a Yahoo Messenger account for personal reasons during working hours, despite the strict prohibition in employer's internal regulations. The court noted that countries must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic communications of a non-professional nature by its employees. However, the Court accepted that this discretion was not unlimited and prescribed a number of criteria which should be assessed in case of monitoring. The criterion relies on the extensive international law framework and its data protection principles. In this case the ECHR considers that the domestic authorities failed to strike a fair balance between the employee's interests to respect for his private life and the employer's right to engage in monitoring.[21]

The aforementioned point is the reason why we have decided to place the data protection principles at the core of this paper. Relying on the personal stories and reflections of employers and employees regarding data processing from social media, we set out to explore if data protection principles are actually followed in everyday practices.

2. THEORETICAL AND EMPIRICAL BACKGROUND

Various authors have brought up a variety of different possible problems in relation to data processing from social media in the course of employment relationships. In the following section, we will first introduce the findings of empirical

[18] The working party was established by Article 29 of the DPD. It provides the European Commission with independent advice on data protection matters. It is composed of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission.
[19] Article 29 Data Protection Working Party, "Opinion 2/2017 on data processing at work" (June 2017): 3 //https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/07/Opinion22017ondataprocessingatwork-wp249.pdf.
[20] Article 29 Data Protection Working Party, "The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data" (December 2009): 2 // http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.
[21] *Bărbulescu v Romania*, European Court of Human Rights (2017, no. 61496/08).

studies on the topic and then move on to give a short overview of the legal background by introducing the data protection principles.

2.1. PROCESSING EMPLOYEES' OR APPLICANTS' DATA ON SOCIAL MEDIA

The growing popularity of using social media to process employees' or applicants' data is usually explained by the fact that such an approach is fast, inexpensive and makes it possible to draw quick conclusions about a person's character.[22] For instance, studies[23] reveal that human resource departments process information on applicants' social media profiles in order to detect any differences between their resumes and cover letters as compared to their postings on social media.

Given the expanding number of employers using SNS to process employees' personal data, it is reasonable to expect this practice to affect various human resource decisions, including hiring, training, promotion and termination.[24] A survey by Jobvite[25], for example, reveals that 93% of recruiters had monitored candidates' SNS profiles before making hiring decisions. Furthermore, 55% of the recruiters had reconsidered candidates based on their profiles, with 61% of those reconsiderations being negative. According to Sprague,[26] in the majority of cases applicants get rejected due to lifestyle concerns revealed in the form of inappropriate comments, texts, photos, videos and other information posted on profiles. Furthermore, as suggested by Valentino-DeVries,[27] employers can also use the information available on public profiles to discriminate against applicants on the basis of protected class information (e.g. religion, race, sexuality etc.), but also due to applicants' lifestyle behaviour (e.g. personal relationships, political or civic activities, daily habits etc.),

[22] Leigh A. Clark and Sherry J. Roberts, "Employer's use of social networking sites: A socially irresponsible practice," *Journal of Business Ethics* Vol. 95, No. 4 (February 2010): 509 // DOI: 10.1007/s10551-010-0436-y.
[23] Torsten Reiners and Paul Alexander, "Social network perception alignment of e-recruiters and potential applicants," *46th Hawaii International Conference on System Sciences* (2013); Robin Kroeze, "Recruitment via Social Media Sites: A critical Review and Research Agenda," *5th IBA Bachelor Thesis Conference* (November 2015) // http://essay.utwente.nl/68499/1/Kroeze_BA_BMS.pdf; H. Kristl Davison, Catherine C. Maraist, R. H. Hamilton, and Mark N. Bing, "To screen or not to screen? Using the internet for selection decisions," *Employee Responsibility Rights Journal* Vol. 24, No. 1 (2012) // DOI: 10.1007/s10672-011-9178-y.
[24] Victoria R. Brown and E. Daly Vaugh, *supra* note 1: 219.
[25] Jobvite, "Social Recruiting Survey" (2014) // https://www.jobvite.com/wp-content/uploads/2014/10/Jobvite_SocialRecruiting_Survey2014.pdf.
[26] 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): 5.
[27] Jennifer Valentino-DeVries, "Bosses May Use Social Media to Discriminate Against Job Seekers," *The Wall Street Journal* (November 2013) // https://www.wsj.com/articles/bosses-may-use-social-media-to-discriminate-against-job-seekers-1384979412?tesla=y.

which when they clash with employers' interests take the form of "lifestyle discrimination."[28]

Employees believe that such processing of information might lead to premature conclusions about applicants' personalities and skills and thus consider such screening to be unacceptable. For example, Abril, Levin's and Riego's[29] findings indicate that 56% of US employees participating in their study considered it "somewhat" or "very inappropriate" for employers to seek information about candidates using SNS. Research indicates that employees are cognisant of their reputational vulnerability on SNS and they rely on others, including employers, to refrain from judging them across contexts.[30]

The biggest danger associated with social media background checks is that employers' actions may breach "contextual integrity", a term that ties adequate protection of privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to the context.[31] Negative information conveyed through a personal profile may not be considered in the proper context, and could therefore result in a hasty rejection decision on an applicant[32] or an ill-considered termination of an employment contract.[33] Considering the fact that there are also companies that use information from social media to build candidate profiles for employers, breaches in the contextual integrity of applicants is even more likely.[34]

Regardless of the fact that a majority of the employees in the United States, for example, strongly disapprove of employers accessing their SNS profiles – 75% of the respondents found this practice to be "somewhat" or "very inappropriate"[35] – employers are becoming more interested in monitoring and limiting their staff behaviour on social media.

Studies also suggest that social media have "amplified corporate reputation risks",[36] e.g. present-day employers are facing new risks when trying to engage their employees in the reputation building of the organisation. As many stakeholders can be reached directly through social media, employers encourage their employees to

[28] Stephen D. Sugarman, "Lifestyle Discrimination in Employment," *Berkeley Journal of Employment and Labor Law* Vol. 24, No. 377 (2003) // DOI: http://dx.doi.org/doi:10.15779/Z38D06N.
[29] Patricia Sánchez Abril, Avner Levin, and Alissa Del Riego, *supra* note 3: 108.
[30] *Ibid*.
[31] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009).
[32] Victoria R. Brown and E. Daly Vaugh, *supra* note 1: 221.
[33] Patricia Sánchez Abril, Avner Levin, and Alissa Del Riego, *supra* note 3: 85.
[34] Alex Rosenblat, Tamara Kneese, and Danah Boyd, "Networked Employment Discrimination," *Open Society Foundations' Future of Work Commissioned Research Papers 2014* (October 2014) // DOI: 10.2139/ssrn.2543507.
[35] Patricia Sánchez Abril, Avner Levin, and Alissa Del Riego, *supra* note 3: 100.
[36] Joonas Rokka, Katariina Karlsson, and Janne Tienari, "Balancing acts: Managing employees and reputation in social media," *Journal of Marketing Management* Vol. 30, No. 7-8 (2014) // DOI: 10.1080/0267257X.2013.813577.

"'live the brand' online"[37] and build the reputation of the organisation online. Employers also show a growing concern for the fact that many employees are making defamatory and outspoken remarks in social media about the company, supervisors, co-workers, clients etc. For instance, according to the HubShout survey, 41.2% of employees were sure that they could post whatever they wanted to and that they could not lose their jobs as a result. However, only 8.1% of employees in the sample confessed to having posted criticism of their employers or colleagues on social media and only 15.7% confessed to complaining about their jobs.[38]

Numerous authors[39] have shown that employers invite trouble if they fail to develop policies governing what is said about the organisation in social media. Kaplan and Haenlein warn that if companies encourage employees to be active on blogs, they may need to live with the consequences of staff members writing negatively about the company.[40] Thus, as noted by Rokka, Karlsson and Tienari,[41] it is crucial for employers to find a suitable balance between control and trust.

These examples suggest that the users of social media are only slowly starting to become aware of the fact that personal issues and statements made in a specific online context are visible not only to one's "ideal audience"[42] i.e. family and friends, but also to "nightmare readers",[43] i.e. employers, colleagues, recruiters, clients etc. Nevertheless, a social media profile owner often still relies on the hope that the viewers of their private information share similar norms of contextual integrity.[44] These expectations, however, are not always met by businesses or guaranteed by law.

2.2. DATA PROTECTION PRINCIPLES

Such scholars as Bonner and Chiasson have been highly critical of data protection principles and have expressed doubts about whether these cornerstones

[37] Manto Gotsi and Alan M. Wilson, "Corporate reputation: seeking a definition," *Corporate Communications: An International Journal* Vol. 6, No. 1 (2001) // DOI: 10.1108/13563280110381189.
[38] HubShout, "You're Fired! 71.6% Unaware that the First Amendment Does Not Apply to Social Media Recklessness" (2016) // http://hubshout.com/?2016-Social-Media-Conduct&AID=1732.
[39] TechRepublic, "Why your company needs a social media policy" (November 2016) // http://www.techrepublic.com/article/why-your-company-needs-a-social-media-policy/; Mike Johansson, "8 Reasons Your Organization Must Have a Social Media Policy" (February 2015) // http://www.socialmediatoday.com/content/8-reasons-your-organization-must-have-social-media-policy-0.
[40] Andreas M. Kaplan and Michael Haenlein, "Users of the world, unite! The challenges and opportunities of social media," *Business Horizons* Vol. 53, No. 1 (January–February 2010): 63 // DOI: 10.1016/j.bushor.2009.09.003.
[41] Joonas Rokka, Katariina Karlsson, and Janne Tienari, *supra* note 36.
[42] Alice E. Marwick and Danah Boyd, "I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience," *New Media & Society* Vol. 13, No 1 (February 2011): 120 // DOI: https://doi.org/10.1177/1461444810365313.
[43] *Ibid.*: 125.
[44] Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy* Vol. 17, No. 5 (November 1998) // DOI: 10.1023/A:1006184504201.

of data protection benefit privacy.[45] Other researchers, including Tene, have brought to our attention the fact that these principles originate from the Data Protection Convention 108 of the Council of Europe of 1981[46] and thus rely on a different technological landscape than we are currently dealing with, incorporating ideas dating from the 1990s or even earlier.[47] Regardless of the criticism, the European Commission is convinced that data protection principles remain sound.[48] Therefore, these principles are to a large extent addressed similarly in the DPD and in the GDPR.

Given the expanding percentage of employers using SNS to process employees' personal data and the importance of the principles as the main legal guidelines in these situations, we will give a short overview of the data protection principles as they are enacted in the GDPR. While the principles under the GDPR are similar to those found in the DPD, certain concepts are more fully developed, for example the explicit reference and clarification of the transparency and minimisation principle and the establishment of a new principle called "integrity and confidentiality".

Under the EU data protection law, employers are allowed to collect data for legitimate purposes. Not surprisingly, the principle of lawfulness – the right to process personal data only under certain legislative guidelines[49] – was therefore the first principle enacted in the GDPR[50]. The GDPR also requires employers to process data fairly and transparently.[51] The employer must provide the employee with information about his/her personal data processing in a concise, transparent and intelligible manner, and in a form that is easily accessible.[52]

Employers must collect data only for specified, explicit and legitimate purposes (the principle of purpose limitation[53]) and minimise the information that is gathered (the principle of data minimisation[54]). Employers should therefore collect only adequate and relevant data and limit collection to what is necessary for the purposes of the processing.

Collected data must be accurate (the data accuracy principle[55]) and kept in a form which permits identification of data subjects for no longer than is necessary (the

[45] William Bonner and Mike Chiasson, *supra* note 15.
[46] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Council of Europe, ETS No. 108.
[47] Omer Tene, "Privacy: The New Generations," *International Data Privacy Law* Vol. 1, No. 1 (February 2011) // https://doi.org/10.1093/idpl/ipq003.[48] European Commission, "Commission Staff Working Paper. Impact Assessment" (2012) // http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.
[48] European Commission, "Commission Staff Working Paper. Impact Assessment" (2012) // http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.
[49] *General Data Protection Regulation*, *supra* note 12, art. 6, sec. 1.
[50] *Ibid.*, art. 5, sec. 1(a).
[51] *Ibid*., art. 5 sec. 1(a).
[52] Article 29 Data Protection Working Party, "Opinion 8/2001 on the processing of personal data in the employment context" (2001) // http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.
[53] *General Data Protection Regulation*, *supra* note 12, art. 5, sec. 1(b).
[54] *Ibid*., art. 5, sec. 1(c).
[55] *Ibid*., art. 5 sec. 1(d).

principle of storage limitation[56]). Employers must, therefore, take every reasonable step to ensure that personal data that are inaccurate are erased or corrected.

According to the GDPR, personal data must also be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (the principle of integrity and confidentiality).[57]

Furthermore, the employer is responsible for, and must be able to demonstrate compliance with, all of the mentioned data protection principles in the GDPR (the principle of accountability).[58] One of the notable changes under the GDPR, as compared with the DPD, was the increased compliance burden, much of which was sparked by the accountability principle. It is not enough to comply; you have to be seen to be complying.[59]

3. DATA AND METHODS

3.1. STUDY DESIGN

This paper is based on the empirical material gathered during four small qualitative case studies carried out in 2013-2015 (see Table 1 for an overview).

Table 1: Description of the data set

Semi-structured individual interviews with employers from the service sector who are used to carrying out background checks of job applicants on social media	N= 10	Carried out in spring 2013
Semi-structured individual interviews with employers of different organisations who have had problems due to employees' posts on social media	N= 15	Carried out in spring 2014
Semi-structured individual interviews with employers from the field of media and communication who are used to carrying out background checks on job applicants on social media	N=15	Carried out in spring 2015
Semi-structured individual interviews with employees working in the financial sector whose organisations have issued social media guidelines	N=14	Carried out in spring 2015

[56] *Ibid*., art 5, sec. 1(e).
[57] *General Data Protection Regulation*, *supra* note 12, art 5, sec. 1(d).
[58] *Ibid*., art 5, sec. 2.
[59] TaylorWessing, "The data protection principles under the General Data Protection Regulation" (November 2016) // https://www.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html.

The aim of presenting the findings from these case studies together as one data set has to do with the aim of the paper: we have made use of the data collected during the semi-structured interviews with employers and employees so as to study whether there is a mismatch of the social reality of data subjects and the data protection principles that should be used as guidelines on the topic. We aim to demonstrate that this mismatch applies not only regardless of the sector employers and employees' work in and whether the employers have encountered actual (e.g. reputational) problems due to their employees' social media posts, but also regardless of having specific social media guidelines issued by the organisation.

3.2. PARTICIPANTS

A purposeful sample was used for all four case studies in order to find information-rich participants.

We aimed to study the practices of employers and employees from different sectors because we wanted to get as wide an overview as possible of the data processing trends of employers. We included the employers from the service sector in our sample because the average job tenure, i.e. the length of time the workers had been in their current jobs or with the current employers, tended to be on average lower in the service sector than in the goods-producing sector.[60] This is also the reason why human resource departments in the service sector are frequently occupied with hiring new personnel. Our aim was to carry out interviews with only those employers who confessed to making use of social media for the pre-employment screening of applicants. In order to find interviewees for our study, we first made use of the webpage of The Best Customer Service Association and its list of the TOP 100 customer service organisations in Estonia, and contacted the human resource departments of these organisations. Furthermore, we also contacted those organisations from the service sector who were actively advertising for new employees in spring 2013. The final sample was comprised of 10 interviewees.

We were also interested in interviewing employers from organisations that had had negative experiences due to things their employees had posted on social media. These interviewees (N=14) were found through convenience sampling: suitable interviewees were either recommended by acquaintances or they answered our call on Facebook.

Employers from the field of media and communication were included in the study due to the fact that people working in that field need to be constantly prepared

[60] OECD, "The Characteristics and Quality of Service Sector Jobs" (2001): 93 // https://www.oecd.org/els/emp/2079411.pdf.

for public scrutiny. We ended up interviewing employers (N=15) from different media organisations, including radio and TV stations and newspaper newsrooms, as well as communication agencies, all of whom confessed to using social media in pre-employment screening.

We were also interested in interviewing people from the financial sector because this is a sector in which success is mainly built on trust and confidentiality, which is also the reason why different financial organisations have been among the first to adopt internal social media guidelines. We aimed to carry out interviews with people who were either working in the financial sector at the time of the interviews or who had been recently employed there. The final sample was comprised of 15 employees.

Participating in the study was voluntary, and anonymity was protected for all of the participants.

3.3. DATA COLLECTION PROCEDURE

The aim of the interviews was to study the personal experiences and perceptions of all of our interviewees regarding the dominant SNS data processing practices. For instance, we were interested in studying the rationalisations employers use to justify the pre-employment screening of employees' social media use, but also aimed to capture employees' experiences with such SNS data processing. Thus during the interviews the employers were asked such questions as "Why have you started to make use of pre-employment screening on social media?; "How much social media usage is there among the employees monitored in your organisation?"; "How ethical do you think it is to use social media for pre-employment screening?", etc. In the interviews with employees, questions were asked such as: "How do you feel about the fact that the information you post on social media might be read by your boss or your colleague?"; "Why do you think employers use SNS for data processing?" "Do employers notify employees about SNS data processing?", etc.

The interviews were carried out by four different interviewers, one for each case study. Each of the interviews lasted between a half an hour and an hour, and each was recorded and later transcribed.

3.4. DATA ANALYSIS

We used qualitative text analysis to analyse the interview data. First, the material gathered for each case study was analysed separately by one independent coder. All of the coders started the analysis with hierarchical coding, as suggested by

Straus and Corbin.[61] First the interview material was divided into smaller units of analysis through initial open coding. Then, after a close reading of the interview material, focused coding was used to look for common themes and patterns in the respondents' comments. Such an analysis was carried out for each case study separately and only then did the second author of the paper move on to analyse the collected interview data following an approach similar to that described above.

4. RESULTS

4.1. FOLLOWING THE PRINCIPLES OF LAWFULNESS

The processing of personal data is lawful only if and to the extent that it is permitted under EU data protection law. Each data processing activity requires a lawful basis. The most common available grounds for employers to process information from social media, including SNS, are the consent of the employee[62] or necessity arising from the contract,[63] e.g. to conclude or fulfil an employment contract. Recent case from ECHR indicates that the legitimate reasons to justify monitoring employee's internet use must be weightier than simply stating that the employer has the right and the duty to ensure the smooth running of the company and the right to supervise its employees' performing their professional tasks.[64]

The GDPR made no change to the principle that consent may provide a lawful basis for data processing. However, the GDPR made it more difficult for employers to obtain valid consent from employees. The reliance on consent has to be confined to cases where the employee has a genuine free choice and is subsequently able to withdraw the consent without detriment.[65] Therefore, employers are generally ill-advised to rely solely on the consent of an employee or applicant. In its opinion the Article 29 Data Protection Working Party suggests that employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employment relationship. Unless in exceptional situations, employers will therefore need to rely on another legal ground than consent.[66]

> *A member of an organisation who had experienced problems (Interviewee 5):* As most of our civil servants who start working [here] process state secrets to some extent, whether it be on a lower or higher scale, they need to sign permission that background checks on their behalf are acceptable. Background checks mean

[61] Anselm Strauss and Juliet Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 4thed (SAGE Publications, 2015).
[62] *General Data Protection Regulation*, *supra* note 12, art. 6, sec. 1(a).
[63] *Ibid*., art. 6, sec. 1(b).
[64] *Bărbulescu v Romania*, *supra* note 21.
[65] *General Data Protection Regulation*, *supra* note 12, rec. 32, 43; art. 7, sec. 4.
[66] Article 29 Data Protection Working Party, *supra* note 19: 4.

> [screening] online as well as the possibility that there might be a knock on a neighbour's door to ask "hey, who is this guy?"

As the extract above illustrates, our findings reveal that both the legal grounds and consent for data processing is generally followed in the case of public service and civil servants. However, for the majority of our informants, pre-employment screening had become such a routine practice that most of them never considered the need for any legitimate grounds for data processing from SNS. Mainly our interviewees justified the background screening by saying that if the information were public, everyone had a right to search for and look at it.

> *A member of an organisation who had experienced problems (Interviewee 6):* I do not think [background checks of applicants'] are unethical if the information is publicly available. When using and being on social media, a person needs to consider that this information can go public./…/ If this information is publicly available, I do not see any reason why an employer should not use it. By making this information public, the person basically gives permission and everyone can look at it.

The above indicates that the employers in our sample rarely questioned whether such data processing was at all necessary for the performance of an employment contract or whether consent was needed for data processing, and thus whether they actually had legitimate grounds for data processing. Rather, they viewed the information found on SNS as a publicly available free source of information and saw no need to contact the person to ask for their consent or search for any other legal basis for data processing activities.

However, the Article 29 Data Protection Working Party has stated in its opinion that employers should not assume that merely because an individual's social media profile is publicly available they are allowed to process those data for their own purposes. Working party suggested making sure whether the social media profile of the employee is related to business or private purposes, as this can be an important indication for the legal admissibility of the data inspection.[67]

> *An employer from the field of media and communication (Interviewee 1):* I cannot imagine that looking at a Facebook profile or searching on Google would be an invasion of privacy. This is public information. If I were to hire a private detective to snoop around someone, then that would be a case where it would be polite to inform the applicant. Why do I say so? On Facebook a person can control what is made public and what is shown. A Google search is public. I believe there is no need to inform a person in the case of [processing data from] these two channels. If a person were to say that they would not allow a background search of

[67] *Ibid*.: 11.

> themselves, then I would automatically start to question why I couldn't. That would not be good for the employee either.

4.2. FOLLOWING THE PRINCIPLES OF FAIRNESS AND TRASNPERENCY

The principle of fair and transparent processing means that the employer must provide information to employees about its processing of their data. The GDPR requires more extensive information to be provided than the DPD.[68] For example, employers are obligated to keep employees informed that their data is being used and about the legitimate interests pursued by the employer, as well as the categories of personal data concerned, and the existence of the right to request access to and erasure of personal data. Employees should also have knowledge of the source from which the personal data originates and, if applicable, whether the data came from publicly accessible sources (e.g. from social media).[69] The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language.[70] Therefore, there must be no secret and covert processing of personal data and such processing should not have unforeseen negative effects.

Our interviews with employers revealed that in the majority of cases they did not inform either their applicants or employees about SNS data processing. For instance, personal experiences shared by the employees from the financial sector revealed that in their organisations senior managers were encouraged to "friend" their employees on Facebook with the aim of receiving additional information about the employees' SNS practices. In other words, our interviewed employees from the financial sector had experienced secret and excessive data processing practices, all of which were not in accordance with the data protection principles.

> *An employee of the financial sector (Interviewee 1):* There definitely was [monitoring of employees' social media profiles]. It was executed so that a higher ranking manager even ordered lower ranking managers to "friend" their employees on Facebook and then monitor what they posted there, if their posts gave some hints of whether the employee was currently ill or not, and if and what…Yes-yes.//No, definitely not [the employees were not informed about this practice]. Rather things were supposed to appear the opposite way.

Only in a few cases did our empirical data confirm that employers were informing their applicants about online screening and on those occasions it was done through job adverts.

---

[68] *General Data Protection Regulation*, *supra* note 12, rec. 39, 58, 60, 71, 78; art. 5 sec, 1(a), art 12, art 14.
[69] *Ibid*., art 14.
[70] *Ibid*., rec. 58, art 12.

> *An employer from the service sector (Interviewee 2):* … We have a job advert where it is noted that when applying and sending their CVs they have given [us] permission to keep their CVs in our database as well as for carrying out background checks. Such consent was quite general, so that many of the individuals may not have noticed at all.

Although the example above illustrates how some employers tried to make the processing of information lawful, none of the descriptions our interviewees gave about their SNS data processing practices led us to believe that the transparency principle was followed.

According to transparency principles, employers need to disclose their screening practices on SNS, including the ways they use online information in making employment decisions. For example, an applicant or an employee has the right to access files that contain personal data gathered from SNS. Processing operations must be explained to the employee and the employee must understand what will happen to their data. Nothing of the kind was revealed in our interviews. Rather, the majority of interviewees never informed the applicants or employees that they had been processing their data on SNS, not to mention revealing how any information found was used in making employment decisions.

> *An employer from the service sector (Interviewee 2):* [Did you inform the applicant later about the online screening?] … probably not, like how am I supposed to go and say, 'you know, your room was so messy in that photo that this is the reason I am not hiring you'.

In order to ensure fair and transparent processing in respect to the employee, the employer should also take into account the specific circumstances and context in which the personal data are processed.[71] In other words, the fairness principle also means that employers must handle employees' personal data only in ways the employees would reasonably expect and not use the information in a manner that unjustifiably has a negative effect on employees.[72]

Interviews with our respondents, however, indicated that employers' actions often breached contextual integrity and brought unjustifiable negative consequences to employees. For instance, some of the interviewed employers from the media and communication field who had had previous negative experiences with employees' alcoholism took special notice during social media background checks of various party photos and photos in which alcohol was displayed.

[71] *Ibid*., rec. 60, 71.
[72] Information Commissioner's Office, "Guide to data protection. Processing personal data fairly and lawfully" (2017) // https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/.

> *An employer from the field of media and communication (Interviewee 11):* If the background check displays something really bad, then they [the applicants] will not last long. I believe that people who consume a lot of alcohol are not good employees. They have a problem and at some point they will not turn up or will fake being ill. We have had such experiences. Not any more. We have eliminated that problem.

Displaying party photos or photos with alcohol on Facebook is similar to presenting personal information out of context or inaccurately, and may lead employers to judge employees or applicants unfairly. Harm that may arise as a result of employers seeking information on SNS can be defined as "informational injustice",[73] i.e. information presented in one context being used in another. Employers should therefore consider the role of context when monitoring employees' or applicants' SNS profiles and refrain from any unjust activities (e.g. eliminating an applicant from the potential list of employees). At the same time, as is clear in the extract below, such a practice is quite hard to undertake as people tend to "read" social media messages very differently and the posts made on SNS can very well lead to real problems with one's employer or employee.

> *An employee of the financial sector (Interviewee 3):* What happened was that I was on Facebook during my spare time, in the middle of the night when I was ill and shared some kind of a page, or commented on my girlfriends' photo or something like that, and…and then my employer saw that and asked my boss to print out that part of Facebook where I had shared or commented and asked my boss to have a chat with me. And to tell me that they would take 0.5% from my personal incentive wage, and that was done.

Another controversial issue surrounding the use of SNS is the variability in type and amount of information publicly available. This inevitable situation prevents a completely standardised and fair collection of predictor information across all applicants and employees.[74] As a result, when an employer decides to use internet background checks, but not all applicants or employees have SNS profiles, the potential for illegal disparate treatment and/or impact is present; at the very least, employees are evaluated using different selection criteria, and the reliability and subsequent validity of the selection process is compromised.[75] Our findings suggest that many employers even tend to consider it very suspicious if no information can be found about an applicant during a Google search.

[73] Jeroen van den Hoven, *Information Technology and Moral Philosophy*, edited by Jeroen van den Hoven and John Weckert (New York: Cambridge University Press, 2008), 314.
[74] Victoria R. Brown and E. Daly Vaugh, *supra* note 1: 221.
[75] H. Kristl Davison *et. al*, *supra* note 23: 16.

4.3 FOLLOWING THE PRINCIPLE OF PURPOSE LIMITATION

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.[76] With this restriction, the GDPR made no changes to the principle of purpose limitation. Hereby, the processing of personal data for undefined or unlimited purposes is unlawful. Employers' habits of searching SNS profiles without any specific aim are therefore at variance with the purpose limitation principle.

Interviews with all of our respondents, however, indicated that as background checks had become such routine tasks they were generally carried out without having a clear aim or purpose in mind. For instance, interviews with employers in the service sector suggested that background checks on social media were carried out for every applicant who might have a chance to proceed either to another round of interviews or who was considered a possible candidate for a job.

> *An employer from the service sector (Interviewee 4):* [I do a background check] on absolutely everyone whom I have considered or whom I am planning to invite [for an interview]. I do not want to waste my time, time is a very valuable thing, and I choose only those about whom I think there is a high probability that they might be suitable. I check all of them on Facebook.

Furthermore, data from our case studies revealed that often employers were not looking for any specific information when carrying out these background checks; rather these checks were carried out with the hope of finding some new information about the applicant.

> *An employer from the field of media and communication (Interviewee 2):* When we are hiring someone, I do want to know what their speciality is. When I see [from an online background search] that he is an active sportsman, plays basketball and some other this and that, I know that probably his knowledge and interests are greater in that field. Obviously, if he is almost a professional athlete, I do take into account the fact that he probably wants to train five times a week. When I see that he has written his thesis on the topic of economics, I presume that he is acquainted with economic issues, banking and financial issues. This gives me a hint that I could probably use him in that field.

On many occasions the background checks on the internet are carried out with the aim of finding additional information about the applicant's personality. The employers from the media and communication sector, for instance, justified their practice by emphasising that the applicant needed to "fit in" with the rest of the staff. As CVs or cover letters do not reveal much about an applicant's personality, their

[76] *General Data Protection Regulation*, *supra* note 12, rec. 50; art. 5 sec. 1(b).

values, hobbies, likes and dislikes, employers turn to social media to find additional information about these areas.

> *An employer from the field of media and communication (Interviewee 1):* I think I can say clearly that especially in a small collective an individual's personal self is very important. Maybe in a big organisation with a few hundred people it is not as important; a person sits in their cubicle and does their job. In a small organisation, this person is part of the team and their everyday personality affects the way the whole team operates. A Facebook profile gives the first impression of what kind of person this is.

Furthermore, our respondents agreed that when searching for additional information about an applicant on SNS, they are often able to discover information about an employee's or applicant's political activities, national origin, religion and other information that might not be disclosed by the applicant in their CV.

Interviewed employers from the journalism and communication field, as well as from the service sector, also claimed that in addition to looking for the previous work done by the applicant, they browsed through the applicant's social media posts and photo galleries to find out if the applicant had any personal commercial or political interests that might affect their work. In other words, the information found on the SNS might be useful for getting hired but it might also be a basis for not hiring someone.

> *An employer from the service sector (Interviewee 3):* All very radical religious beliefs … I definitely do not discriminate but this does stand out; if these are emphasised and brought out then I get a feeling that this might become an issue some day.

4.4. FOLLOWING THE PRINCIPLES OF DATA MINIMATION AND STORAGE LIMITATION

According to the data minimisation principle, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which data are processed.[77] Recent ECHR case also reaffirms the need to take into account the extent of the monitoring and the degree of intrusion into the employee's privacy and make sure that it would not have been possible for the employer to establish a monitoring system based on less intrusive methods.[78] Employers need to carefully review their data processing operations to consider whether they process any personal data that are not strictly necessary in relation to the relevant purposes. The principle of storage limitation also means that data must be erased when those

[77] *Ibid.*, rec. 39, art. 5 sec. 1(c).
[78] *Bărbulescu v Romania*, *supra* note 21.

purposes have been served.[79] Therefore, employers should collect only the personal data they really need, and should keep it only for as long as they need it. However, as noted previously, our interviewees had very broad and vague purposes for SNS data processing. Rather than aiming to collect as limited an amount of data as possible about the applicant or employee, our informants were eager to gather as much and as varied information as possible.

> *An employer from the service sector (Interviewee 4):* Well, we do check them all …as much information as we are able to get. If I know the individual personally, then we don't [do background checks], but if it's a stranger, we do.

For instance, many of the interviewees claimed that they were definitely interested in looking through profile images and other photos as they generally gave a clear impression of the person and their self-presentation strategies.

> *An employer from the service sector (Interviewee 8):* Photos definitely give a lot of information about a person, such as what kind of photos they have uploaded. CVs are also sent… where someone is there holding a bottle and drinking ... and that kind of photo has been uploaded. Facebook is full of photos of that kind.

In addition to visual clues, interviewed employers also said they were interested in gathering information that would enable them to get an overview of the personality and character of the person. For instance, employers were interested in gathering information about the social circle (friends' list) of the person, their hobbies and skills, likes and dislikes, and their communication and self-expression skills. According to the principles of minimisation, monitoring must be carried out in the least intrusive way possible so as to ensure that the intrusion of privacy is kept to a minimum. Our empirical data, however, indicated that the principles of minimisation and storage limitation were rarely considered, much less followed.

4.5. FOLLOWING THE PRINCIPLES OF DATA ACCURACY

An employer having personal information is not supposed to use that information without taking steps to ensure, with reasonable certainty, that the data are accurate and up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or corrected as quickly as possible.[80]

At the same time, it should be taken into account that SNS profiles allow individuals to post whatever information they want to, without regard to the veracity of the information. Our empirical data, however, suggests that many of the employers rarely questioned the accuracy of data presented on SNS or acknowledged

[79] *General Data Protection Regulation*, *supra* note 12, rec. 39, art. 5 sec. 1(e).
[80] *Ibid.*, rec. 39, art.5 sec. 1(d).

the need to critically assess the processed information. In fact, our interviews with employers working in different sectors suggested that employers tended to regard the info found on social media to be accurate, mainly because they believe that if a person had uploaded the information on his/her profile then that person must have processed it carefully before making it public.

> *An employer from the service sector (Interviewee 4):* Why shouldn't I consider [the information found on an SNS] trustworthy. This has been created by the individual and the information…or I do not believe that someone would make a fake account for themselves or something.

The above extract indicates that the employers did not consider the fact that SNS users might be making conscious use of social media and thus distorting the information employers come across with social desirability or high levels of self-monitoring. Furthermore, our data indicated that many SNS users envisioned their long-term friends, i.e. ideal readers, as the main audience of their posts and therefore their self-presentation strategies might appear totally inappropriate in the eyes of employers.

> *An employee in the financial sector (Interviewee 5):* … For a person who is supposed to be a higher ranking official, posting nude photos of him/herself on a social networking site is not a very exemplary [thing to do]. It is very difficult to honour such a person. In my opinion, this person was not on my "friends" list, but I do not remember. I did see those photos and it was also discussed inside our organisation.// But it did not lead to anything good, that is for sure; it was not thought of well. But the person must have thought it was totally normal behaviour.

Our interviews also revealed that sometimes it was very difficult for employers to differentiate between the private and public selves presented on social media. One of our interviewees, for instance, talked about a case where a person who was sent on a diplomatic mission to represent Estonia abroad started to keep a blog which was mainly related to the private sphere and had very little to do with representing Estonia.

> *A member of an organisation who has had problems (Interviewee 12):* This [case] was brought up in different meetings, and it was questioned whether such behaviour was suitable for our ambassador.

4.6. FOLLOWING THE PRINCIPLES OF DATA INTEGRITY, CONFIDENTIALITY AND ACCOUNTABILITY OF THE DATA CONTROLLER

The GDPR obliges employers to process personal data in a manner that ensures appropriate security for the personal data (the integrity and confidentiality

principle)[81] and requires employers to demonstrate compliance with data protection principles (the accountability principle).[82] Employers are therefore required to take all necessary measures to protect the data against unauthorized access.[83]

A good and clear policy on what constitutes an unacceptable use of social media will help both the employer and the employee to understand where the boundaries between acceptable and non-acceptable use lie. Broughton et al recommend that organisations establish explicit policies and procedures concerning the use of SNS as screening devices enabling both employers and employees to know their rights and responsibilities when communicating on social media so that the policy will at least provide guidance on when and how an employer can use information obtained from online sources.[84]

The findings of our empirical study however suggested that having a social media usage policy or guidelines did not necessarily simplify matters. In fact, semi-structured interviews with the employees in the financial sector revealed that although there were social media guidelines and policies in all of the organisations the interviewees belonged to, there was not a single interviewee who was actually informed about the content of these documents. In the majority of cases, they had simply forgotten that content, but there were also some who had never even read the guidelines.

> *An employee of the financial sector (Interviewee 5):* There were some guidelines. I remember being sent a new version of the employment contract, but I think I did not find it on the inner web. There were guidelines but I am not aware of them.

Furthermore, as has been argued by Broughton et al, the mere existence of a policy may also not be sufficient in court, as policies can be too broad, ambiguous or unwise.[85] Article 29 of the Data Protection Working Party has suggested that a blanket ban on communication for personal reasons is impractical and enforcement may require a level of monitoring that may be disproportionate.[86] The ECHR has also reaffirmed that an employer's instructions cannot reduce private social life in the workplace to zero. Employer's restrictive regulations have to leave the employee with a reasonable expectation of privacy.[87] Therefore, employers should be extra careful in that written policies must be carried out, enforced consistently and incorporated

[81] *Ibid.*, rec. 29, 71, 156, art. 5 sec. 1(f), 24(1), 25(1)-(2), 28, 39, 32.
[82] *Ibid.*, rec. 85, art. 5 sec (2).
[83] Article 29 Data Protection Working Party, *supra* note 19: 5.
[84] Andrea Broughton, Tom Higgins, Ben Hicks, and Annette Cox, *Workplaces and social networking-The implications for employment relations* (Brighton: Institute for Employment Studies, 2009).
[85] *Ibid*.
[86] Article 29 Data Protection Working Party, *supra* note 19: 11.
[87] *Bărbulescu v Romania*, *supra* note 21.

into the organisation's culture to form the rational foundation of employees' privacy expectations.[88]

CONCLUSIONS

Data protection principles clearly form the backbone for the new GDPR and give needed guidance for all processing of personal data. They form an important set of standards for member states to follow and in theory give the data subject and data controller a comprehensive set of rules to abide by. The aim of our interdisciplinary article was to question whether there is a mismatch between social reality and the core set of key data protection principles enacted in the GDPR. We made use of different qualitative case studies carried out amongst employers and employees from different organisations in Estonia, with the aim of determining whether these main data protection guidelines are actually followed in everyday practice.

Our analysis indicates that in the light of employer-employee relations on social media, the data protection principles are very difficult to follow in practice. In fact, even though the data protection principles emphasise the need for fair, purposeful, transparent, minimal and accurate processing of personal data, our interviews with employers and employees revealed that the actual SNS processing practices rarely lived up to the standards.

Data protection principles state that employers should only process information from SNS if they have legitimate grounds for processing it. Our interviews with employers, however, revealed that the employers rarely questioned whether personal data processing was at all necessary for the performance of an employment contract or whether consent was needed for data processing and thus whether they actually had legitimate grounds for data processing. In fact, our interviews with employers demonstrated a clear tendency to consider the information from SNS to be readily available for anyone to use and for any reason, without the knowledge of the data subject. Such an assumption, however, is not without flaws and, as many have pointed out,[89] clearly breaches employees' right to privacy.

Employers are also obligated to be fair and transparent when processing personal data from SNS by keeping data subjects informed that their data is being used and taking account of the context of gathered information. Nothing of the kind was revealed in our interviews. Rather, the majority of interviewees never informed applicants or employees that they had been processing their data on SNS, not to

[88] Patricia Sánchez Abril, Avner Levin, and Alissa Del Riego, *supra* note 3: 115.
[89] Robert Sprague, *supra* note 26; Peter B. Baumhart, "Social Media and the Job Market: How to Reconcile Applicant Privacy with Employer Needs," *University of Michigan Journal of Law Reform* Vol. 48, No. 2 (2015).

mention that they did not reveal how this information was used in making employment decisions. Furthermore, employees from the financial sector had also experienced mandatory friending, i.e. their employers had required that they be included on the employees' contacts list on SNS. The latter practice has been outlawed in several states in the US[90] and is not in accordance with the data protection principles.

The data protection principles also state that employers must define the purpose of data collection clearly and explicitly before processing is started. Our findings indicate that the employers mainly processed information on SNS with the aim of "weeding out" some candidates. However, in order to fulfil that aim, the employers usually gathered personal data from SNS for unlimited purposes. Furthermore, although data processing must be carried out in the least intrusive way possible so as to ensure that the intrusion of privacy is kept to a minimum, our informants were also eager to gather as much and as varied information as possible. In fact, interviewees' attitudes clearly indicated that processing minimum amounts of data from SNS was neither practical nor possible. At the same time, it is crucial to remember that "the information often cannot be 'unseen' once someone who has hiring authority has viewed it."[91] Scholars[92] have often warned employers about the inherent risks of inaccuracy, misinterpretation and the lack of verifiable data gathered from the internet and have urged them to use the data collected only with non-discriminatory hiring practices and policies. Our interviews, however, suggested that employers usually tended to regard the info found on social media to be accurate, mainly because they believed that if a person had uploaded the information on his/her profile then that person must have processed it carefully before making it public. Hence, similar to the findings of Davison et al,[93] such a stance reveals that employers rarely considered potential issues of mistaken identity and identity theft, or the fact that SNS users might be making conscious use of social media and thus distorting the information employers came across with social desirability or high levels of self-monitoring, as scholars[94]suggest. Furthermore, many of the interviewees seemed to believe that the SNS profiles could be used to provide a full picture of the individual,

[90] Robert T. Quackenboss, "Lesser-Known Social Media Legislation," *Risk Management* (2013) // http://www.rmmagazine.com/2013/10/01/lesser-known-social-media-legislation/.
[91] Michael E. Lackey and Joseph P. Minta, "Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging," *Touro Law Review* Vol. 28, No. 1 (2012): 180.
[92] Donald H. Kluemper, "Chapter 1 Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection"; in: Miguel R. Olivas-Lujan and Tanya Bondarouk, eds., *Social Media in Human Resources Management (Advanced Series in Management)*, Vol. 12 (Bingley: Emerald Group Publishing Limited: 2013).
[93] H. Kristl Davison *et. al*, *supra* note 23: 10.
[94] Victoria R. Brown and E. Daly Vaugh, *supra* note 1.

rather than revealing a snapshot of a person's state of mind at a particular moment in time, as indicated by Davison et al.[95]

Employers are supposed to ensure appropriate security of personal data, demonstrate compliance with data protection principles and actively implement measures to promote and safeguard data protection in their processing activities. The essence of these obligations is the employer's obligation to put in place measures which guarantee that data protection rules are adhered to in the context of processing operations. Our research revealed that, although there were social media guidelines and policies in all of the financial sector organisations our interviewed employees belonged to, there was not a single employee who was actually informed about the content of these documents. In the majority of cases, they had simply forgotten that content, but there were also some who had never even read the guidelines.

All of the aforementioned suggests that employers seldom relied on the data protection principles when processing employees' or applicants' data on SNS. In fact, the specific nature of social media made following such principles almost impossible. Thus additional discussions amongst legal scholars and practitioners are needed about whether the data protection principles can actually be applied and if they are necessary to follow in the context of SNS data processing.

Although limited in scope, we believe this paper offers valuable insights about the routine data processing practices employers engage in on social media. As there currently is a lack of empirical studies on the topic, future research is needed. For instance, scholars could investigate the impact of the new GDPR on employers' practices, as well as the social media policies of organisations.

As we await the new version of the data protection regulation to be put into force, employers and employees in different EU countries could profit from a specific set of tools or opinions that would help them to use all of the principles of data protection in practise.

BIBLIOGRAPHY

1. Abril, Patricia Sánchez, Avner Levin, and Alissa Del Riego. "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee." *American Business Law Journal* Vol. 49, No. 1 (2012): 63–124 // DOI: 10.1111/j.1744-1714.2011.01127.x.
2. Andrade, Norberto Nuno Gomes, and Shara Monteleone. "Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications": 119–144.

[95] H. Kristl Davison *et. al*, *supra* note 23: 4.

In: Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet, eds. *European Data Protection: Coming of Age*. Dordrecht and Heidelberg, New York, London: Springer, 2013.

3. Article 29 Data Protection Working Party. "Opinion 2/2017 on data processing at work" (June 2017) // https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/07/Opinion22017ondataprocessingatwork-wp249.pdf.
4. Article 29 Data Protection Working Party. "Opinion 8/2001 on the processing of personal data in the employment context" (2001) // http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.
5. Article 29 Data Protection Working Party. "The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data" (December 2009) // http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.
6. Baumhart, Peter B. "Social Media and the Job Market: How to Reconcile Applicant Privacy with Employer Needs." *University of Michigan Journal of Law Reform* 48 (2015): 503–533.
7. Bicky, Sarah L., and Linchi Kwok. "Social Media as an Employee Recruitment Tool." 16th Graduate Students Research Conference (2011). Track 2. Poster Session // http://scholarworks.umass.edu/gradconf_hospitality/2011/Poster/94/.
8. Bond, Jennifer, and George Waggott. "Social Media Policies in the Workplace: Case Studies" (2017) // https://www.go2hr.ca/articles/social-media-policies-workplace-case-studies.
9. Bonner, William, and Mike Chiasson. "If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy." *Information and Organization* Vol. 15, No. 4 (October 2005): 267–293 // DOI: 10.1016/j.infoandorg.2005.03.001.
10. Broughton, Andrea, Tom Higgins, Ben Hicks, and Annette Cox. *Workplaces and social networking – The implications for employment relations*. Brighton: Institute for Employment Studies, 2009.
11. Brown, Victoria R., and E. Daly Vaughn. "The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decision." *Journal of Business and Psychology* Vol. 26, No. 2. (May 2011): 219–225 //

DOI:10.1007/s10869-011-9221-x.

12. CareerBuilder. "Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade" (April 2016) // http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=4%2f28%2f2016&siteid=cbpr&sc_cmp1=cb_pr945_&id=pr945&ed=12%2f31%2f2016.
13. Cate, Fred H. "The Failure of Fair Information Practice Principles": 341–378. In: Jane K. Winn, ed. *Consumer Protection in the Age of the 'Information Economy'*. Routledge, 2006.
14. Clark, Leigh A., and Sherry J. Roberts. "Employer's use of social networking sites: A socially irresponsible practice." *Journal of Business Ethics* Vol. 95, No. 4 (February 2010): 507–525 // DOI: 10.1007/s10551-010-0436-y.
15. Davison, H. Kristl, Catherine C. Maraist, R. H. Hamilton, and Mark N. Bing. "To screen or not to screen? Using the internet for selection decisions." *Employee Responsibility Rights Journal* Vol. 24, No. 1 (2012): 1–21 // DOI: 10.1007/s10672-011-9178-y.
16. El Ouirdi, Asma, Mariam El Ouirdi, Jesse Segers, and Erik Henderickx. "Employees' use of social media technologies: a methodological and thematic review." *Behaviour & Information Technology* Vol. 34, No. 5 (May 2015): 454–464 // DOI: 10.1080/0144929X.2015.1004647.
17. European Commission. "Commission Staff Working Paper. Impact Assessment" (2012) // http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.
18. European Commission. "Questions and Answers - Data protection reform" (December 2015) // http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm.
19. Gotsi, Manto, and Alan M. Wilson. "Corporate reputation: seeking a definition." *Corporate Communications: An International Journal* Vol. 6, No. 1 (2001): 24–30 // DOI: 10.1108/13563280110381189.
20. Hoven, Jeroen vd. *Information Technology and Moral Philosophy*. Edited by Jeroen van den Hoven and John Weckert. New York: Cambridge University Press, 2008.
21. HubShout. "You're Fired! 71.6% Unaware that the First Amendment Does Not Apply to Social Media Recklessness" (2016) //

http://hubshout.com/?2016-Social-Media-Conduct&AID=1732.

22. Information Commissioner's Office. "Guide to data protection. Processing personal data fairly and lawfully" (2017) // https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/.
23. Jobvite. "Social Recruiting Survey" (2014) // https://www.jobvite.com/wp-content/uploads/2014/10/Jobvite_SocialRecruiting_Survey2014.pdf.
24. Johansson, Mike, "8 Reasons Your Organization Must Have a Social Media Policy" (February 2015) // http://www.socialmediatoday.com/content/8-reasons-your-organization-must-have-social-media-policy-0.
25. Kaplan, Andreas M., and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of social media." *Business Horizons* Vol. 53, No. 1 (January–February 2010): 59–68 // DOI: 10.1016/j.bushor.2009.09.003.
26. Karyda, Maria, Stefanos Gritzalis, Jong Hyuk Park, and Spyros Kokolakis. "Privacy and fair information practices in ubiquitous environments: Research challenges and future directions." *Internet Research* Vol. 19, No. 2 (April 2009): 194–208 // DOI: 10.1108/10662240910952346.
27. Kluemper, Donald H. "Chapter 1 Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection": 1–21. In: Miguel R. Olivas-Lujan and Tanya Bondarouk, eds. *Social Media in Human Resources Management (Advanced Series in Management).* Vol. 12. Bingley: Emerald Group Publishing Limited, 2013.
28. Kroeze, Robin. "Recruitment via Social Media Sites: A critical Review and Research Agenda." *5th IBA Bachelor Thesis Conference* (November 2015) // http://essay.utwente.nl/68499/1/Kroeze_BA_BMS.pdf.
29. Lackey, Michael E., and Joseph P. Minta. "Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging." *Touro Law Review* Vol. 28, No. 1 (2012).
30. Marwick, Alice E., and Danah Boyd. "I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience." *New Media & Society* Vol. 13, No. 1 (February 2011): 114–133 // DOI: https://doi.org/10.1177/1461444810365313.
31. Nissenbaum, Helen. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* Vol. 17, No. 5 (November 1998): 559–596 //

DOI: 10.1023/A:1006184504201.

32. Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.
33. OECD. "The Characteristics and Quality of Service Sector Jobs" (2001) // https://www.oecd.org/els/emp/2079411.pdf.
34. Peacock, Louisa. "Employers watch Facebook usage." *Employers Law* (2008).
35. Quackenboss, Robert T. "Lesser-Known Social Media Legislation." *Risk Management* (2013) // http://www.rmmagazine.com/2013/10/01/lesser-known-social-media-legislation/.
36. Reiners, Torsten, and Paul Alexander. "Social network perception alignment of e-recruiters and potential applicants." *46th Hawaii International Conference on System Sciences* (2013): 4576–4585.
37. Rokka, Jonas, Karlsson, Katariina, and Janne Tienari. "Balancing acts: Managing employees and reputation in social media." *Journal of Marketing Management* Vol. 30, No. 7-8 (2014): 802–827 // DOI: 10.1080/0267257X.2013.813577.
38. Rosenblat, Alex, Tamara Kneese, and Danah Boyd. "Networked Employment Discrimination." *Open Society Foundations' Future of Work Commissioned Research Papers 2014* (October 2014) // DOI: 10.2139/ssrn.2543507.
39. Special Eurobarometer. "Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union" (June 2011) // http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.
40. Sprague, Robert. "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): 1–34.
41. Strauss, Anselm, and Juliet Corbin. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 4th ed. (SAGE Publications, 2015).
42. Sugarman, Stephen D. "Lifestyle Discrimination in Employment." *Berkeley Journal of Employment and Labor Law* Vol. 24 No. 377 (2003) // DOI: http://dx.doi.org/doi:10.15779/Z38D06N.
43. TaylorWessing. "The data protection principles under the General Data Protection Regulation" (November 2016) // https://www.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html.

44. TechRepublic. "Why your company needs a social media policy" (November 2016) // http://www.techrepublic.com/article/why-your-company-needs-a-social-media-policy/.
45. Tene, Omer. "Privacy: The New Generations." *International Data Privacy Law* Vol. 1, No. 1. (February 2011): 15–27 // https://doi.org/10.1093/idpl/ipq003.
46. Valentino-DeVries, Jennifer. "Bosses May Use Social Media to Discriminate Against Job Seekers." *The Wall Street Journal* (November 2013) // https://www.wsj.com/articles/bosses-may-use-social-media-to-discriminate-against-job-seekers-1384979412?tesla=y.
47. Vinson, Kathleen Elliott. "The blurred boundaries of Social Networking in the Legal Field: Just 'Face' it." *University of Memphis Law Review* 41 (2010): 10–37.

LEGAL REFERENCES

1. *Bărbulescu v Romania*. European Court of Human Rights, 2017, no. 61496/08.
2. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Official Journal of the European Union, L 281, 23.11.1995, 31–50.
3. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Council of Europe, ETS No. 108.
4. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Eur-Lex, COM/2012/011 final – 2012/0011 (COD).
5. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 4.5.2016, 1–88.