Cybervetting: on the way to acceptance

Russian job seekers' perspective on cybervetting and emerging practices as a response to it

Student Name: Maria Terekhina
Student Number: 431105

Supervisor: Dr. Daniel Trottier

Master Media Studies – Media, Culture & Society
Erasmus School of History, Culture and Communication
Erasmus University Rotterdam

Master's Thesis
June 2016

CYBERVETTING: ON THE WAY TO ACCEPTANCE

ABSTRACT

This study examines a relatively new phenomenon of cybervetting from a job seekers' perspective. This practice has been studied within multiple frameworks over recent years – cybervetting and its relation to privacy, employers' perspective on cybervetting or self-presentation and cybervetting. The current study incorporates most of the issues and fulfills the gaps present in the previous academic literature on the topic. The first point is that it addresses the group of people aged 36 and older, previously understudied. The second point is that the perspective of job seekers, previously understudied as well, is explored in more details. The third point is that the actions undertaken by the job seekers' as a response to the possibility of being cybervetted were not covered within the previous framework and are brought up in the current research. The last but not least point is that the practice, becoming widely used in Russia, however has not still received any attention in the academic literature. Which is why the main research question of the paper is "How do practices of managing social media differ among younger and older Russian job seekers once they are aware of a possibility of being cybervetted?" Drawing from a series of fourteen in-depth semi-structured interviews collected from job seekers aged 18-35 years old and 36 years old and older, the conclusions about job candidates' perspective on cybervetting were made.

The research does not provide the evidence for existing difference between age groups, which is why the findings are similarly relevant for all the job seekers from a sample. It was discovered that Russian job seekers do not frame cybervetting as privacy violation, thus they do not express a negative attitude towards it. However, their attitudes may be described as positive, neutral and undecided. The first means a complete acceptance of the practice and high value attached to the results of using cybervetting. The second focuses more on acceptance of this practice by people and their willingness to change the strategies of online behavior if needed. The respondents from the third group, having an undecided opinion, see both – strong advantages and disadvantages of a practice, and cannot decide for themselves, which ones prevail. In general, the practice becomes more accepted by Russian job seekers, and they do not consider employers informing them about it a necessity. Moreover and most importantly, two strategies of managing online space as a response to the possibility of being cybervetted were discovered – preventive and 'ex-post'. The first one stands for initial caution in social networks and posting details that could not compromise a person in the future, while the second one describes the situation when users delete information once they are aware of the possibility of being cybervetted and think that their online profiles may be seen as inappropriate.

KEYWORDS: *Cybervetting*, *Privacy*, *Job Seekers*, *Social Networks*, *Self-Presentation*

Preface

It has been just a year since I graduated from my bachelor program in Moscow, Russia, and now I am finished with my master thesis in Rotterdam, The Netherlands, in one of the best Universities – Erasmus. I am taking this opportunity to express my deepest appreciation to everyone who made it possible.

My family. I would like to thank them for making a dream come true, for giving me a chance to change my life and pursue my goals. To thank them for being a constant moral support, even though far away. A special thanks to my father for telling me for as long as I remember myself that I should be cautious in social networks, which, at the first place, evoked my interest to the topic.

My supervisor and second reader. Looking back at the day when we first met our supervisors I can say that I could not have been more fortunate. I am expressing my sincere gratitude to my thesis mentor, Daniel Trottier, who has always been very helpful and inspiring and could always spare a minute to answer my panicked questions. I was fortunate to get a supervisor who is an expert in social media surveillance and cybervetting and who could always offer me useful suggestions and insights. Constructive criticism from my second reader of the proposal paper, Janelle Ward, helped me to refine my methodology and some of the key aims of the research. Without her feedback it would have been a different study.

My university professors. I would like to thank each and everyone who were teaching the courses this year in Media, Culture & Society for giving me a solid background for writing this research. Special thanks go to Wannes Ribbens for helping all the students and me deepen our understanding of qualitative methods and Isabel Awad for guiding us through the steps of writing a master thesis.

My respondents. Even though I cannot name them, I thank them all endlessly for sparing their time to talk to me and provide me with so much valuable information. None of that could be possible without their invaluable contribution.

My future readers. I would be glad to answer any questions that you may have about the current paper. You can contact me via my e-mail below.

Maria Terekhina
mary.terekhina@gmail.com.

Table of Contents

ABSTRACT **2**

Preface **3**

1. Introduction **5**

2. Theory and previous research **10**
2.1. Privacy on the internet **10**
2.2. Cybervetting and privacy **14**
2.3. Employers' perspective on cybervetting **16**
2.4. Job seekers' perspective on cybervetting **17**
2.5. Impression management online **18**
2.6. Russian context of social networks **19**
2.7. Conclusion **22**

3. Methodology **23**
3.1. Operationalization **25**
3.2. Sampling **26**
3.3. Data collection **28**
3.4. Methods of analysis **30**

4. Results **32**
4.1. Use of internet and social networks **35**
4.2. Knowledge/awareness of cybervetting; personal experience with the practice **37**
4.3. Perception of privacy **40**
4.4. Relations between privacy and cybervetting **45**
4.5. Attitudes towards cybervetting **47**
4.5.1. Positive attitude 48
4.5.2. Neutral attitude 49
4.5.3. 'Undecided' attitude 50
4.6. Rules and regulations of cybervetting **52**
4.7. Actions, undertaken as a response to potential possibility of being cybervetted **58**
4.7.1. Preventive strategy 58
4.7.2. 'Ex-post' strategy 59
4.7.3. Evaluation of employers 60

5. Conclusion and Discussion **62**

References **68**

Appendix A **76**

Appendix B **79**

1. Introduction

Nowadays the amount of people using internet on the daily basis is "…no longer growing arithmetically; it's growing exponentially" (O'Reilly & Batelle, 2009). By different means people are gathering information on the web and sharing their own data. Users keep posting news updates on Facebook and Twitter, sharing their locations on FourSquare, pictures on Instagram, videos on Snapchat and use other applications and websites. Nonetheless, the main question that they should ask themselves is who exactly they are sharing it all with. With development of technologies and growth of transparency on the internet the information that users share online is easily accessible to a lot of individuals who are also involved in using internet (Madden, 2007). In this case, if someone posts something compromising or provocative, it can be seen by someone who it was not intended to be seen by. That is why the phenomenon that is the main focus of the paper is urgent and eligible for the analysis. Namely, it is cybervetting, online- or pre-screening, how it can also be called.

The term was introduced in the beginning of the 20th century, after the Web 2.0 became respectively widely used (O'Reilly, 2007), and it can be described as employers' use of employees' online information for personnel selection (Berkelaar, 2014). Online sources that are used by employers while cybervetting are not usually used for professional tasks (as, for instance, LinkedIn). The employers in this case collect information from "…informal, non-institutional, online sources to inform personnel selection decisions" (Berkelaar, 2014, p. 480). A crucial point is that cybervetting occurs "…without workers' specific knowledge, permission or opportunity for correction" (Berkelaar, 2014, p. 480; also see Ramirez, Walther, Burgoon, & Sunnafrank, 2002). It is possible to establish the connection with what was just said in the first paragraph: all the information that people share online in various social media can be available not only to them and their friends, but can also be visible to their employers or colleagues in general.

Cybervetting has been the topic of several academic studies in the last decade, and these have been devoted to multiple practical aspects of the phenomenon. For instance, there are papers written on the employers' use of cybervetting and reasons for it (Berkelaar & Buzzanell, 2014), about privacy violation and its relation to cybervetting (Yanisky-Ravid, 2014; Ghoshray, 2013a; Craver, 2006; Hunt & Bell, 2014; Kovach, Kenneth, Jordan, Tansey, & Framiñan, 2000; Mitrou & Karyda, 2006) and about the risks for employers, when they use cybervetting (Mikkelson, 2010). A lot of attention is paid to the employers' perspective and different ethical issues; discussions include topics of self-presentation, self-construction and impression management. However, even if a lot of issues connected with cybervetting are already discussed

in the literature, this topic is respectively new and has a few gaps.

For instance, reaction of employees and job seekers to the phenomenon is understudied. There are a few works that are addressing the job seekers perspective (Stoughton, Thompson & Meade, 2013; Berkelaar, 2014), but only in the latter the data is collected in a realistic environment from actual potential employees, while in the first case the situation of employment and other conditions are hypothetical. For understanding the potential directions for the current research, it is necessary to provide more details about those existing empirical projects. In both of them a qualitative approach is used, and they are aimed at finding out the job seekers' attitude towards the phenomenon of cybervetting and their expectations from the employers.

The first article describes two studies. In the first study a realistic selection scenario was applied to participants and after that their reactions to cybervetting were investigated. In the second study the selection scenario was just described to the participants and their reactions were explored (Stoughton, Thompson & Meade, 2013). However, there are limitations to those results, because participants in both cases were informed that they are involved in some kind of experiment. Even if the nature of it was not clear to them, the Hawthorne effect might have had some influence on how they reflected on the process of cybervetting (Dunning, 2008). The article by Berkelaar (2014) is closer to the main idea of the current project, as the author is analyzing the interviews with employees and job candidates about their perception of the phenomenon of cybervetting.

Still, there is enough space for investigations in this field. For instance, the samples in the abovementioned research papers consist of young job applicants: the mean age of the participants was 19.32 in one case (Stoughton, Thompson & Meade, 2013) and median age was 22 in the second case (Berkelaar, 2014). Therefore, the older age group is quite underexplored and there is a solid reason to fulfill this gap. The main idea is that different age groups might perceive being online in various ways, hence, they might perceive cybervetting differently as well. Some researchers suggest that perception of information as public or personal depends on the age group – "…younger generation assumes that everything is public; the older generation does not" (Berkelaar, 2014, p. 493). This can also be viewed from a perspective of technology adoption in general. Younger people are often the early adopters of technology (O'Keefe & O'Connor, 1998), which means that they are more involved in using internet and, as a result, perceive it rather differently from older people's view. Moreover, there are a few terms that also explain the differences between the age groups. The term *digital native* describes people, who were born after year 1980 and were socialized in the internet and personal computer environment (Jones & Shao, 2011). The second term is *digital immigrants* – those, who were born before

1980, but have also adopted technology and started using it in their everyday life. The age of digital natives today is around 35-36 years old, which is used as an additional justification in the methods chapter: groups of people younger and older then 35 years might have different attitudes towards cybervetting and develop new practices of behavior.

Another aspect has not been studied in relation to cybervetting, and current research can help fulfill this gap. In the research available on the topic of cybervetting only the attitudes towards the phenomenon are studied. However, there might be some active response to being cybervetted, expressed in some concrete actions, and in current work it is crucial to have a closer look not only at the attitudes, but also at practices on self-presentation that evolve along with cybervetting.

Some other issues connected with cybervetting were discussed in detail within the research on the topic and provide material for further investigation (see Yanisky-Ravid, 2014; Ghoshray, 2013a; Craver, 2006; Hunt & Bell, 2014; Kovach et al., 2000; Mitrou & Karyda, 2006). For instance, the relation between practices of cybervetting and privacy are quite often studied by researchers – they are trying to figure out if the workers and job seekers perceive cybervetting as intolerable privacy violation, or there can be some kind of balance between private and personal. It is also closely connected with the studies about 'private' and 'public' online. There are two clashing opinions on that. The first is that "…online information [is] public or visible" (i.e., available and easily accessible; Treem & Leonardi, 2012, p. 154), and the second one is that "…online information [is] private, personal, irrelevant, and unstandardized" (Kluemper, 2013, p. 8; see also Sánchez Abril, Levin, & Del Riego, 2012). Even if the second perspective is taken into account, meaning that online information is considered to be private and employers' use of social networks constitutes a violation of applicants' privacy (see Finder, 2006; Levinson, 2011), in recent years "…the use of social media forms a regular part of the recruitment process" (Grant & Lewis, 2014, p.17), which presupposes that with time the practice must only become more popular.

As long as cybervetting is a respectively new phenomenon, the fact that the attitude towards it may be changing can also be explained in terms of the diffusion of innovation. Katz, Levin and Hamilton (1963) define the process of diffusion, or, in other words, adoption of innovation, as acceptance over time of specific item, or idea, or practice by individuals, groups or other units, linked to specific channels of communication, to a social culture and to a given system of values. So, cybervetting as a newly emerged social practice is going to move through steps of being accepted over time by employers and employees within corporate culture. When the pervasive adoption of technology occurs, people start expressing new attitudes towards it

(Fichman & Kemerer, 2013).

The last but not least thing to mention is that, despite the growing interest towards the phenomenon and its spreading use, it is mostly researched within a Western European and American context. As mentioned in an American study by Mikkelson (2010), 79% of employers used online information of job candidates for evaluation by they year of the study. Later Grasz (ca. 2014) has also discovered that, according to a report based on the survey by CareerBuilder, 51% of employers did not hire a candidate because of the information that was obtained my means of screenin social networks.

However, as a person with a non-European background I became interested whether a similar phenomenon is of concern in Russian society. After a careful investigation of existing information I came to the conclusion that there has not been any research works written on this topic, except for a master thesis that has not been published online (Tsvetkova, 2014), but the name of the author and the abstract are available on the website of a Moscow University Higher School of Economics (https://www.hse.ru/edu/vkr/125124386). But at the same time a lot of the information regarding cybervetting is located on various forums or websites for job search in the form of advice for both, employers and job candidates, which supports the claim that the practice is existent and widely used. Employers are told that they can find a lot of useful information if they address the online space of their potential employees; job seekers, in their turn, are told that they should delete everything that can compromise them from the social networks in order to make it impossible for an employer find something discrediting (see Murakhovsky, 2014; Prokofieva, 2009; Umarov, 2010; "Social Networks and Job Search", 2015). This kind of vicious circle does not really give any idea about the use of this practice in the country or attitudes and practices that are developed in relation and response to it, and studying the phenomenon in the Russian setting seems a novel and challenging task.

By briefly outlining the main theoretical and practical achievements in the field I aim to demonstrate that the project is scientifically and socially relevant. The study will fulfill the knowledge gap, which is still present around cybervetting – elder age group is understudied, the actual practices as a response to cybervetting are not discussed in the scientific literature, and the phenomenon is not studied within Russian context.

The aforementioned observations leads to narrowing the focus of the paper and presenting the main research question: How do practices of managing social media differ among younger and older Russian job seekers once they are aware of a possibility of being cybervetted? Younger group consists of job seekers aged from 18 to 35 years old, and elder group – from job seekers aged older than 36 years old. For the purpose of answering the main question, I would

also need to answer to the following sub-questions: “How do Russian job seekers frame cybervetting?”, “What is the attitude of Russian job seekers to cybervetting?”, “How do Russian job seekers frame privacy?”, “What is the relationship between privacy and cybervetting in the opinion of Russian job seekers?” and “What are the actions of managing online space, undertaken by Russian job seekers?”

In order to be able to answer those questions, a qualitative approach was chosen, and in-depth interviews are a method of data collection. This method proved to be successful in previous research on the topic, and even though it does not provide a researcher with an opportunity to generalize the results, it is perfectly suitable for studying this phenomenon as well as practices, attitudes and opinions (Neuman, 2005). Theoretical insights were used in order to create and structure an interview guide for semi-structured interviews (see Appendix A), which were chosen as long as the open-ended nature of the questions allows new themes to emerge during the interview (Dicicco-Bloom & Crabtree, 2006). This method of data collection led to the fact that future steps of analysis – open coding, axial coding and selective coding – were both, theory-driven and data-driven. Some concepts were initially placed in the interview guide and further emerged as categories for analysis, but other concepts were presented by the respondents themselves and further included in the analysis as well. However, that will be more elaborated on in the methodological part.

In the introductory part of the research I tried to demonstrate societal and scientific importance of the studied phenomenon at least at a basic level. Further findings about the practice of cybervetting are presented in the second chapter of the current project in a theoretical overview. The issues discussed touch upon privacy on the internet and in the offline space, as well as its relation to cybervetting. Employers’ and job seekers’ attitude towards the phenomenon is also covered in the theoretical chapter. After that the main ideas about impression management are present in the chapter, and followed up with a final part, concerning Russian context. It is followed by a more detailed methodological chapter, which includes description of the procedures of operationalization of main concepts, sampling, data collection and analysis. After that a results chapter is presented, which includes the following constituents: information about use of internet and social networks by the respondents, their knowledge and awareness of cybervetting, privacy issues that are raised in relation to cybervetting. Moreover, attitudes towards cybervetting, offered regulations to cybervetting and actions, undertaken as a response to potential possibility of being cybervetted are discussed in this chapter. The study ends with a general conclusion and prospects for future research on the topic.

2. Theory and previous research

There is quite an extensive body of literature about the phenomenon of cybervetting, even though it is relatively new. The literature regarding this topic can be roughly divided into a few categories, briefly discussed in the introduction. There are studies that appear to be an overview of the phenomenon of cybervetting and they cover various theoretical issues, connected to it. Other studies mostly address cybervetting as a general practice: they present it from the employers' and job candidates' perspective, also demonstrate the advantages and disadvantages of the screening method for those groups of people. Privacy issues are also addressed in the literature on cybervetting. However, in order to better understand the attitudes and practices that may emerge as a response to cybervetting in Russian society, it is necessary to consider other topics as well. The first one is privacy, so that it is clearer to the reader, what can be seen as public or private space as well as how privacy violation is in social networks is understood. The second one is digital footprint, which is an important term to take into consideration while speaking about managing online space. Managing online space, in its turn, has a lot to do with impression management tools. The last thing to address in this chapter is the Russian historical context and issues, connected with social networks use.

Taking the abovementioned themes into consideration, it was decided to structure the literature review part in the following way. The first part is an attempt to define privacy and bring up the challenges connected with its understanding, as well as other phenomena that can influence perception of privacy (for instance, the digital footprint). The next section brings up the topic about relations between cybervetting and privacy. It is followed by two sections, devoted to employers' and job seekers' perspective on cybervetting. A separate section deals with impression management online, and the last section is description of Russian context of social networks.

2.1. Privacy on the internet

There is a debate about how to define privacy, and the opinions vary from the "right to be alone" in the offline space (Brandeis & Warren, 1890, p. 195) to the "right to prevent the disclosure of personal information" (Joinson & Paine, 2007, p. 242). Distinguishing those two accounts is necessary because the latter suggests a degree of control and some autonomy of person's information, while the former presupposes the absence of external contacts. Distinguishing those different approaches leads to the fact that privacy could be understood in different ways by the participants of the study, and they might express different concerns related to it. Another work, written by Parker (1973) offers a set of definitions and possibilities to define privacy. From the author's viewpoint, it can be seen as a form of power, a psychological state,

and a right, or a claim, or freedom not to participate (Parker, 1973). A key point that the author also makes that the definition should first and most importantly fit the data and be not too extensive or too narrow. Which is why it is possible to conclude that, for instance, the "right to be alone", as Brandeis and Warren (1890) define privacy, is too broad and not very suitable for current research, but it seems quite reasonable to take the definition by Joinson and Paine (2007) as an initial one for understanding privacy.

Despite the fact that there is no unitary concept of privacy, the society in general and the individuals in particular attach high levels of importance to privacy and protecting it. Over time multiple works have been written on privacy issues in general (see Altman, 1975; Brandeis & Warren, 1980; Rubenfeld, 1989; Bennett, Brassard, Crépeau, & Maurer, 1995; Sweeney, 2002) and in the last decade – privacy in cybervetting (see Cohen & Cohen, 2007; Mikkelson, 2010; Hunt & Bell, 2014; Ghoshray, 2013a). Those works provide evidence for the fact that people are concerned about their privacy and its possible violation by other people. Still, as it was mentioned, people can attach different meanings to privacy. That is why in recognition of the diverging accounts of privacy in academic literature, one of the goals within the current study will be to address personal perception of privacy in people's offline and online spaces so that it would be possible to better understand what can be considered by them as privacy violation.

The concepts that are closely connected to privacy are public and private space. Even though the latter seems to be identical to privacy, it is narrower and can be understood in different ways. The basis for defining public and private space can be grounded in Goffman's theory of self-presentation. The author introduces two main concepts, frontstage and backstage in real life communications. In general words, the frontstage is a setting where the actor is performing, creating an image of himself, using impression management tools to bring a message to other people. That can be also called a public space, where people are communicating with outer world. The backstage, in its turn, is the space where the 'inner self' exists, this is a private territory, where other people are most likely not allowed (Goffman, 1973). In terms of social networks, public space or rather frontstage is present in the open profiles of users. Thus, there is a major concern in terms of privacy, as it is not clear who is this information is really aimed at and is it perceived by users as available to everyone. Private space, or backstage, is almost absent in social networks; however, partly it can be observed, for instance, in the instant messages between individuals, or when some information with privacy settings is concerned (Hogan, 2010). This situation, though, is comparable with offline communication with closest friends, when a person also discloses his inner self more than while contacting a stranger or an acquaintance. Such an idea can also be supported by the model

offered by Subrahmanyam, Reich, Waechter, & Espinoza (2008). The authors suggest that one of the reasons why users are concerned about their privacy online may be co-construction of identity, which is related to the offline world. A major implication of this model is that those worlds are connected, which is why is it expected that users bring people and privacy issues from their offline worlds into their online ones. Most importantly, analyzing behavior of an individual in one of these contexts may lead to making assumptions about his possible behavior in the other one.

The term that is necessary to pay attention to in this context as well is self-disclosure. It means telling about previously unknown so that it becomes shared knowledge; it is the "process of making the self known to others" (Jourard & Lasakow, 1958, p. 91), and as well as it can happen offline, it can take place online. The main concern in this case is that sometimes a person is not willing to self-disclose to others, but information that he provides on the internet can tell more about him than he implied to be seen. More importantly, disclosure can happen on different levels – between individuals or within smaller or bigger groups (Joinson & Paine, 2007), and if in personal offline communication it is possible to choose between those levels, the information online makes disclosure public and available to different groups of people.

The concept of privacy, as it is seen, has been studied not only on the offline level, but it has been applied to technologies and the internet (see Agre & Rotenberg, 1997; Austin, 2003; Cranor, 1999). A lot of attention in this context is paid to computer-mediated communication (CMC). Present body of literature demonstrates that CMC entails high levels of self-disclosure, thus small space for privacy (Walther, 2011). That is why it can be a clear explanation for people's unwillingness to share their personal information online. It only stresses their privacy concerns, and the most important of them are level and type of information that is collected online about them, and also lack of knowledge about how this information may be used by those who can get access to it (Metzger 2004). That is why more extreme positions emerge that new technologies allow intrusion into originally private spaces and compromise the very idea of private space, making it nonexistent. However, Boyd and Ellison (2007) introduce a concept of public or semi-public profile in social networking sites. Basically, in such a distinction private profile actually does not exist, but some private features are present, as it was mentioned before – for example, instant messages or privacy settings, that can partly protect the profile from onlookers. This is an important consideration, because it becomes clear that the distinction is not just binary – public and private, – but there can be other nuances like the abovementioned.

A lot of the personal information about users is available online, mostly in self-descriptive personal profiles (Gross & Acquisti, 2005). In this case it becomes more than just

information, but rather data that can be used for any purposes and analyses (Joinson & Paine, 2007), and the value of this data is just increasing over time. It can be used in order to make statistical generalizations in terms of socio-demographic characteristics of people as well as help create psychological portrays of particular individuals (Gould & Belyakova, 2013). Not all the users are eager to share this kind of information, but while registering online they are inevitably leaving a digital footprint, making themselves visible to other individuals online. This is another term, closely connected to privacy. Spark-Jones (2003) points out the general patterns of the kind of information, collected by means of tracing a digital footprint. The first pattern is that it is permanent, meaning that once collected, it rarely is deleted. The second is that the information can be collected in huge amounts due to highly technological systems and enough space for storage. The third pattern is that the means of how the information is collected are invisible to people from whom the information is collected. It also entails accessibility, meaning that information can be seen by any number of people. So, all those patterns affect privacy, and taking into account the high level of connectivity on the internet and penetration of internet in people's lives, it is clear why those issues are so acute in the context of current research.

All in all, a lack of users' confidence in information privacy online has been identified as a major problem entailing the growth of internet use (Malhotra, Kim & Agarwal, 2004). Despite the fact that every year more people join the internet, privacy issues are still acute. Joinson and Paine (2007) have classified online users by their level of concern about privacy online by means of a quantitative study. For this purpose the participants were offered a number of Likert statements about privacy to evaluate, and in the end three groups of users emerged based on their concerns. Participants of the study were divided into fundamentalists – those, who are concerned about their privacy online and offline, unconcerned users, and pragmatists, that are partly concerned about some particular issues. Overall results also show that 84% of all users are either concerned about their privacy or at least partly concerned (fundamentalists and pragmatists). However, this is an American study, and it would be interesting to see whether such a distinction can be applied in Russian context.

Nonetheless, even taking into account seemingly high level of people's concern about their privacy, some scholars point out that this topic is more relevant when talking about filling in questionnaires online or in terms of e-commerce rather then in the context of social networks and cybervetting (Zukowski & Brown, 2007). That may be connected with the fact that while filling in some information about themselves or sharing their payment details people are more aware of risk taking. Risk taking is often associated with privacy in social networks and it is reflected in such actions as sharing specific personal information like an address, phone number

or online purchases with providing details of credit cards or bank accounts (Fogel & Nehmad, 2009). So, while people are creating profiles in social networks, the setting is not the same with filling in the payment details, which may influence their perception in terms of privacy. In the first case the risk is not as tangible and immediate as it is in case of online payment. However, even though the risks, connected with online payments are linked directly to money, in less evident situations, as mentioned before, other types of capital may also come in play and fall under the risk – autonomy, privacy or reputation. That is why in more recent years the cases in which the users are concerned about disclosing their information in social networks are occurring more often (see "Depressed Woman", 2009; Arthur, 2012). Online users start to realize that "… surveillance and visibility are at the heart of the interpersonal use of Facebook…" and other social networks, and they see it mostly as 'creeping' and 'stalking' (Trottier, 2012, p. 321). This evidence supports the social relevance of the current study, and even though the observations were made within American and European context, non-academic sources in Russia also suggest that this topic becomes widely discussed (see Bedareva, 2014; Savchenko, 2012; "Fired for Love to Facebook", 2016). Still, the relationship between privacy and social networks are covered in more details directly within the studies about cybervetting.

2.2. Cybervetting and privacy

Privacy issues are one of the main concerns that are associated with cybervetting. The definition of cybervetting has already been brought to notice in the introduction; nonetheless there are a few clarifications that need to be made. As it was mentioned above, cybervetting does not give job candidates or workers an opportunity to knowingly control the information that is available to the employer, because the employers most often are not announcing the fact that they are using cybervetting for personnel selection (Berkelaar, 2014). That is closely interrelated with a definition of privacy, presented by Parker (1973) in the previous chapter. By not letting job seekers to know about them being cybervetted, employers, from this viewpoint, are violating their privacy. So, on the one hand, information online is publicly available to anyone and employers must not be an exception. On the other hand, social networks were primarily created for sharing information and communicating (Kaplan & Haenlein, 2010), not informing personnel selection. However, as it was mentioned by Trottier and Lyon (2012), social media apart from those functions becomes an important surveillance tool, and the main question that is of concern to researchers is whether there can be a balance between privacy and opportunity of the employers to get additional relevant information about job candidates or workers.

As well as privacy issues in general, privacy in the context of personnel selection can be discussed on two levels – workplace surveillance offline and cybervetting. Craver (2006),

Kovach et al. (2000) and Mitrou and Karyda (2006) write mostly about privacy issues in general, connected with procedures of employment or work. The authors mention surveillance cameras and medical and personality tests along with e-mail and various online activity checks as the methods of getting additional information, performed by the employers. The authors focus on the fact that if even some of those activities may seem unethical from the viewpoint of job candidates, their usage can be invaluable to the employers, as long as some behavioral or psychological peculiarities may not be visible straight away during job interviews. However, as it was mentioned, the works by those authors cover workplace surveillance mostly in an offline sense and within the boundaries of a workplace, which is still important for framing cybervetting as a practice that is rooted in those measures. One of the reasons why they do not mention cybervetting a lot is because the platforms that are usually explored in the context of cybervetting nowadays are Facebook, that was launched in 2004, MySpace – in 2005, Twitter – in 2006, while the e-mail became more or less common since 1993 (Crocker, n.d.).

More recent works by Cohen and Cohen (2007) and Hunt and Bell (2014) focus on the division between on-duty and off-duty times and connected to it surveillance practices in social media. The authors do not directly talk about checking information about potential candidates or even workers. However, what is important in this case is tracking online activities at the job place. If using, for instance, social networks is not necessary for professional tasks, its usage by the employees at work may entail negative attitude from the employer. Otherwise, use of social networks and their content outside of the job place are not evaluated by the employer and do not influence the relationships between the employee and the employer. The balance, in authors' eyes, can be achieved if the off-duty activity of workers will not be tracked, which gives them privacy in their personal life. But even though the main idea seems to be that there is a rigid boundary between online and offline, it is also blurring over time (see Wittel, 2001).

The last but not least authors to be mentioned in this section are Ghoshray (2013a), Hayes and Cooley (2013) and Yaninsky-Ravid (2014), who cover the phenomenon of cybervetting exactly in the sense, in which we understand it in this work, and also add Instagram (launched in 2010) to the list of online platforms that can be screened in order to get additional information about the job candidates. One of those authors mentions the fact that privacy in social media in general is "…heading towards annihilation" (Ghoshray, 2013a). Even though this is a rather stark perspective on privacy, it is closely connected with the fact that any personal information, provided online, as Spark-Jones (2003) mentioned, is collected over longer periods of time and can be accessible by an undetermined amount of individuals. So, drawing from that, it is important to see whether job seekers, especially in the Russian context, perceive social networks

as a setting where privacy is non-existent, or they think that there is place for privacy. Then it can be discovered whether the respondents think of cybervetting as their privacy violation or just a mechanism for protecting employers' legitimate business interests.

However, a reasonable point is made by Mikkelson (2010), who mentions that even though people may treat cybervetting as a general practice neutrally, there might be valid reasons why people may want to maintain their privacy on social networks – they may be afraid of facing racial, gender or other types of discrimination. That is why the author emphasized the necessity of creating well-crafted policies of cybervetting that could regulate the activity of the employers and inform the job seekers about what they can expect. However, before turning to the position of the latter, it is still important to look at how the employers see the practice, because this issue was touched upon in the interviews multiple times.

2.3. Employers' perspective on cybervetting

The attitudes that employers express towards cybervetting that are described in literature can be summarized as 'cybervetting as a useful method', 'cybervetting as an available method' and 'cybervetting as fun'. That is reported in more detail in the next paragraphs.

Some employers find cybervetting to be quite a useful tool for finding additional job-related information on their workers and job candidates, and that is the actual point of the practice according to its definition. The first point that they believe in is that checking online information may help them find someone with a right fit for the job (Berkelaar & Buzzanell, 2014), because it is possible to trace some interests or characteristics of a person, that can be invaluable for a certain position. It is also possible to reveal some peculiarities that may become a barrier for getting along with a person. The second point is that the information online seems undisguised (Yaninsky-Ravid, 2014), which may be not the same in the CV or during the job interview, which tend to be deceptive, because various tools of impression management could be used. At the same time, undisguised information is quite often named as a disadvantage by the job seekers, but it will be covered in the next section. The third point that is mentioned by the employers is connected with previous two and it is about managing the risk of employing people, who are not suitable for the job or who can be harmful for organizational reputation management or confidential information protection.

Employers also tend to characterize cybervetting as a method that is becoming more available over time. It is becoming widely used and acceptable, and more people find it convenient. That is why some employers start using cybervetting not because it is inevitable to get more information about the applicants, but because it becomes a common and accepted practice. As Mikkelson (2010) also mentioned in her study, in 2009 the amount of people using

screening to evaluate the candidates online increased to 45% compared to 22% in 2008, and 11% of the participants of the survey in 2009 also stated that they plan to start using this practice. One of the reasons for it was that employers did not want to be less informed about the candidates than were those employers, who possessed online information. So, the practice in general, as perceived by employers, can be described as available and efficient (Ghoshray, 2013b), and as transformative in a sense that it becomes essential to business practices (Grant & Lewis, 2014).

The last position that is expressed in respect to cybervetting is seeing the practice as 'fun' (Ghoshray, 2013a). Some employers tend to use it in order to get some interesting facts about the workers that may be not seen in a working environment. In this case cybervetting ceases to be a criterion that influences making a decision about hiring a person, because it is rather getting additional knowledge without practical needs. Although this is a possible way of using cybervetting, as long as it may be seen as a supplement to the broader evaluating process, it is still not the focus of this paper, and it seems crucial to explore more practical issues.

2.4. Job seekers' perspective on cybervetting

As it was discovered, based on a previous research, job seekers have quite a homogenous opinion about cybervetting, and it can be described as a rather negative one. One of the ways in which job candidates frame the phenomenon is closely connected to the issues of privacy. They tend to describe cybervetting as invasion and violation of privacy and lack of respect to their personal life (Craver, 2006). So, respondents in this case consider social networks a part of their private life, and, according to the definition, they possess certain control over the information that they provide. Checking this information without their permission is obviously seen by them as a privacy violation. What is more, some of the respondents mentioned that pre-screening could be the sign that they will be treated badly in the future while working for a company that does not respect one's privacy (Berkelaar, 2014).

Another pattern that was noticed in US- and European-based studies on cybervetting is the job seekers' inclination to be quite defensive while talking about cybervetting. They point out that the fact that the employers use pre-screening does not give them the opportunity to defend themselves or even "…twist things to be positive" (Berkelaar, 2014, p. 490) as it is possible during the interviews. So, while it is a well-known fact that during the interviews candidates tend to be strategic in terms of self-presentation and, hence, sometimes deceptive, and also give socially desirable answers (Nederhof, 1985), it is important to have a look at strategies of online impression management, which will be done in the next section.

The last thing to mention is that job seekers want, but do not really expect the employers to be transparent about their cybervetting practices, which makes it one-sided and is not

appreciated by the job seekers (Ghoshray, 2013a). The reason for such an opinion is that the employers possess certain power over job candidates and employees and they do not have to report to them about their actions and decisions. However, from a purely human viewpoint the job candidates would appreciate being informed about cybervetting as about an additional criterion.

Despite all the differences, there is one viewpoint or rather gap in opinions that is shared by both employers and job candidates. There is still no agreement on what is legitimate and possible in cybervetting, and both parties agree that the whole process needs standardization in order to be used without unsatisfactory consequences (Mikkelson, 2010).

2.5. Impression management online

Impression management or self-presentation online is a phenomenon that, as well as the ones previously discussed, emerged in the offline space and later became used in the online space, especially within social networks. The same incentive is valid for using the tools of impression management online as offline – to make a desirable impression on the interlocutor (Nederhof, 1985). However, different users see desirable image of themselves differently, as long as they pursue different goals in their impression-management. That is why it is possible to divide the main strategies of self-presentation online into three main groups: presenting oneself closely to reality, presenting a 'best self' and presenting oneself deceptively (including anonymity and pseudonymity).

The first strategy, according to numerous research papers (see Vazire & Gosling, 2004; Gosling, Augustine, & Vazire, 2011) is used by people most often. It is explained by the fact that online and offline spaces are still closely connected in the mind of users, and they often think about the situation in which they are going to be compared to their online profile in reality, for instance when they are going to meet someone for the first time (Ellison, Hancock, Toma, 2008). In this case people do not want to be overly deceptive, because disappointment may follow during the personal contact. It is also true that as long as an individual provides more or less realistic information about him-/herself online, it becomes easier for other people to evaluate him/her and find common ideas and interests. Creating a realistic image of oneself also entails a bigger possibility of being contacted by people who are interesting in a person, not the image that he/she has created (Hughes & Beer, 2013). What is more, deceptive and misleading profiles can be considered by other people as less trustworthy (DeAndrea & Walther, 2011). Overall, in terms of cybervetting profiles that most closely match reality can be the most informative to the employers and the most honest from the perspective of the candidate. However, it is not always easy to determine whether the profile is realistic or, as the following example, embellished.

The desire to seem better is understandable and refers to initial principles of self-presentation, which imply being oriented at other people's opinion about oneself (Hughes & Beer, 2013). That is why the second strategy of managing online space is used – presenting your best or, as Hall, Pennington and Lueders (2013) also mention, 'ideal self' online. Their main focus of the paper is Facebook, and even though the realistic strategy was just discussed as a most used, the authors insist that Facebook and similar social networks can be far from reality in terms of self-presentation. That happens due to the communal sense that presents itself on different websites and certain expectations and rules that are supported by the members of the community. For instance, there is a certain kind of profile picture that is applicable on LinkedIn – it should be quite formal in order for an employer to take a person seriously (Van Dijck, 2013). Even if a person wants to be original, he/she would rather stick to the format, or his/her originality might cost him/her a workplace. So, in this case it is more important to keep to established norms of behavior rather then being concerned about inconsistencies between online profile and offline personality. Embellished profiles are almost always the most attractive to other users and even employers, who are checking online information. Though, they can also rise doubts, as long as they are 'too ideal', which is why by creating the attractive profile users can sometimes reach the opposite aim – scare off potential employers (Hall et al., 2013).

There is also a third strategy that is can be used by people – deceptive strategy. It is rarely expressed by creating a worse image of oneself, but rather creating a fake identity (e.g. under a pseudonym), or a completely empty or anonymous profile. Those actions are taken by the users in order to protect their privacy and not to share the information with the outer world (Scott, 2004). Seemingly, it can be quite successful in order to protect personal information from pre-screening from the employer and following risks. Nonetheless, those methods also may entail serious problems. There is a possibility that lack of online presence can negatively characterize a person, because he/she is rather not media literate or has some reasons to undertake actions in order to hide his/her identity (Scott, 2004). So, even in case when people are not providing any personal information about themselves on the internet, they can still provide other people, including potential employers, with some ideas or at least guesses about themselves.

2.6. Russian context of social networks

However, in addition to general information about cybervetting and privacy, it is quite crucial to mention a few peculiarities connected with use of internet, social networks and cybervetting in Russia in general. Also a few historical remarks should be made prior to addressing the reactions of respondents.

The main source used for this part of the literature review is an industrial report "Internet

in Russia: State, Tendencies and Development Perspectives" (Guscheva et al., 2013), which describes the main tendencies currently happening in this sphere. In 1991 the internet in Russia started developing quite fast. In fact, WorldWideWeb, almost as it is known now, was created in 1989, and its features were improved by 1993, which is why the development of internet in Russia was evolving more or less in parallel with the rest of world. In 1992 first websites in Russian language started to appear, by 1996 first advertisement was created, and by 1997 the internet in Russia was considered to be quite developed, with appearance of first online journals and first mailing system mail.ru in 1998. At the same time as elsewhere user-generated content was present in Russia with the development of Web 2.0 and further Web Squared (O'Reilly, 2007; O'Reilly, 2009). Which is why it is possible to conclude that there are no significant differences in basic use of internet within Russian and Western context. The main difference, however, which is now present between Russia and USA and a lot of European countries, is that Russia occupies the 50th place in the rank of all countries, by number of people using internet, while, for instance, USA occupies the 17th place, UK – the 9th, The Netherlands – the 7th place, etc. ("Internet Users by Country", 2016).

However, Russia is quite different in terms of using social networks. Most of the platforms used by people in Russia are not only well-known platforms like Facebook, but in Russian language, but rather analogous programs developed in Russia itself, but with more user-friendly interface and more appealing content. The examples of those platforms are Vkontakte (VK, launched in 2006) and Odnoklassniki (OK, launched in 2006), which are based on the idea of Facebook, but are targeting differing demographic categories. For instance, Vkontakte is used by mostly young people (below 35 years old) in Moscow and regions, while Odnoklassniki is used by people of different age groups, but mostly in regions (see "Social Networks in Russia", 2015). At the same time, prevailing audience of Facebook in Russia are middle-aged people (25-44 years old), who are quite successful in their career and income and live in Moscow, because they tend to have professional or informal contacts with foreigners who constitute the main audience of the website. Still, Russian audience uses international platforms as Instagram, Twitter or Snapchat as long as there are no worthy analogues in Russian market in terms of functionality. Recent statistics on social networks in Russia shows that Vkontakte has the biggest audience in Russia and the biggest amounts of original posts per month. This platform is followed by Instagram that gained exceptional popularity in last two years, and the third position is occupied by Facebook. Twitter takes the fifth position in this rating ("Social Networks in Russia", 2016). It demonstrates that along with Russian platforms, foreign ones take an important niche on the market, and, all in all, it is possible to say that, as well as in European

countries, employers in Russia have quite a lot of tools in order to be able to get some additional information about potential candidates online.

There are some other areas where information in social networks is being used in order to inform future decisions. One of those cases is connected with issuance of credit by banks. Undoubtedly, the main criteria for acknowledging someone as a solvent or insolvent person are still quite formal: information about the income, credit history, current job position, etc., but checking social networks becomes a source of additional information ("Pictures in Social Networks", 2016). As well as with the banks, information on social networks, even including personal messages, can be used during a court case as evidence or means of justification (Galachieva, 2012).

In respect of talking about Russian setting it is also important to make a point about privacy perception. The first and very important thing is that Soviet and Russian history has undergone periods of severe espionage and lack of personal privacy in different time periods (Petrov & Edelman, 2002). Nowadays the only case when personal details or messages can be exposed to other people is if a person committed a crime or is a suspect; however, in previous époque this type of information was mainly addressed in order to try to find something suspicious and even convict a person.

Speaking about employment procedures in particular, approximately up to the beginning of the XXI century those were also quite strict in general. Soviet questionnaires, requesting all kinds of personal information, were used for personnel selection. The information that could be of interest for an employee could vary from the property that a person had in ownership to his/her relatives living abroad (Katanova, 2009). However, those kinds of enquiries were not perceived as a privacy violation, which can influence perception of cybervetting as well.

Recently there has been a small increase of studies, connected with privacy perception in Russia. One of them, conducted by Soldatova and Olkina (2015) was aimed at revealing the attitudes towards privacy online between children and adolescents. The findings of this study justify the urgency of the current research: it was discovered that at least one third of Russian adolescents (aged less than 18 years old) make a potential risk group, because they do not completely understand the necessity of private settings online and provide excessive information about themselves and other people on social networks. This information is usually unprotected or protected by weak passwords, which is why it is easily available to other users. More importantly, and that brings us closer to the studied age groups, it was discovered that their parents seriously underestimate the capabilities of the internet and availability of this kind of information.

Another position that was expressed by John (2015) is that Russian people seem to be concerned about their privacy online and especially about the fact that other 'unwanted' people can see something that was not intended to be seen by them. At the same time they do not change their behavior online. As the author stresses out, "…judging by a lot of provocative pictures in social networks and a strange desire to post on Twitter about some illegal actions, internet users still haven't got wits". So, it can be seen that there is some controversy in terms of desiring to be private, but providing unnecessary and alerting information. Based on those findings, it is possible to suppose that Russian people might express their concerns about privacy in general to a lesser extent, which might also influence the perception of cybervetting in particular.

2.7. Conclusion

Summarizing the abovementioned empirical and conceptual developments in the field it is important to keep the research question in mind and relate all that has been studied to the job seekers' perspective.

There are a few things that have been mentioned in the introduction and literature overview that are definitely underexplored in the field. Russian historical and cultural context as well as the fact that the phenomenon is understudied in the country add to the novelty of the research. The fact that most of the observations described above were based on empirical research with the participants aged below approximately 40 years old also makes this research stand out, as two age groups are going to be compared: 18-35 and 36+. Perception of cybervetting as well as privacy is expected be different between those age groups, digital natives and immigrants (Jones & Shao, 2011) in terms of how they use internet and social media in particular, because they adopted technology in various periods of their lives. And, in general, as long as the population for current research is people, seeking job or those who have currently found one in Russia, where the pension age is 55 years for women and 60 for men, quite a large group of people has been left out in previous studies.

Privacy is one of the main concerns in cybervetting, so studying privacy issues and perceptions is inevitable in the current research in order to better understand the nature of emerging attitudes and practices. Understanding of privacy by Russian people as well as their attitude towards cybervetting in this context are one of the main topics for the analysis.

The last but not least point that was covered in a literature review and is going to be studied in the framework of cybervetting is online impression management, because it is the only available tool for job seekers on the internet in order to create an impression for the potential employer and be evaluated based on this impression.

3. Methodology

As demonstrated by the literature review, the concept of cybervetting has been problematized in diverse projects due to its complexity and controversy. It was studied within multiple frameworks with use of both quantitative and qualitative methods. Even though the idea of comparing two different age groups might be more suitable for quantitative methods with available statistical generalizations, there are a few reasons, which can support the efficiency of employing qualitative methods for this research.

As long as the main concept that is addressed in this paper are the practices of managing job seekers' public space as a response to cybervetting, it is relevant to use the qualitative methods, as they provide profound and thorough data about opinions, values, practices, etc., – concepts that are usually studied with the help of qualitative methods (Neuman, 2005). The other reason why a qualitative design is chosen is because this project is aimed at getting the insights on the awareness of job seekers about cybervetting, their attitude to this phenomenon and the way they change behavioral patterns once they know they are cybervetted, and exploratory qualitative approach is the most appropriate.

In the research works that were written on the topics connected with cybervetting, interviews and experiments are most often used as methodological tools. The information gained with the help of those methods is undoubtedly valuable. In case of interviews the researchers have and opportunity to get in-depth information about the interviewees thoughts and opinions. If the respondents misunderstand questions, it is always possible to clarify it, offer alternative questions or skip the question, if the respondent does not feel comfortable with providing certain information (Legard, Keegan, & Ward, 2003). Being able to clarify or offer alternative explanations is especially valuable while dealing with a respectively new phenomenon like cybervetting, as it might be not easy to explain in common language. What is more, there are also linguistic difficulties connected with the fact that the interviews were conducted in Russian, and cybervetting is a phenomenon that does not have a direct translation into Russian. However, that will be discussed separately.

During the experiments it is possible to see the behavior of participants, which is close to their behavior in real situation situations of employment and cybervetting. However, as it was mentioned before, the Hawthorne effect may result in inaccuracy of data (Dunning, 2008).

Therefore, semi-structured in-depth interviews were chosen as a method of data collection for the current research. This tool might be considered one of the best to address actual people's opinion. The topic list helps the researcher to guide the respondent through urgent issues, while other topics may as well emerge during the interviews themselves given the

open-ended nature of the questions of the guide (Dicicco-Bloom & Crabtree, 2006). Semi-structured interviews have already proved to be an efficient way to collect information about cybervetting. Yet, the main novelty of the current research is that the opinions of people of two different age groups are going to be studied, digital natives and digital immigrants (18-35 and 36 and older). Based on this research by Jones & Shao (2011) it was possible to suggest that there may be some differences in terms of practices, as long as both groups adopted the technology at a different point. The same idea can be found in the abovementioned study by Soldatova and Olkina (2015); however, the researchers were studying adolescents (below 18 years old) and paid less attention to elder people. As they also mentioned in the study, those aged below 18 are 'technological children', so the idea that is expressed overlaps with what Jones and Shao try to prove: younger and older generations perceive online space and manage it differently.

Another important point is that in the current study the data was collected from Russian respondents. This decision was made to some extent due to practical and pragmatic reasons: it was easier to communicate in Russian and discuss more in-depth topics as there was no language barrier, which is important while handling in-depth interviews. It was also more feasible to find respondents in both age categories

Nevertheless, there was another important reason for data collection from Russian people – as it was mentioned before, the concept of cybervetting has not been studied by Russian authors. The information provided about the phenomenon limits to the advice for job seekers, mentioned on career websites. This raises awareness of people about the fact that they can be cybervetted, however, does not address the phenomenon, attitudes or practices from a scientific viewpoint. Understanding the perspective of Russian job seekers on the phenomenon as well as their emerging practices widens the scope of the knowledge and creates a background for further research that can be comparative (between countries or cultures) or quantitative in order to generalize the results.

The topic of cybervetting has not yet resonated in the society in Russia; however, the case about banks using social networks of the candidate in order to inform their choice of potential borrowers was recently covered in media ("Pictures in Social Networks", 2016). Although it is not directly connected with the focus of the study, it shows that there can be a broader use of social media presence for evaluative purposes in various aspects of people's lives. Discussing this case with participants was a possibility to switch from talking about cybervetting in general to talking about particular spheres and professions, where cybervetting could be applied. This aspect is also based on the research by Berkelaar (2014), where the informants expressed the opinion that not all of the professions are equally important to be cybervetted.

3.1. Operationalization

The guide for conducting semi-structured interviews was used for data collection. In order to make the main concepts – attitude to cybervetting, privacy, practices of managing online space – measurable and actually observable, it was necessary to create the indicators, which will become the topic list for the interviews. For this purpose the main research question was operationalized within sub-questions and eventually within the topic list (see Appendix A). Studying attitudes to cybervetting, privacy framing and actions of respondents' managing online space inevitably led to understanding possible explanations of emerging behavior and practices as a response to cybervetting.

Before the interviews were actually conducted, the participants were informed that the topic of job seeking procedures and relationships between employers and job candidates are going to be touched upon as well as the use of the internet. However, it was not explicitly stated that cybervetting is going to be the main focus of the study, so that the following technique could be implied.

Operationalization of the first concept – attitudes towards cybervetting – presents itself indirectly throughout all the interview questions; however, the main tool for measuring this concept are experimental scenarios of job-seeking procedures. The main idea is based on the research by Stoughton, Thompson & Meade (2013), but the scenarios in this case are the tool of getting the insight about the attitude of respondent to the phenomenon in two situations: while being hired or rejected because of being cybervetted. Possible limitations, that can be caused by the abovementioned Hawthorne affect, are minimized, because attitudes towards cybervetting are analyzed based not only on those scenarios, but on any other ideas expressed by the respondents during the interviews in general. Moreover, the respondents are offered to come up with possible rules and regulations for employers' use of cybervetting. By means of providing the job candidates an opportunity to think about policy making it was expected to see which aspects of this practice they do not appreciate and would like to change. Another important idea is tested in the third, additional scenario, mentioned in the research by Ghoshray (2013a), and it is the importance of being explicitly informed about the fact of cybervetting. Scenarios within a topic list are accompanied by questions about personal experience of respondents with cybervetting and their awareness of the phenomenon, as long as information provided by those topics could also more objectively describe the attitude to the phenomenon rather then the direct question about it.

The concept of privacy was also addressed in the topic list, because it was numerously touched upon in previous research about cybervetting. In those works it was framed as both a

privacy violation and a phenomenon that does not overlap with privacy at all. However, it was not clear how privacy is framed by the respondents and what exactly they perceive as its violation. In order to be able to figure that in the current research, the questions about privacy were included in the topic list. First, the respondents were asked, how they understand privacy in general, and, most importantly, within social networks. Second, they were asked to define public and private space and explain, what social networks are for them in those terms. The last point was aimed directly at relation between cybervetting and privacy, because by this point the respondents has already developed the understanding of both phenomenon and could work with more abstract constructions rather then experimental scenarios of employment.

The last concept that needed to be studied in order to be able to answer the research question were practices of managing online space. Even though one of the questions in the topic list was about any specific actions that may help to manage online space of the respondent, relevant information could be withdrawn from other questions or statements as well. For instance, one of the questions was about the concept of digital footprint and awareness of it. Another question touched upon discovering the actions that could protect some personal information online. What is more, there was a question aimed at finding out whether the respondent has ever posted something online and later deleted it due to some reasons, with explanation of those reasons. All those questions along with the nature of semi-structured interviews helped to find out what are the practices of managing online space that are used by the respondents once they are aware of the possibility of being cybervetted.

3.2. Sampling

There are various approaches to the sampling procedure and justification. For instance, Patton (1990) argues that all the sampling in qualitative research is selective and purposeful, as it is shaped and restricted by the researcher's chosen framework, time, available to the researcher, his starting and developing interests and even some territorial restrictions. In general, this approach seems suitable, as long as I have certain criteria for the respondents and I was recruiting them based on those criteria.

The main criteria were (1) age, (2) online presence and (3) the fact that the respondent is currently seeking a job or has recently found the job (within a twelve-month period). The age related to the initial age groups 18-35 and 36+. The second criterion was online presence of participants, meaning that they are using internet in their everyday life (at least, once a week) for any kinds of purposes. It is important to mention that it was not crucial that the respondents were present in social networks at the time (for instance, they might have had no account), because that could also be a strategy of coping with the practice of cybervetting. The third criterion was a

key one as long as the practice itself is respectively new and people could have faced it only in recent years. But, in general, people tend to reflect clearer to the events that happened within some relatively short time period, which is why a twelve-month period of being employed was chosen.

The approach that was used for recruiting can be better described as a mixed method, because it was a snowball sampling combined with a quota sampling. The recruitment of respondents was initiated online in two social networks: Vkontakte and Facebook. The request to participate in a research aimed at studying attitudes and practices connected with the employer–job seekers relationships was posted in my feed and reposted by my friends, acquaintances and, afterwards, their connections. One of my acquaintances is a public persona who has over 6000 friends on Vkontakte, which is why a repost, made on his page, almost equaled a post in a community, helping me to reduce the ego-network bias. By those means my message reached people who were my third or fourth connections, so that my personal attitude could not influence my objectivity, as long as I did not personally know any of the respondents. Still, out of all the people who contacted me offering help with the research it was necessary to choose those who filled the quotas. Eventually, in order to obtain multiple perspectives on cybervetting, 14 interviews were conducted with people aged 18-35 years old (N=8), and 36 and older (N=6). The mean age in the first group is 23,13 years old, and in the older group – 47 years old. Within each group there was an equal distribution in terms of gender (four and three male and female respondents in each group, accordingly). The interviews began with gathering information about interviewees' background, their current employment status, their actions of job search and basic information about social networks use, and then proceeded to main questions.

But before conducting final interviews for the research, a trial interview was held with a 21-year-old respondent from Moscow. It was made in order to make adjustments to the guide and get insights about how the respondents understand the questions, how they react to them and what can be improved. After the trial interview the scenarios of a job-seeking procedure were shortened in order to get more information with less questions, because some of them proved to be inefficient. More detailed information about those scenarios is presented in the analytical part of the research.

Even though it is not possible to generalize the results according to quotas, the idea was to get insights about any possible differences that can be found within different groups and could later be studied by means of quantitative methods such as a large-scale survey. Previous research on cybervetting does not provide information about possible gender differences in the attitude

towards cybervetting, but researchers still suggest that sampling including equal gender and age groups provides with more diverse and structured results (Zukowski & Brown, 2007).

3.3. Data collection

The interviews were conducted via Skype and lasted on average 50 minutes. Use of Skype interviews over face-to-face is justifiable within a current research. Undoubtedly, both methods have their own advantages and disadvantages. One of the main reasons for collecting data via Skype was convenience of reaching the respondents in any time they find preferable. Another reason is that Skype calls offer the option of video, which is why the dialogue that takes place is almost the same as a real conversation with a person. It also gave an opportunity to reflect on non-verbal communication, such as tone of the voice, pauses or body language (Voida et al., 2004). As well as during face-to-face interviews it was possible to make a recording with a good quality in order to further handle the data. It was also convenient to conduct interviews with people who were territorially far away.

However, Skype interviews as well as all the procedures that involve using technological devices entailed certain problems. The main and the most expected issue was establishing internet connection, because the respondents tend to lose concentration once the dialogue is broken. Though, the connection never disappeared for a long time, so it was easy to cope with short pauses. An important point to mention here as well is that it was a personal choice of some respondents to communicate without a video. That was made due to several reasons – some of them did not have a camera, some said that they do not look presentable. That entailed two issues, connected with previously discussed points. The first one is that there were no opportunities to evaluate non-verbal communication and the extent to which the participant is actually involved in the conversation, though it was understandable from the intonations and pauses that the informants made in their speech. The second one is that while using a video call it was always easy to spot when the internet connection broke, because the picture became frozen. While having a no-video calls sometimes it was impossible to understand ahead if an interviewee was not responding because he/she was thinking, or because there was no internet connection. Still, all those issues are minor concerns and they did not really influence the process of data collection and its quality.

Before moving to the analytical part, it is necessary to mention an interesting fact that I discovered even before I started analyzing the data, which was partially connected with understanding privacy issues and overall attitude to personal information. Before the interviews I offered the participants to sign a consent form (as long as the interviews were conducted via Skype, I offered the possibility to sign them electronically). Another aspect that I clarified with

each of the respondents was whether they were against me using their names without surnames in a research. The reaction that I got was that, firstly, none of the respondents expressed a desire to sign the consent form as long as they mentioned that they trusted me as a researcher and a person who is their friends' or acquaintances' connection. Some respondents from the elder age group also mentioned that they are not familiar with digital signature and they do not find the reason important enough to learn about it. Secondly, all the participants agreed that disclosing their real names without surnames in a research would not be an issue as long as it is not possible to make any connections with their personality based only on their names. For this reason no consent forms were signed and it might be seen as a problem, but the research ethics did not allow me to insist on signing those forms. However, the best choice that I could make in order to minimize the hazards of disclosing any personal information of the respondents was to replace actual names with pseudonyms, which are reflected in the table with information about the respondents instead of their real names (see Appendix B).

The data collection process was followed up by transcribing the data. The following decision was taken in order to facilitate data analysis – the interviews were directly translated into English, as long as it is more convenient to have the data and analysis in the same language. However, a few limitations in this case were also taken into consideration, and those are linguistic peculiarities, which were mentioned before. I was addressing those as an interpreter with experience and a person who lived in Russia for my whole life. Terms 'privacy', 'cybervetting' or 'digital footprint' cannot be directly translated into Russian language, as there are no terms with exactly the same meaning. 'Privacy' could be translated as 'private space', 'cybervetting' as 'checking online information of the candidates', and 'digital footprint' as a digital trace'. That is why I was trying different strategies while talking about those terms in Russian. First I tried to name the term in Russian with its closest translation and see whether the respondent frames it correctly. If it did not happen, follow-up explanations in Russian were given in order to guide the respondent in the right direction. However, another technique proved to be even more effective after a pilot interview was conducted. As most of the respondents were literate in English language, the decision was made that it might be better to first mention the original term in English in order to get a more precise response. In order to make the responses more reliable, I was making sure that everyone understands the terms the same, if the purpose was not to discover the way in which the respondents frame them. If it was necessary to proceed with relating those terms to other concepts, and the initial understanding was not complete or wrong, the detailed explanation of terms, such as cybervetting or digital footprint, was provided.

What is also important to mention in connection to direct translation is verbatim nature of the transcript. A few things were counted out of the transcripts, such as stumbling in sentences or repetitions of words, which were caused by tempo of the speech or some other minor factors. However, when the respondent spent considerable time thinking the question over or was laughing while answering, this information was included in transcripts.

3.4. Methods of analysis

The interviews produced a lot of data, so it was necessary to systematize it. It is important to note that transcription and coding of the interviews was an effective way to familiarize myself with the data, and during this stage some patterns could already been found. However, it was necessary to minimalize the bias and subjectivity, and take everything into account – the spoken language along with the reflections about the interview and, if applicable, body language of the participants, which was observed during the interviews and later noted in the transcripts.

Thematic analysis is the method that allows the researcher to focus on some identifiable themes and patterns of living and behavior (Aronson, 1995). It also helps to go beyond the manifested and directly observed meanings and may refer to a more latent level, something implicitly referred to (Joffe & Yardley, 2004). Before the analytical interpretation itself three steps of coding were applied to the dataset: open coding, axial coding and selective coding (Boeije, 2010). An important feature in the analysis is that it was both, theory-driven and data-driven. Some of the concepts were purposefully included in the topic list and that led to emergence of corresponding categories. However, some of the categories were unforeseen and were discovered only while handling the coding procedures. For instance, such categories as ‘attitudes towards cybervetting’ or ‘practices of managing online space’ emerged as a result of operationalizing the main research question. At the same time, such categories as ‘evaluating the employer’, ‘differences between social networks’ or ‘online VS offline’ were formed by means of analyzing the data and merging the codes.

So, during the first step it was important to give codes to all the fragments in the transcript in order to see if there may be some patterns that are stressed upon or repeated. The most convenient way to do so was using software AtlasTI, which allows handling big amounts of information and emerging codes. At this stage the information from the transcript was segmented and each fragment got the code. After that the transcripts and the codes were reviewed, and similarities and differences of the codes within one transcript and between the transcripts were noted. The next stage was axial coding, and it was aimed at primary merging of similar open codes in order to create second-order themes (Babbie, 2008; Boyce & Neale, 2006). Those themes are on a more abstract level than the open codes, and even though they still are based on

the informant labels, they are already more influenced by the perception of the researcher. The last step of preparing data for interpretation was selective coding, which was aimed at finding the most important and relevant topics for the analysis and description of results. This approach also gave an opportunity not only to systematize the information that is directly connected with the guide of the interview, but also develop themes from the narratives of research participants.

4. Results

The results of the qualitative study are comprised of 14 interviews with people who are currently looking for a job (N=6) and have recently, within a year, found one (N=7), which conforms with my selection criteria. All of them are using internet on the everyday basis for different purposes, which is further demonstrated by the fact that the interviews were conducted via Skype. However, there is one case that stands out of the sample, because the last respondent has been working for a few years by now in her own business, but as long as she offers consultancy services, she has to be contacted by potential clients every time and she finds it similar to the job-seeking process.

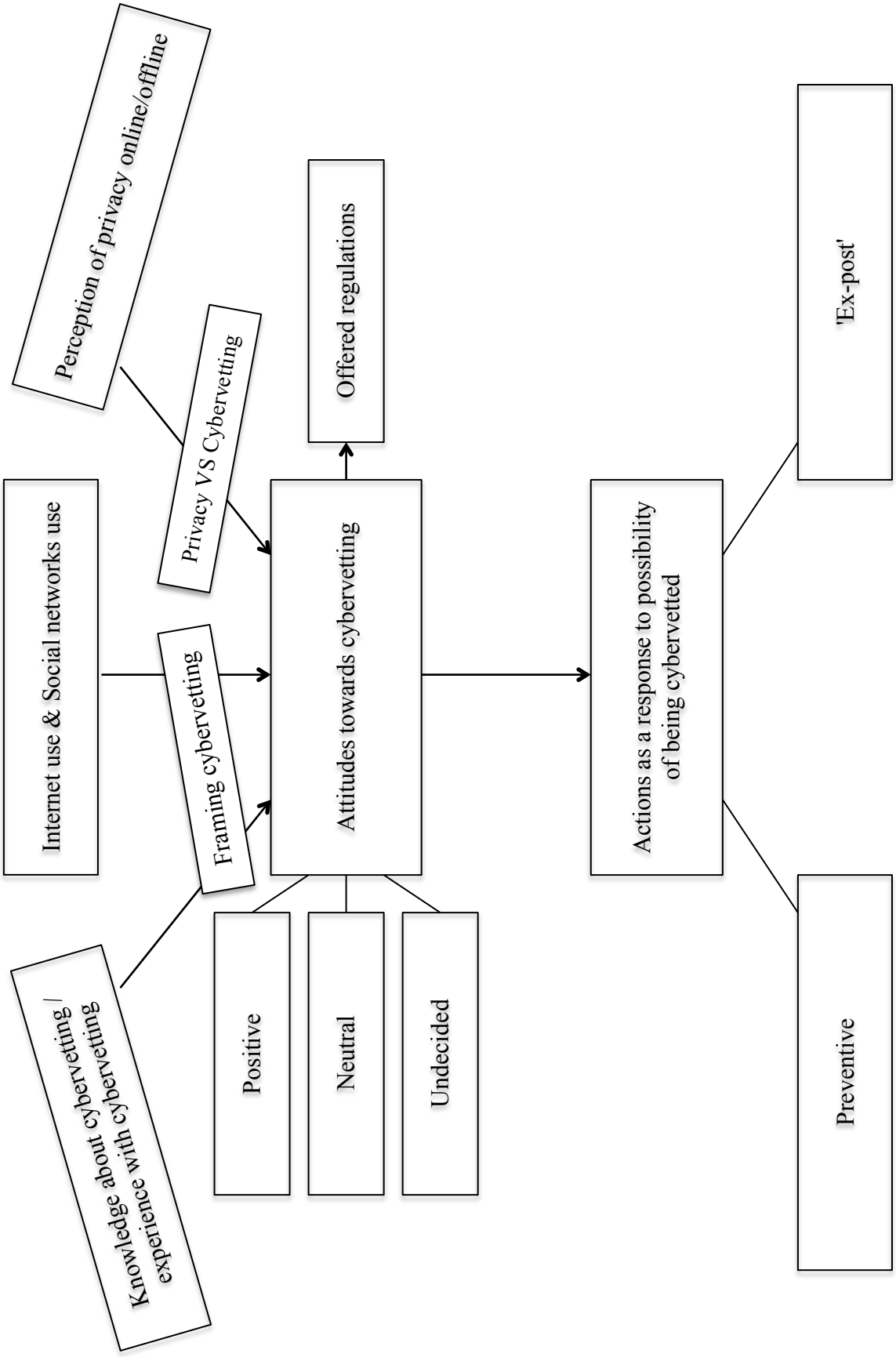
> And between the point when the clients recommend me to their friends there is some time that they spend on learning about my reputation. That's why it is very much alike with the procedure when a person is looking for an employee. . . . A lot of mechanisms can be seen from both sides – what I'm evaluating and how other people are evaluating me while hiring me to help them with projects. Katerina, 36, consultancy and marketing.

I did not pursue the aim to focus on some particular professions, however, the variety of backgrounds only allowed to get detailed, robust and accurate insights into this topic. The respondents currently occupy or are seeking for jobs in the following sectors: medicine (stomatology), marketing, consulting, education (teaching), IT, banking, engineering, accountancy, law (jurisprudence), courier services and finance. In the previous studies about cybervetting professions were sometimes named as an important criterion for cybervetting to be a reasonable measure (Berkelaar, 2014). That it why at the later stages of analysis a lot of attention was paid to making connections between the person's profession and his/her opinions and attitudes. For instance, one of the respondents, working as a courier, mentioned that he finds his job sector unsuitable for the research, because in this sphere cybervetting is an unnecessary practice. However, overall answers were informative and meaningful.

Analysis of the interviews in relation to the main research question and sub-questions resulted in creating a map that reflects on the relations between the concepts within a sample. By iterating back and forth between existing literature on the topic and information emerging from the interviews, I came to the conclusion that the main concept, defining other ones, is attitude towards the phenomenon of cybervetting. Even though it is not possible to say whether some parameters or details influence others within a qualitative study, my observations show that some connections between certain patterns exist, at least in a current sample. For instance, attitude to cybervetting can be formed according to the following categories: knowledge and awareness of cybervetting, personal experience with cybervetting, overall experience with using internet and

social networks, perception of privacy and digital footprint. The attitude towards the phenomenon can, in its turn, influence offered rules and regulations for the use of this practice by employers. Finally, and most importantly, the actions that the respondents undertake as a response to potential possibility of being cybervetted are also depending on their attitude towards the phenomenon. Figure 1 is a visual demonstration of the connections between the categories that emerged during the analysis and described in the chapter 3. After that a more detailed description of the results is presented.

Figure 1. Connections between the categories



4.1. Use of internet and social networks

In the methodological chapter main socio-demographic characteristics of the sample such as gender and age were mentioned. The latter characteristic is especially important as long as the age division is based on the idea of digital natives and immigrants and possible differences that it can entail. However, there was other additional information that the respondents provided about themselves that can be used in order to better understand the attitudes to cybervetting and the practices that are used by the participants as a response to the possibility of being cybervetted.

One of the questions in the guide of the interview was about the approximate moment of time when the participants started to use internet and social networks. The findings suggest a different perspective from what was anticipated based on the previous research by Jones & Shao (2011). However, those differences are not conceptual, but more explained by the peculiarities of the concrete sample of the current study. Jones & Shao (2011) point out that digital natives, people born in 1980 and later (aged 35-36 and younger in 2016), were growing up in the time when technologies were developing faster than before and more information was available due to the internet. That is why digital natives might be more aware of the current situation with social media. All of the respondents in this age group within the current research are below 30, with the mean age 23,13. This means that in the years 1998-2000, when the internet became relatively wide used, they were still quite young to start exploring it. That is why in the overall sample the older people had more time to get used to the internet. While younger participants started using it on average in 2005 and social networks in 2009, older people started using internet around 1999-2000 and social networks in 2006, when they just appeared in Russia. Moreover, most of them had experience before using social networks in other sources of communication online, like blogs or forums: “Social networks… Well, in the beginning there were... That were not even social networks, but more forums of interest. Rambler just started…” (Sergey, 41, financial analyst; currently unemployed).

Eventually, it is possible to conclude that even though digital immigrants in the current sample did not have the technology from the beginning, they have familiarized themselves with it, and even at earlier, in terms of the year, stages. But it is important to take into account the fact that the age of digital natives and immigrants changes over years, and in a different sample the findings would most likely indicate the difference, mentioned by Jones & Shao (2011), meaning that digital natives would be more literate and advanced users. For instance, in 2013 the situation was already changed drastically, and children aged three years old started exploring internet (Ward, 2013), which speaks in favor of Jones and Shao’s theory. So, in general, digital natives within the current sample were too young to start using internet earlier, as it was not a common

practice to introduce children to internet at a very early age. There is only one case when a 22-year old respondent started using internet quite actively in the year 1998-1999, as he says, when he was around five years old. The reason for that lies mainly in upbringing, but in general it seems not to be a trend among people around 22-26 years old. “I have a really progressive family, yes. So, just as we got Internet, I started to explore it. Of course, first under the guidance of my parents” (Lenya, 22, unemployed). That is an additional point that demonstrates the fact that in a sense digital immigrants of certain explored age group started to explore online space earlier than digital natives.

Another point to look at in this context was whether the aims of using social networks differed according to age. After coding the transcripts, different aims were discovered.

Table 1. Aims of using social networks

Communication	- informal communication (with friends and family) - formal communication (job-related or study-related)
Maintaining contacts	- with family - with colleagues/coworkers - with classmates/university mates
Organizational moments	- organize people/events
Job-related functions	- promotion of business/oneself - consulting
Entertainment	- listening to music - watching videos - playing games online - reading funny stories
Getting information	- about other people’s lives - about news - about job possibilities - about shopping
Informing other people	- about personal life - about where you are - about your hobbies
Getting noticed	- for fame - for feeling like a public persona
Saving memories	- saving pictures - saving comments - not deleting what has been posted

A few findings should be elaborated on here. The first one is that social networks, despite their growing popularity among people, were not used by the respondents as ways to look for job opportunities – this still remains a prerogative of career websites. Even though one of the aims mentioned was job communication, it was rather with colleagues or directors, but not with potential employers. The second one is that, despite the expectations, the aims of using social

networks did not really differ between the age groups within a sample. All the respondents stress that the main aims for them online are communication with people, maintaining the contacts and getting information about them or about what is happening in the world.

> So I'm using it only for communication. My study group is texting there, my students are texting me. So we can cope with some working tasks. Of course, there are also some friends, who are only in VK. Lena, 25, lecturer.
>
> (The question was about the main aim of using social networks) Communication. For learning more and for looking for colleagues and friends. Anton Alexandrovich, 58, engineer.

Similar thoughts were expressed by every respondent, which means that those aims are actually important for the participants regardless of their age, gender or occupation. A few of the participants also mentioned entertainment as one of the reasons for using social networks. However, there was still no observable difference in terms of age or other parameters, because people from both, younger and older age groups named that aim.

Other aims, presented in the Table 1 were at some point mentioned in the interviews by one or two respondents in different age groups. However, respectively small size of the sample and continuous mentioning of the same aims give grounds to say that if it was possible to increase the amount of participants, similar trends might have been found among people of different socio-demographic characteristics.

In general, aims of using the internet may not seem to be directly connected with cybervetting. However, it was noticed that people who were naming different aims were also expressing their awareness of the phenomenon or their response to it in different ways. For instance, participants who were talking about promoting themselves or their business online mentioned that they were more careful about what they post on the internet, because their goal was to attract other people. A person, who said that entertainment is the main aim of using social networks, on the contrary, said that he does not really care about what he posts on the internet, as long as he does not take it seriously (Sasha, 23, financial analyst). However, it will be more elaborated on in the chapter devoted to impression management online and actions, taken by the participants of the study as a response to possibility of being cybervetted.

4.2. Knowledge/awareness of cybervetting; personal experience with the practice

Some questions and topics in the guide were an attempt to establish the foundation for understanding whether job candidates are aware of the phenomenon in general and what exactly they know about it. As long as the knowledge does not always come from the experience, and,

according to the data, most likely is gathered from some other sources, the categories were separated in the analysis.

To begin with, the respondents were presented scenarios of job employment procedure and after discussing the outcomes they were asked whether they are aware of the phenomenon and how they first learnt about it. The answers were mostly homogenous – 11 out of 14 respondents were aware of the practice prior to the research, and 2 respondents did not know about the fact that the employers can possibly screen their online information. 1 of the respondents also noted. "I could guess that it exists, but I didn't really spend much time thinking about it" (Sasha, 23, financial analyst).

As it was expected, unfamiliarity with the term 'cybervetting' did not mean that the respondents were unaware of the practice itself. The term, in general, is mostly used by scholars, and is not widely recognized in English as well. That is why the experiences and opinions that the participants described were much more important that their recognition of a particular term or its partly imprecise translation into Russian. In the recent years they have encountered with it, mostly on media and more rare – in their personal or their friend's experience. Respondents mentioned that the information about the possibility of being screened on the internet has recently been discussed a lot on TV and on the internet, and they as people who are looking for jobs noted that they were especially attentive to this trend. A few peculiarities were also noticed during questioning the participants about their knowledge and experience with cybervetting. One of the respondents expressed the opinion of other people while answering the question about his own awareness of the phenomenon.

> Well, actually, I think, I heard more not about the practice itself, but about people condemning/judging it. . . . Yes, well, I can understand people. They've been posting some bullshit on their walls for their whole life, from the parties, and now they need to find a job, and they have to check their posts for 10 years and clean it. So this tedious work causes a feeling of indignation. Lenya, 22, unemployed.

It is important to note that along with the information about awareness the respondent labels the phenomenon with a common attitude as he perceives it, and explains the reasons for this attitude. Still, his own opinion differs from an opinion that the majority of respondents shares, but the attitudes will be discussed more precisely later on.

Another participant mentioned that her mother was working in HR and was always telling her to pay attention to the contents of social networks, as they are available to future employers. So, in this case the source of getting information about the possibility of cybervetting lies within the closest surroundings of a person – within a family, which is why it may be

perceived more seriously as family is most often an important referent group in people's lives (Shibutani, 1955). So, at this point the respondent claimed to have posted some pictures years ago that were ". . .not too intimate, but they were quite aggressive. . ." (Lena, 25, lecturer), and, eventually, a few years later she thought about it in terms of possible cybervetting. That was the main reasons that she made the folders with those pictures private, meaning, visible only to herself. She also mentioned that she did not want to delete them, as it is still a memory.

Another point that was interesting about one of the respondents is that she addressed the instruments of finding additional information about the candidates during the first times when she was looking for a job. Nataliya, a 50-year-old unemployed woman, has been looking for a job for quite a long time in her life and has followed changing trends in job seeking procedures. She claimed that the first time when she thought about the possibility of the employers to check her social networks was almost at the same time when those networks appeared. It was connected with the fact that a lot of positions that she applied to involved some additional checks, which, as she said, were rooted in Soviet practices.

> Just small private companies were collecting the information almost as in Soviet times. So, do you have a flat in your private ownership? Do you have a car in your private ownership? Do you have any relatives living abroad? So it was a questionnaire… I understood that this questionnaire was taken from this Soviet questionnaire. I can understand everything because there was security service in Soviet times; recruitment team of those companies doesn't want to work on new questionnaires. Everything could be possible, so, in comparison to that, social nets are just nothing. Nataliya, 50, PR; currently unemployed.

What is important to understand here is that perception of the phenomenon is dependent on the historical and cultural background of people, as it was suggested in the literature review. Younger people from the sample have not lived during the Soviet regime, which is why the topic of Soviet practices emerged in the most answers of only elder respondents. It also led to the fact that both background and personal experience influenced their attitude to the phenomenon and the actions, taken at the later stages. In general, other sources also support the fact that certain political regimes, such as authoritarian one, can influence the perception of social networks by certain age categories of people. For instance, elder Russian respondents mentioned Soviet security services, meaning KGB, which functioned in the time period 1954-1991 and did not attach high levels of importance to people's privacy. German Ministry for State Security, MfS, functioning from 1950 to 1990 (Murphy, 1999) presented the same functions within the similar regime. That is why, as long as Stasi (MfS) surveillance methods are compared with Facebook

functionality (see “Infographic: Facebook Vs the Stasi”, 2014), it is an understandable tendency that people who experienced the same regimes can make the same connections and compare cybervetting in social networks in Russia with Soviet practices.

The last cases to mention in this chapter are three respondents, who have actually faced this practice in real life, in spite of the opinion that this practice is not widely used in Russia (that opinion was expressed by almost half of the respondents). Encountering such a practice in two cases evoked quite a negative reaction. Here is one of the examples:

> And I didn’t really expect that when I come to that shaggy closet, the people would possess that kind of information about me. But in general it doesn’t matter. Eventually, nothing worked out with them. . . . He wasn't interested in my professional skills, I don't know at all what was interesting for him. Elena, 53, accountant; currently unemployed.

As it is clear from the situation, the first encounter with the practice happened before the respondent was actually aware of existence of this phenomenon, and afterwards she was trying to study more about pre-screening in order to be ready for the occurrence of such situations further.

Overall, it is possible to say that interviewed people are literate in terms of cybervetting. They are aware about what this practice is, which tools can be used for pre-screening and in which conditions it can be performed. That is why all the following answers and attitudes are well informed by previous experience or knowledge. What is more, all of the respondents at some point of time were looking for a job on the job listing sites, which is why they were constructing their profiles in the professional networks. In those profiles they posted their working experience along with the information about themselves, as long as it is the main resource for the employer. An outstanding feature, common to most of the respondents (12 out of 14) is that they were searching for a job quite passively. It means that they just posted information about themselves on the websites for job search and were waiting until the employer would contact them. Two other respondents have also been replying to the vacancies themselves. It is important to mention in this context because it shows the readiness of people to be observed and invited for an interview based on the information they provide. However, when it comes to cybervetting as checking profiles other then in professional networks, it is getting more complicated in terms of attitudes.

4.3. Perception of privacy

According to the literature, privacy is one of the main concerns related to cybervetting. Not crossing the borders of employees’ and job seekers’ privacy is seen as a serious issue by the

employers; however, it is noticeable that the candidates pay more attention to their privacy as they do not want it to be violated.

The first goal of this research in terms of studying privacy issues was to indicate how the respondents actually understand the term itself in relation to internet. This question is acute, because, as it was stated in the literature review, privacy can be defined in multiple ways, and even though the definition that was chosen as an initial one for the current research is privacy as a 'right to prevent the disclosure of personal information' (Joinson & Paine, 2007, p. 242), it was important to discover how the participants of the study conceptualize it. Authors touching upon questions of privacy have also not come to an agreement whether there is space for privacy on the internet and social networks. That is why the respondents were asked the questions about how they understand the term, how they understand public and private space, what is private in the social networks and how the concepts of privacy and cybervetting are related to one another. All the data collected from the respondents creates a theoretical framework that is different from what has been described in the previous research about cybervetting and privacy-related issues.

One of the main reasons for that has been already described in the theory part within the historical context. The Federal Security Service (FSS) is well known in Russia, and, how one of the respondents mentioned, it is an 'unspoken rule' (Sveta, 24, unemployed) that social networks are being checked by FSS. This measure can already be seen as a privacy violation itself, because in this case the messages are checked as well as the profiles. However, this measure is rather preventive than invasive, so the participants prefer to 'close their eyes' to what is happening and not to be 'paranoid' (Evgeny, 22, marketing assistant). The best solution of escaping being observed by FSS, in the respondents' words, is to delete all the information from the social networks and never register on any websites. This opinion is crucial, because it alters the whole attitude to privacy issues – when people are used to being observed, they start paying less attention to it and eventually stop treating it as a privacy violation. That is why the opinion of Russian respondents differs from what has been discovered previously by European and American authors. But before actually addressing the issues connected with privacy and its relation to cybervetting I am going to summarize the results in respect to conceptualizing privacy, both offline and online.

As it was mentioned in the literature review, Brandeis and Warren (1890) defined privacy as a fundamental right of being alone, rooted in the concept of liberty. Since that period of time the understanding of privacy in the offline world has not changed significantly as it is still described by scholars and understood by people as something personal, unavailable to others (see Rubenfeld, 1989; Petronio, 2012). While the majority of respondents at some point of time

talked about privacy only slightly touching upon the topic, some of the participants give definitions to how they perceive privacy in their everyday life. From those interviews it seems clear that there are two viewpoints dominating in this sample. One of them is that privacy is exceptionally personal and is not seen by other people. “Your privacy is something that you're hiding from people, maybe it's your habits or your weaknesses, some, I don’t know, worries…” (Vitya, 22, courier)

The second opinion, shared by the majority of respondents (nine out of fourteen), is that privacy can be shared with a certain person/with certain people. “Well, I think, private is something that you want to show to a particular circle of people” (Sveta, 24, unemployed).

Those definitions seemingly overlap with each other and the one given by Brandeis and Warren (1890) and later authors. Despite the fact that they include different amounts of people who can access one’s private information, both refer to restrictions and rights of a person to hide something or to share it with limited amount of people. That is also related with a definition of privacy by Parker (1973), who states that privacy is a form of power. So, some people make a decision not to share their information with anyone, while others choose a particular group of people to share private information with. At the same time, the definitions given by the respondents are different, and those differences also influence perception of privacy on the internet. Participants stating that privacy is something completely personal tended to be more categorical in terms of privacy presence online. As long as privacy is only something that is available to one person and no one else, there cannot be privacy on the internet at all.

> If you want something really personal – well, don’t make this social page, and then you will be clear and honest with yourself. Sasha, 23, financial analyst.
>
> I was saying that because I don’t understand a lot of people, who post their private information publicly, and then they are not content… they are terrified that this information actually becomes public. Lenya, 22, unemployed.

The point that is made by those few respondents (five out of fourteen) is that internet in general and social networks in particular are a public space, and something initially related to privacy can become publicly available if posted online. Though, there is an exception in terms of online messaging, but it will be discussed further.

However, there was another opinion distinguished in a sample, expressed by people who mentioned that privacy can be shared with a certain circle of people. In this case a few opportunities for preserving privacy online were discovered. The first one is privacy settings – making content available for everyone, for friends or for no one. For instance, Katerina, a 36-

year-old respondent, makes a clear distinction between social platforms and extent of privacy that she has within those networks.

> Let's start with Instagram, it's more interesting. There I have a closed profile, very small amount of people. . . .
>
> (Speaking about Facebook) The second function is maintaining some basic information about myself for some potential employers or ex-colleagues, who, due to the specifics of my profession, can be ex-colleagues and current colleagues. And even ways to get to a new employer or client. And also it's an image page for my clients. Katerina, 36, consultancy and marketing.

It is possible to conclude that by managing their privacy settings respondents were reaching particular aims on social networks, as, for instance, in the abovementioned case when open profile on Facebook is aimed at promoting a person, so it is publicly available and there is no private information. The same idea applies to the cases when people wanted to advertise their business or their interests online – in this situation the best strategy was to remove overly personal information from social networks and be ready for it to be seen by public.

Despite the fact that there were a few differences in how the respondents understand privacy, both online and offline, there was one point, which became an agreement for all the participants of the study. Sending messages in social networks as well as using applications for instant messaging was clearly perceived as a space for privacy and private interactions. For instance, people who shared the idea about privacy being completely personal mentioned that they will probably not use social networks at all for communicating important issues to other people, though it might be possible over messaging.

> If you have an urgent thing to discuss – just call your friend, than put your phone back on the table and go meet him. All those kind of questions… They should be discussed in person, that's what I think. If you really need to text something really quick, well, then… You can, of course, use instant messages – they are called 'instant' for a reason (laughing). But I wouldn't. Vladimir Sergeevich, 44, IT specialist.

People who said that privacy could be shared with a particular circle of people expressed an opinion that messages in social networks are perfectly suitable for this task.

However, it also touched upon the previously mentioned topic of the situation with privacy in Russia in general. Ten out of fourteen respondents noted that they feel that messaging is more private than publishing something for everyone, but they still allow for the possibility that their personal conversations may be see by someone else (mostly meaning FSS). Four other respondents were not concerned about that issue, but they mentioned that they do not want to be

‘paranoid’, because then the only solution, as it was offered already, is to delete everything from social networks. An interesting fact that can also be embedded in the Russian cultural background is that privacy concerns seem to be connected more with Russian systems rather then messengers in general. For instance, one of the respondents is mentioning that Facebook has two parts, private and public, and messenger is private in this case. However, later she clarifies that she trusts in it more because it is not a Russian platform.

> Messenger in this case is absolutely… absolutely private, personal thing, where there can be absolutely private information. . . . Actually I'm trying not to be too paranoid, and I'm trying to calm myself down by the thought that messenger is not a Russian platform. Katerina, 36, consultancy and marketing.

Still, despite the fact that all the respondents are to some extent aware of the possibility of their information to be seen, also even their messages to be available to other people, they claim a more free behavior in personal messages rather than in the space that is available to everyone. It goes in parallel with interpersonal relationships online. When communication happens between an individual and a group, then there are more formal rules of communications; however, communication between two people, especially those who know each other well, can be more informal.

The last point to touch upon in this section is the notion of the digital footprint. As it was stated in the literature review, Spark-Jones (2003) mentioned that digital footprint affects privacy as it includes features that are unlikely associated with right for privacy. For instance, the author stressed that once the information appears on the internet, it can rarely be completely deleted. Even if a person deletes something from his own profile, it is most likely to be saved in any kind of online storage, still accessible to other people. Which is why the respondents were asked whether they have heard about the term ‘digital footprint’ and how they understand it as well as whether the knowledge of this term makes them somewhat more aware of their actions online.

Despite the fact that all the respondents were unaware of the exact term ‘digital footprint’, only five out of them could not guess the meaning of the phenomenon and associated it with digital ID, digital signature, digital fingerprint/retina scan or could not make any guesses. The other nine respondents managed to grasp the meaning of the term and its relation to their privacy and cybervetting. The most important thing was that all the respondents after being told what digital footprint is understood clearly that it does not only consist of the information that they consciously publish online, like pictures or posts, but also something that they do without actually thinking about it.

> I understand it like this. In principle, the internet stores everything, and even if… someone told me that is not possible to delete anything from the Internet. So, even if you delete some kind of picture, it's still remains there in some bases. And, all in all, experienced people can always find it. So, for me those footprints are everything that we do, all he search queries, all the clicks. Lena, 25, lecturer.

So, after discussing the phenomenon in detail and making sure that everyone understands it, I proceeded to the question, which was aimed at finding out whether the respondents actually think about this digital footprint when they manage their online space. It was important to find out whether the knowledge about all the information being stored could actually be the reason of a more cautious behavior. The findings were quite interesting: despite the fact that all the participants were aware about the peculiarities of digital footprint, most of them mentioned that they were trying not to overreact and behave in a usual way, meaning that if there was some information that they wanted to share, they did not think about the fact that it is going to stay forever on the internet or that it is going to be seen by someone unwanted. At the same time all of them said that digital footprint is just an inseparable part of internet and it is just necessary to get used to it, which may be an outcome of Russian understanding of privacy. All in all it is possible to say that awareness of this phenomenon does not really result in changing the usual behavior of participants online.

4.4. Relations between privacy and cybervetting

After analyzing all the observations regarding interviewees' opinion on privacy online and offline it is possible to finally address the issues connected with relations between privacy and the main phenomenon of the current study – cybervetting. As it was demonstrated in the literature overview, privacy is one of the main concerns while talking about cybervetting.

As long as the prevailing opinion between the respondents was that there is rather no privacy or very limited space for privacy in social networks, it was discovered that, in the eyes of most of participants, cybervetting and privacy do not overlap. As long as profiles in social networks are not seen as a private space, it is not possible to violate that nonexistent privacy. One of the respondents sums it up for everyone else in one paragraph.

> Well, if we talk about my personal page, like Vkontakte or Instagram, I don't think that it is a violation of my private space. If they read my personal messages, my e-mails, then it's another thing. Then I think that they don't have any rights to do so, but if it is about only about checking some information that I post, that I let people see, then I think… I don't think it is a private space, so cybervetting is not a violation. Alexandra, 23, stomatologist.

The noticeable trend among the respondents is that they understand the availability of the information that they post online and, hence, the possibility of this information to be seen by the potential employee. The most interesting point in this case is that in such a sense a term 'cybervetting' as the employers' use of employees' online information for personnel selection loses its meaning. Employers are not different from all the other people who have an access to a public page on the internet, which is why, in the opinion of most of the respondents, they can use the information that they found for any purpose, such as evaluating fit for a certain position.

Even though there is no aim in the current research to make a comparative analysis between the existing studies on cybervetting and the results of this study, it is still necessary to summarize a few main points mentioned in the literature, which are radically different for the sample. As it is observed, those differences are mostly grounded in the cultural background of people rather some other individual parameters as age or gender. The first main difference lies in understanding the limits of privacy on the internet in general. From the previous research on the topic (Yanisky-Ravid, 2014; Ghoshray, 2013a; Craver, 2006; Hunt & Bell, 2014; Kovach et al., 2000; Mitrou & Karyda, 2006) it is possible to conclude that the participants of the studies perceived their social networks as their private space, which entailed perceiving cybervetting as a privacy violation. Most of the participants of the current study did not share this opinion and perceived their social networks as their public space. However, this brings me to the second point: none of the respondents said that the practice of cybervetting is violating their privacy, as long as it does not mean hacking into account or reading personal messages. That relates with understanding of privacy as a right to prevent the disclosure of personal information, because messages are seen as private information, while profile is not.

Still, once it was discovered that a possibility of being cybervetted is not the biggest concern for the participants while managing their online space, a different perspective was also taken into consideration. As it was stated before, the main reason for making a private profile was to share information with only a particular circle of people. Hence there was a question if there are some other reasons why people chose to make their profiles closed and was awareness of cybervetting one of them.

Based on the data collected it is possible to say that cybervetting is mentioned as a concern in nine cases, but it is rarely the main reason for closing profiles in social networks. What was stated by the majority of the respondents is that they want to protect their pages from unnecessary attention from other users in general rather then from potential employers.

> It protects from spam, from some idlers/onlookers. Well, now it's not so important anymore, I think, it was more in this faraway 8th-9th grade I turned on the privacy

> settings from some gossips, discussions, something… to protect from the unnecessary attention from people that I didn't want to get it from. Let's call it like that. Well, basically, first of all it protects me from spam, something like that. Alexandra, 23, stomatologist.

The term "spam" was also used in other interviews and it was related mostly to promotional pages on different websites and people, who were trying to sell some goods on the internet. However, there were more extreme cases when respondents decided to make their account private after some time being registered because they have encountered harassment or rudeness online and did not want the situation to repeat. All in all, it is clear from the viewpoints of the respondents that even though the possibility of being cybervetted can be a reason for closing the profile in social networks, more often there are other reasons influencing this decision.

4.5. Attitudes towards cybervetting

After describing the findings connected with privacy, it is possible to proceed to one of the most important concepts of the study – attitude of job seekers to cybervetting. Attitudes were measured during the whole interview; however, there was a special set of three job employment scenarios that were aimed exactly at discovering attitudes not only to the practice itself, but also to the way in which it was performed. The first scenario that was offered to the participant described a situation in which the company hired this person and also informed him/her about the fact that they were collecting additional information on social networks. The second scenario described a situation when a participant was rejected from a position because of the information that the employer found in social networks, and in this case the employer also informed the candidate about the act of cybervetting. In the third scenario it was more important to figure out whether the respondent wanted to be informed by the employer about the fact of cybervetting. So, the respondent was asked to reflect on the first two scenarios, imagining that he was not informed about the reason of being hired or rejected. However, while applying those scenarios I was aware that, as Dunning (2008) mentions in the research, the results obtained with the help of such a method might not be an accurate reflection of what the respondent would actually think or do in the real analogous situation. It can be explained by the fact that even if the experiments may describe the situation closely to reality, they cannot make a person feel as he/she would feel in real life situation. However, despite the limitations, experiments still remain the method that can demonstrate the behavior that is the most close to the one, discovered during the observations in the realistic environment (Winer, Brown & Michels, 1971). So, the conclusions were made based on the data collected.

After addressing the questions of privacy it became somewhat clear that overall trend in this sample may be that people do not have a negative view on cybervetting, as they do not see it as privacy violation. That proved to be true, however, three other types of attitudes towards cybervetting were discovered and those are: positive, neutral and 'undecided'. Each of them is going to be described in more detail.

4.5.1. Positive attitude

Quite a small number of respondents (three out of fourteen) explicitly expressed their positive attitude to the phenomenon of cybervetting. That could be explained by different parameters – one of the participants was overall more technologically literate then the others and also was close to the position of an employer herself. Two other respondents posed themselves as public and goal-oriented people, so their social networks were partly made specifically to be seen and evaluated, that is why those respondents marked especial usefulness of this practice. When the scenarios were offered to them, they tended to answer that they were aware of the practice and the fact that internet and social networks are transparent and could be possibly seen by potential employers.

> (The question was about how a person would react if he/she were told that their social networks were checked) Well, you know... With readiness, I guess. I mean that now there are a lot of materials on the internet about how to prepare for an interview, and also my mom was working in HR, so… Well, everyone always says that you should keep everything in order, especially if you're applying for some high position, they will most likely look for information about you on the Internet. Lena, 25, lecturer.

What also characterized participants who were favorably positioned towards cybervetting is the fact that they did not express any negativity or aggression when they were offered a situation about being rejected from the position based on findings from cybervetting. Usually, being rejected from a position evokes distress or negative emotions (Ployhart, Ryan & Bennett 1999). Moreover, privacy issues, connected with cybervetting and their perception by other people, described in previous research, suggest that the respondents might have expressed negative attitude towards the offered situation of rejection. However, the respondents reacted in a different way. As long as they perceived the information found by means of checking social networks a reasonable source, they just said that they might think about changing their strategy of behavior online, because other employers might not like it as well.

> The only thing is that I can ask them to clarify what exactly they didn't like in order to change my actions in future. So, for instance, when I was talking about Redbull and them not being content with the fact that I don't have any pictures of me playing team sports, I

> won't change this situation, because I don't want to seem better for this company, of course I won't do that. But if they didn't like some picture, on which I was, for instance, with very bright make up, maybe it could be understood ambiguously, then of course I will correct that and then there will be situation when I will finally delete some information, maybe. In any case, I would ask for information and depending on what they say I will decide whether I need to change the information or not. Katerina, 36, consultancy and marketing.

It seems important to elaborate more on this case. The first thing that should be brought to notice is that the position, for which Katerina was applying, had nothing to do with sports – her specialization is marketing and consultancy. However, and this topic will be also discussed later in the analysis, in this case the person's interests and private life did not match corporate ethics of the company. It was important for Redbull that employees spent enough time together playing team sports, as it strengthened the relationships in the group. As long as Katerina does not like team sports, the position in such a company was not worth considering in the first place. However, as she fairly notes, if the company pointed at some flaws that can be corrected in her profile in order to be better prepared for further interviews and positions, she should have paid attention to that and corrected information in social networks.

So, what characterizes the people who find cybervetting a useful practice is the fact that they are well aware of it and perceive it as a useful tool for creating an impression that benefits them in the eyes of an employer, and that implies a specific self-presentation strategy – presenting your better self –, as stated in the literature overview (Hughes & Beer, 2013; Hall, Pennington & Lueders, 2014). As long as they know that everyone else can also be cybervetted, they can even find a way to stand out or correct their information if the employer finds it necessary.

4.5.2. Neutral attitude

Most of the respondents (eight out of fourteen) expressed the most expected attitude to the practice of cybervetting, which is neutral. It means that people are aware of the phenomenon, but they do not really express their consent or disapproval of the practice. They rather accept the fact that cybervetting is used among the employers and find it reasonable to adapt to those new conditions. As it may be clear by now, the conclusions are not only based on the respondents' stated attitudes during the scenarios, but also more generally observed during different stages of the interview.

The neutral attitude was the most expected due to a few reasons. The first one is that most of the respondents were either aware of the existing phenomenon before the research or at least

had an assumption about its possible existence. Each of them has known about the phenomenon for at least one year, and previous research on the topic were conducted earlier, when cybervetting was even less common. So, the awareness of the phenomenon familiarized participants with the idea of the possibility of being cybervetted, so it was not a shock as it may have been a few years ago. The second one is that overall understanding of privacy, attitude towards privacy and understanding of the relations between privacy and cybervetting are more or less homogenous in the sample. It was described in detail, which is why it can just be concluded that the attitude to privacy did not suggest people being negatively or positively positioned to the phenomenon, but rather neutrally. One of the respondents stated that cybervetting in general seems not informative to her, but she can see, which kind of information other people can probably discover by its means. For another respondent her personal experience with cybervetting as well as public acceptance became a reason why she started treating it neutrally.

> And also they just started to ask the questions… but I know for sure that I can mind my tongue, I don't post anything, and I found a decent response for those questions. Another thing is that I couldn't say that I liked it too much. Only after some time more people started using it and it became okay, but before that it was quite not pleasant. Elena, 53, accountant; currently unemployed.

But even though there were no such cases in a research, personal experience could also possibly cause the opposite effect. It is closely connected with the experimental nature of the scenarios and limitations connected to it. As it was previously mentioned, only three respondents faced the practice themselves, and their opinion is a reflection on actual situations rather then an experimental model. Other respondents had to imagine the situation or at least remember someone who they know who has faced it. That is why the extent to which they express their emotions may be not full, as it is only reaction to imaginary situations. Still, the results indicate that the practice in general does not evoke negative emotions, especially after some time that it is generally becoming adopted in Russia.

4.5.3. 'Undecided' attitude

However, there were also three cases that were difficult to categorize in terms of their attitude, because the respondents provided with a lot of additional information and insights into topics that were not initially touched upon by the questionnaire, and they also fluctuated while discussing the scenarios and answering the questions about their attitude towards cybervetting. One of the respondents even mentioned that he would be glad to talk for longer time because he has noticed that his opinion is not consistent.

The category of people who do not have a determined positive, negative or neutral attitude can be characterized by the fact that they can name positive and negative traits of cybervetting and they can also understand the perspective of both sides, employers and job candidates. What distinguishes them from the group of people who have a neutral attitude is that they do not try to adjust to the practice and accept it as it is, but they actually want to get more knowledgeable about the phenomenon and have a certain opinion about how to further manage their online space. In connection to it an interesting observation was made during the recruitment process. As long as the respondents contacted me via social networks, I had and opportunity to see their public profiles, and out of the whole sample those three people were the ones who appeared to have the least information available about them on the internet on the websites – Vkontakte or Facebook, – they did not have a profile picture, and Lenya and Irina did not have any description on their pages. They have explained that in terms of them not being sure about what is better when the employers are cybervetting – being too informative or not informative at all. In case of being informative, as was mentioned, it is possible to publish something that can be understood ambiguously by the employer; there is always a possibility to post too much. However, there was another opinion, also shared by those respondents.

> Well, the fact that I have no details and nice profiles is a minus. Because now the employers can really evaluate the person with the help of social nets, and if a person has an empty profile that can usually mean that a person is a freak or something like that. Lack of information is always kind of scary. And if you don't see anything on the profile, it may cause uncertainty about the candidate. And, well, I see a problem in that. I think that it can be a bad thing for my job application procedure. Lenya, 22, unemployed.

This quote shows that the respondents who are ‘undecided’ tend to analyze the impact of an image that they create in social networks on the potential employer. However, even understanding the risks of being misjudged does not make those three participants change their strategy, at least, as they say, until the employer is going to reject them based on the lack of information that they provide.

An interesting finding to include in this section is that there is tendency between all the respondents that they are mostly looking for information or checking the profiles of other users rather than posting information themselves. It cannot be observed from direct quotes, but after talking with participants and further handling the transcripts, I discovered that those patterns are visible. As the respondents note, since they became more aware of the peculiarities of information storage on the internet, about digital footprint or cybervetting, they became more

cautious about what the post online and prefer to share information over private messages rather then posting it publicly.

Another reason for posting less was expressed by Lena, when she was talking about Vkontakte: “No Likes! People really reacted to what you were posting”. The respondent refers to the fact that in 2010 ‘likes’ were introduced in Vkontakte as a form of appreciation of content. After that the amount of comments to pictures and posts decreased, as long as it was easier to put a ‘heart’ under a picture rather then write a whole sentence or a shorter comment. Those comments, as Lena also noted, were meaningful, and showed what people really thought about the content that was posted. ‘Likes’ in her opinion are more artificial and not always sincere, which is why, as it was mentioned before, it seems better to send information directly to people who will be interested in it and appreciate it.

Now, after making this remark, I am returning to the viewpoint of people, who are ‘undecided’ about their attitude towards cybervetting. On the one hand, they see that cybervetting can be useful and can provide employers with additional information about the candidates. On the other hand, participants who could not decide how they actually see cybervetting, brought up the topic of discrimination in a sense that cybervetting is only a good thing if everyone has social networks and provides the same type of information, which is impossible. That is why people who are not registered in social networks or those who, as Lenya, Anton Alexandrovich and Irina, do not have a lot information in their profile, will be treated with suspicion and maybe even discriminated in terms of not getting a job.

And the final note is that those respondents also believe that sooner or later most of the people will be doing the same thing – either deleting information about themselves or creating a desirable image, and then cybervetting will not give the anticipated results anymore. There will be no authentic information on social networks, but rather socially desirable profiles – at least those, which are not private, and it will not be possible to actually evaluate the candidates based on this kind of information.

4.6. Rules and regulations of cybervetting

Respondents have also had an opportunity to imagine themselves as policy makers and offer their rules or regulations to how the employers should use cybervetting, what exactly they can and cannot do. It was done in order to stimulate their thinking out of the box and broaden the understanding of their attitudes towards cybervetting, which is one of the sub-questions of the current study. It was expected that while offering rules and regulations the respondents would unconsciously point out to the features that they do not like about cybervetting, even though

overall attitude in general is quite neutral. Those responses also helped discovering whether there are any expectations, expressed by participants towards the employers.

Based on the research by Ghoshray (2013a) it was suggested that job seekers may be in favor of employers being explicit to candidates about cybervetting. As in this work, none of the respondents mentioned it as a necessity, so, if they would be creating a set of rules, they would not make it a mandatory requirement that an employer has to inform a job candidate about cybervetting. But most of the participants expressed an opinion that it would be good to know whether the information in social networks is being evaluated; not even in order to change something but just to be aware of the fact, which corresponds with the results of the research by Ghoshray (2013a).

> I think that they should inform. Well, as it's written everywhere – you're being recorded by the surveillance camera. I think that they should write something like this or at least give a sign. Then the person can decide for himself, if he wants to pay attention to it or he doesn't want to. Nataliya, 50, PR; currently unemployed.

As well as in the situation when communication online was compared with communication and interpersonal relations offline, here online behavior is compared with offline situation with cameras. The main reason for it was not that the participants believe that cybervetting is a privacy violation, but rather that the company, which informs about such a practice, is more trustworthy and may later treat employees better than companies that do not inform about performing cybervetting. Such an idea has not been expressed in other studies. However, a research by Berkelaar (2014) describes a viewpoint that using a practice of cybervetting may be a sign that they job seekers will be treated badly at the workplace after being hired. It is not directly connected to the findings of current research, but the aspect of trustworthiness is overlapping, which gives me the opportunity to describe this case as a suitable example for comparison.

However, some of the respondents, including those who were positioned favorably towards cybervetting, expressed an opinion that cybervetting is an available tool for employers (as it was stated in the study by Ghoshray (2013b), so that is their right to inform about it or keep the information to themselves. It is much related to their understanding of privacy on the internet. Once social networks are understood as a public space, there cannot be distinction between people who are looking at social networks profiles in categories 'employers' and 'others'. While making a profile open to other people, participants make it available to their potential employers as well. But as it was already mentioned, hacking into job seekers' profiles or reading private messages is unacceptable in the viewpoint of the respondents. What was also

counted as a disagreeable practice is when the employer adds potential employee in the friend list in order to get more information about him/her. However, maintaining informal contacts in social networks after a person is already hired is a norm, according to the participants, and it is observed in all cases where the respondents already have a job.

A few other possible regulations emerged while analyzing the data along with concerns about using this practice. Those are interconnected, because there were a few parameters that were considered by the participants as suitable for online checking, but at the same time this kind of information may be not easily retrievable or not even available online. What is also important that half of the participants expressed uncertainty while answering a question about regulations. It was connected with the fact that it was not easy for them to understand how exactly the criteria for evaluation social media could be made and how to avoid the subjectivity. It was mentioned by Mikkelson (2010) as well, and as long as there are no standardized criteria and maybe even computer programs for evaluating social nets, the decisions made on their basis may still be biased by personal perception of people, as any other decisions in the offline world. However, as it was already mentioned, some possible aspects for evaluation were offered by the participants of the study.

The first thing that was mentioned is any kind of online activity that could be prosecuted – crime, pornography, child molestation, drugs or terrorism. If a person is involved in any of those activities or at least shows interest in them, it should be seriously considered by a potential employer. It can also be a sufficient ground for not hiring a person, which is an important thing to mention, because mostly cybervetting is treated by the informants as a additional criterion, rather than the key one.

> Mostly additional, but except for some cases like social sphere or law enforcement, I wanted to say that it's except for some extreme cases. Sergey, 41, financial analyst; currently unemployed.
>
> Well, so posting pornography or advertising some forbidden drugs through internet, that can, by law, influence the opinion of the employer towards rejecting the candidate. But some other things like pictures, smoking, some leisure activities, hobbies, etc, etc, I would forbid for it to have any influence on the decision. Alexandra, 23, stomatologist.

So, there is a noticeable distinction between activities that can influence the final decision about hiring or rejecting a candidate. Something that is prohibited by law but is promoted in social networks of a person may be considered a sufficient criterion while hiring him/her, while personal interests, hobbies or leisure activities must not influence the decision. Moreover, in any case the company policies play the main role. This topic was already touched upon before, while

describing the case of a respondent, who was trying to get the position in Red Bull, but the company's corporal ethics was contrary to her perception. At the same time, the company could also decide according to the profile in social networks that the candidate can be unsuitable because, for instance, his/her key values significantly differ from the company's principles.

> I don't know, that's a primitive example, you're applying to Coca-Cola, but it's written on your wall that Coca-Cola is shit and you drink only Pepsi (laughing) there may be problems. So you should be ready for that. Lena, 25, lecturer.

Promoting competing companies, as it is seen from the example, can also be a reason for not hiring a person for the position, because if other people are going to check social networks of an employee of the company and see that he/she is advertising competitive products, there may be serious questions towards the company, as it cannot discipline its own workers.

Another factor that can influence the process of decision-making is the sector, in which the job candidate is seeking an opportunity. There was a separate question in the interview guide in order to understand whether there are some particular professions that require more attention towards the information found by means of cybervetting. Also, the respondents mentioned different professions while making examples during the interviews.

> Depends on which sector this person is going to. Which position he wants to take. If it is a financial director or an accountant, I would be checking all the information, about his previous job places and social nets. A person is going to work with loans and finance. Something like that. I would be collecting all kinds of information, without any restrictions. Elena, 53, accountant; currently unemployed.

In the abovementioned situation the respondent imagines herself in the role of an employer and she sees the necessity of checking online information along with other resources because the person is going to work with valuable and confidential information, so it is possible to learn more about his personality from social networks in order to make a more informed choice. However, respondents were also offered an opportunity to think whether cybervetting could be a main or even separate criterion for hiring or rejecting a person when he/she is seeking a position that is connected with working with vulnerable populations, positions of power or publicity.

The professions that were mentioned by the respondents are quite uniform, however, the opinions about the possibility of cybervetting being the key criterion for hiring or rejecting from a position were strikingly different. The majority of respondents expressed an opinion that the information obtained by means of cybervetting can be evaluated along with other information, mentioned in CV, profiles in professional networks as HeadHunter or LinkedIn, motivational

letters, letters of recommendations and reviews from previous job places but it can almost never be a key criterion itself.

> No, I don't think that there are some professions where the profile evaluation can be the main factor. We're moving to some virtual reality, and we can remember again some people who want to present their other identity, but eventually they're not like that. So, it's important to communicate. It also happens that some employers are inviting the psychologists. And there are conversations with psychologists, who can tell, which kind of a person is an employee, tell about his stress-resistance, does he have it. Some criteria can be only evaluated by a specialist. Sveta, 24, unemployed.

The respondent mentions a term 'virtual reality', and she refers it to the fact that people start paying too much attention to the information on the internet in general and in social networks in particular, underestimating the value of live communication in the offline world. As long as cybervetting is a phenomenon that takes place online, in this 'virtual reality', it should be treated accordingly – with attention, but without attaching great levels of importance to it. So, even though cybervetting, in general, is perceived by the respondents as an acceptable practice, some of the them expressed an opinion that there are other criteria that cybervetting cannot replace.

During the interviews the respondents named the positions that required additional attention to the information discovered with the help of cybervetting. Those are: teachers, people who work on internet (e.g. with social media marketing, PR or copyright), security services, doctors, people working in financial industry (e.g. banking). One of the respondents brought up a case that has recently been discussed on television.

> Teachers, in general… Well, if I was a teacher, I would think about it, because there was recently a scandal that the teacher was working in the evenings as a woman… briefly, prostitute. There were… There was the whole show about it, someone was saying that it's her own thing and her own time, while someone was saying that they don't want such a person to work with their children. Elena, 53, accountant; currently unemployed.

The implication of this case to analysis is quite clear, as it touches upon things that were previously discussed in the literature and analysis. The main problem is the distinction between private life of a person, off-duty time (Cohen & Cohen, 2007; Hunt & Bell, 2014), and public life or also time on duty. So, in the opinion of the respondent, the case described was quite extreme, as it demonstrated imbalance between the actual profession of a person and other occupation that she had. Similar cases were mentioned in two more interviews, and based on the

answers of the respondents, the right actions to undertake in those situations would be not letting personal information like that get on the internet in the first place.

So, the criterion that could be evaluated could be called as 'appropriateness'. While pre-screening people that apply for professions connected with working with people, like doctors or teachers, as in the example, it is necessary to pay attention to the appropriateness of information, contained in their social networks. If it is inappropriate, the decisions that can be made about the candidates, offered by the interviewees, were the following: reject a person, give a person an opportunity to explain his/her behavior and offer a probation period. Another option was offered by one of the respondents, when she was talking about hiring a secretary.

> So if I had some ideal picture of a person [for a certain position], I could go and see his social network profile and correct my expectations about him, his intellectual abilities, what he lives for. . . . So to say, if I ask him to bring me a cup of coffee, he will be able to do that despite the fact that he likes or reposted something in social nets. Katerina, 36, consultancy and marketing.

The positions of executive workers, in the opinion of the respondent, do not require as much attention to social networks as the abovementioned professions. In this case cybervetting may be a tool, which helps a person to get some information in order to correct or lower his/her expectations about a future employee.

Another criterion, according to the respondents, is connected with professions in the area of finance or security and it can be named 'trustworthiness'. Though, it is not clear to the respondents who mentioned those professions, which kind of information can be checked in order to see whether a person can handle confidential information or is trustworthy. Nonetheless, at least a general image in social networks, as the respondents mentioned, can tell a lot about a person and be useful in predicting some of his personal characteristics.

The last criterion that was discovered during the interviews and can be evaluated in social networks of every person, applying to any position, is 'literacy'. When people post some textual information on social networks, they may show how literate they are by spelling words correctly and using punctuation marks. It can tell about the overall level of intelligence, but also can be really informative for certain professions.

> Well, for instance, our company needs beautiful and quality presentations to sell our goods, and then we see some strange posts and a lot of mistakes, we won't hire him/her. I also think… I got this idea that it's possible to check social nets in terms to check literacy. For instance, when I see the pages… not completely illiterate, but with some

commas in wrong places, I'm so mad at it. So maybe, if I was an employer, I wouldn't have hired such a person. Evgeny, 22, marketing assistant.

The most important point that the respondent makes is that this kind of information can only be given away in the social networks, where potential candidates feel freer in expressing themselves and do not initially have the aim to impress the employer, as they do in their CVs, letters of motivations or during the interviews.

4.7. Actions, undertaken as a response to potential possibility of being cybervetted

As it was mentioned in the introductory part of the analysis, it is not possible to talk about effects of some parameters on others based on the data of 14 in-depth interviews. However, the observed patterns offer that on this particular sample awareness of cybervetting, personal experience with this practice, perception of privacy, understanding of digital footprint and, accordingly, attitude towards cybervetting play an important role in influencing the strategies of managing online space that are taken by interviewees. As long as the majority of the respondents were aware about the practice and mentioned that they manage their online space taking into consideration the possibility about being cybervetted, it is possible to suggest that the strategies of managing online space that were discovered are at least partially explained by the observed phenomena.

Throughout the interviews a lot of questions were asked in order to be able to construct strategies of managing online space. Some of them were aimed at finding out whether respondents deleted information from social networks and which kind of information they deleted; other questions were more general, but the responses contained the data for summarizing. Hence, two following strategies of managing social networks emerged during the interviews: preventive strategy and an 'ex-post' strategy. Those partly incorporate the strategies mentioned in the literature review – presenting oneself closely to reality, presenting one's 'best self' and deceptive presentation (including anonymity and pseudonymity). What is more, evaluation of employers in social networks was mentioned as a response to the practice by two of the respondents. However, every strategy and action will be described in more details.

4.7.1. Preventive strategy

The actions, undertaken by the majority of the respondents in their online space can be described as a preventive strategy. It is characterized by the initial awareness of cybervetting and, thereby, being attentive to the type of information that is posted on the internet in the first place. Every decision made by respondents, who are using a preventive strategy, is also influenced by their awareness about digital footprint, which is one of the reasons for being

careful about posting online. A deeper understanding of the nature of digital footprint led to the following answer from one of the respondents: “So: don’t like, don’t post and don’t repost. And this creates my image, because I understand really well that the profile is not only what I wrote, but also what I liked” (Katerina, 36, consultancy and marketing).

Katerina and Lena are the only ones from the sample who take this side of digital footprint into account, while others focus on the information that they posted purposefully. Still, it is possible to suppose that such a measure of control – not liking or clicking on something compromising that can be lately discovered by an employer – is also taken by the interviewees using preventive strategy.

> Another opinion on the current situation also explains the actions taken online:
>
> Well, I don't really know, it's more like my personal position, in our world, when people are being watched by all kinds of GPS trackers, even Windows now… Every Windows user has his own identification number that is tracking all the actions. It’s almost impossible to switch off. So publicly posting your own information is like giving out all your private life outside… that's a bit too much, I think. Lenya, 22, unemployed.

Even though the respondent does not mention cybervetting explicitly, this remark was made in relation to it. It is one of the other factors that can influence behavior online. And while Katerina and other respondents tend to use the strategy aimed at creating a realistic or ideal image by means of preventive actions, Lenya used preventive technique in order to follow a deceptive strategy of anonymity.

4.7.2. ‘Ex-post’ strategy

‘Ex-post’ in this case stands for posting information online and after some time deleting it. The reasons for deleting information varied from case to case; for instance, some things were considered by the respondents as inappropriate, overly personal or unsuitable, which is why they deleted it. Most of the respondents were using the ex-post strategy along with the preventive strategy. In this case the initial idea was still to post the information accurately, but eventually, after consideration, deleting some of it due to reasons of desirability. Ex-post strategy could also be used on its own, and it was used by three respondents out of fourteen. This means that initially the respondents did not pursue the goal of creating an image online that would put them in a good light, but after getting knowledge about the possibility of being cybervetted (Nataliya, 50, PR; currently unemployed), after ‘getting older, with coming experience’ (Evgeny, 22, marketing assistant) or due to other reasons, they decided to ‘clean’ their online space and delete information that they found unsuitable – like aggressive pictures, comments with coarse

language (Lena, 25, lecturer) or posts that they did not agree with anymore (Sveta, 24, unemployed).

There were other cases, which show that in general there may be a variety of other reasons for deleting information. One of the respondents mentioned that she deleted the whole album as no one was interested in it anymore – the community of people who were on the pictures started to fall apart, which is why the photos lost their relevance (Sveta, 24, unemployed). Another respondent mentioned that he deleted the pictures that collected the least amount of likes, because they "… spoiled an overall picture" (Evgeny, 22, marketing assistant). This respondent was the one trying to create an image of a popular person, who other people care about. That is why, when he got less 'likes' than expected, it could be interpreted as little attention to his persona, and could be negatively perceived by his followers. Even though those cases are quite different, in both of them deleting pictures relates to other people being indifferent to information posted.

Other situations, when deleting information was explained directly by the possibility of being cybervetted, was also observed in the sample. In this case the interviewees mentioned that once they heard about the phenomenon or faced it themselves, they started thinking about the information contained online, its appropriateness in terms of job seeking.

Another interesting observation was also made in connection with digital footprint. One of the respondents said that she would like to delete some things from the internet, but it did not really seem possible – she was talking about comments to posts in social networks, which could be retrieved by the employer at least by an accident, but are not easily found by her. Basically, those comments were not her main activity online and she did not pay too much attention to it while posting, but eventually this information can negatively affect her.

The 'ex-post' strategy was also named by a number of respondents as a possible response to being rejected from a position. In this case they found it reasonable to listen to the opinion of employer, and if it is constructive enough – it was considered possible to change online information and possibly delete something in order to get a better fit for future positions.

4.7.3. Evaluation of employers

Another point was made in three interviews, which was that job seekers also use the practice of screening in order to get more information about the future employers. In relation to the definition of cybervetting, it turns to be a kind of reversed practice. However, it can be better described as a response to cybervetting as a practice rather than actions of managing online space from the side of job seekers. This point was touched upon while the respondents were talking about the possible aims of cybervetting usage by employers. A question, addressing this

issue, was not included in the guide; however, the respondents touched upon the topic themselves. As it was studied in the previous research on cybervetting, there are a few aims that the employers follow while cybervetting. Cybervetting was called useful (as informative) and available, and also it was described as a method that can be used for 'fun' (Ghoshray, 2013b) Those aims were also mentioned by the respondents at some point as possible measures while checking employers' social networks. However, there was another goal that was named by one of the respondents. It is closely connected with being informative, but it is aimed at a different thing then evaluating a fit of a job candidate. Getting information about future employers may help during the interview in order to better maintain the conversation, as it is possible to know about the interests of a person as well as about something that he/she does not like, or instance. So, the example is given in order to show that practice of cybervetting can also used by the respondents, for instance as an inspiration for the upcoming interview. Another reason why people do that was also described in the literature, and it is mainly because the one-sidedness of information (when only the employer can check online information of the employees) is negatively perceived by job seekers.

5. Conclusion and Discussion

The research detailed above set out to address a relatively new phenomenon, incorporating social media use into job employment procedures – cybervetting. Moreover, the subject was studied in an earlier unexplored setting of Russian society. The fact that there are still no studies about cybervetting in Russia does not mean that the practice is not used in the country. A lot of information about it is contained on different websites and forums dedicated to the topics, connected with job search (see Murakhovsky, 2014; Prokofieva, 2009; Umarov, 2010; "Social Networks and Job Search", 2015), which is why it is possible to say that the issue is urgent but still has not resonated in the academic debates.

The reason why this topic was chosen in a first place is that nowadays the phenomenon clearly becomes used ubiquitously, but there is still not enough attention paid to it in the academic field. Issues such as privacy violation, employers' perspective on cybervetting, their risks, connected with using this practice, and also self-presentation online have been previously addressed by researchers, but the job seekers' perspective on using this practice still remains quite understudied. For this reason one of the main aims of this research paper was to reveal the attitudes that the job seekers express towards this phenomenon. However, a profound scrutiny of existing literature and other information about this phenomenon helped to identify more gaps that could be fulfilled by the current study.

As it was previously mentioned, the authors rarely address the topic of job seekers' perception of cybervetting. A lot of works were written about privacy and its relation to the phenomenon (Yanisky-Ravid, 2014; Ghoshray, 2013a; Craver, 2006; Hunt & Bell, 2014; Kovach et al., 2000; Mitrou & Karyda, 2006), however, the question of how exactly job seekers see this practice is obviously understudied. Even though there are research works, addressing this issue (Stoughton, Thompson & Meade, 2013; Berkelaar, 2014), they do not cover the whole scope of possibilities to study people's attitudes and reactions. The first aspect that could be improved is the age range of participants of the study. In the existing papers young job seekers (below approximately 30 years old) were studied, while the opinions of older job seekers were not taken into consideration. The pension age in Russia allows the assumption that a significant category of people is left out in this case. The second important aspect is that the actions, undertaken by the job seekers once they know about the possibility of being cybervetted are also not directly described in the existing research.

Summarizing all the abovementioned points it was decided to study the practices that emerge as a response to potential possibility of being cybervetted, and as long as in the previous research the age groups were not diverse, it was also decided to compare the age groups within

the sample in order to see whether the practices differ in younger (18-35) and older (36+) age groups. The main justification for such age division is an article by Jones & Shao (2011), who introduce concepts of digital natives and immigrants, who perceive internet and technologies differently, which may result in different reactions to cybervetting. The main research question was formulated, based on the previous findings and gaps in the literature: How do practices of managing social media differ among younger and older Russian job seekers once they are aware of a possibility of being cybervetted? However, this question could not be answered directly without studying some underlying patterns that may explain the differences or similarities of actions between age groups. That is why other issues were addressed in sub-questions before proceeding to final conclusions.

In the beginning of the analytical part a scheme, showing the relations between the concepts, was demonstrated. It showed that framing of cybervetting is formed by knowledge about this phenomenon, personal experience with it and overall tendencies of internet and social networks use. Investigating the latter aspect showed that, in general, the difference lay in the year when the respondents first started using social networks. The elder group of participants started using internet on average in 2000, while the younger group – in 2005, because they were too young to start using the computer before that. There was, however, one 'outlier' – a 22-year old respondent who also started using internet around 1998-1999 year "…under the guidance of [his] parents" (Lenya, 22, unemployed). Those dates are important to consider, because they demonstrate that two age groups were witnessing changes of the internet in different time periods and went through different stages. For instance, elder respondents started using internet while there were no social networks in the current understanding – there were blogs, forums or messengers at this point. Younger respondents joined internet when new social platforms started being developed (Facebook in 2004, Russian analogue – Vkontakte – in 2006). And despite the fact that respondents from both age groups had an opportunity to choose between available social platforms, eventually all of them concentrated on the same ones: such platforms as Vkontakte, Facebook and Instagram dominate in the sample overall. A small trend that was also discovered and suggested by the respondents is that another platform, launched a little earlier than Vkontakte – Odnoklassniki – is traditionally more used by elder people. Odnoklassniki is translated as 'classmates', and was initially created in order for older generation to be able to get in touch with their classmates or group mates, who they lost the connection with after school and university years. Younger participants prefered Vkontakte and Instagram, because they were not yet in the age to restore lost connections, and the main goal that all the participants of the study mention was using those social networks for communication.

As long as it was obvious after primary investigation that people in the sample were quite familiar with using both, internet and social networks, the question about knowledge and experience with cybervetting was risen. Most of the respondents were aware of the practice from different sources – mostly internet and other media, or discussions with friends and colleagues. However, only three respondents out of all the participants actually faced the practice in the real life, which caused negative emotions at first. Still, as long as those encounters happened a few years ago, overall attitude towards the phenomenon was not negative after all, which can be explained by the approach by Katz, Levin and Hamilton (1963) about the diffusion of innovation. The authors believe that with time acceptance of new phenomena occurs and less negativity is expressed towards something that was negatively perceived in the beginning. This may also substantiate the differences between the results of this research and previous papers on the topic.

So, summarizing the information about how the participants of the study frame cybervetting, it is possible to say that they are quite literate about the phenomenon, which is why they understand it as a developing practice of informing personnel selection. However, in their opinion, it is still is not completely comparable with other traditional techniques of evaluating fit for the position – checking CV, motivational letters or letters of recommendation. Cybervetting can be seen as an additional criterion for evaluation, but can rarely be a key one.

Still, the way in which they frame it did not explain their attitude towards the phenomenon. That is why it was necessary to look more in-depth at privacy issues in connection with cybervetting and, consequently, the Russian context that might have had its influence on how people perceive privacy. It was discovered that, in general, all the participants conceptualize privacy offline and online in quite a similar way. In the offline world privacy is understood according to the definition by Brandeis and Warren (1890) as a right to be alone, but in the online space privacy was understood in two different ways. It was seen by the respondents as something exclusively personal and something that can be shared with a particular circle of people, for instance, via instant messaging. However, mostly social media are a public space in the opinion of the respondents, and any personal information, once published online, becomes a public domain.

There is an important finding in terms of age differences in the attitudes towards privacy. All the respondents mentioned FSS at a certain point in their interviews as an organisation that has an unspoken authority to check any kind of information in social networks of people. However, the participants of the elder generation, who lived closer in the time continuum to the periods of Soviet espionage and strict rules of job employment, were a little less critically

positioned to the practice as they got more used to sort of privacy violation in their lives. But overall trend was that there was no openly negative attitude expressed towards cybervetting in the sample. It was explained by the fact that, in the understanding of the respondents, concepts of privacy and cybervetting do not really overlap. The information in social networks, excluding private messages, is considered a public space, available to other people, including employers. This substantiates the value of theories by Treem and Leonardi (2012), who stated that information is social networks is public, and by Walther (2011), who mentioned that CMC leaves small space for privacy in general. That is why the practice of cybervetting as checking online information of the candidates cannot be seen as a privacy violation, hence cannot evoke negative attitude.

Though, the attitudes to the phenomenon that were discovered were positive, neutral and undecided. The first group of people considered cybervetting a practice that can actually inform the personnel selection better, and social networks may help people even stand out of the crowd, while they are aware that they might be cybervetted. Those people also have not expressed any negativity when they were offered a scenario about being rejected from a position because of cybervetting, because they saw it as an opportunity to correct their online information for further positions. This group consisted of three participants, and they were from both age groups, which is why it is not possible to make any conclusions about age differences, especially due to the fact that the sample overall is quite small. Neutral attitude towards cybervetting was expressed by most of the respondents (eight out of fourteen), and it may also be seen as acceptance of the phenomenon, in terms of diffusion on of innovation. 'Undecided' position was also discovered, as long as three respondents could not figure out their attitude towards the phenomenon. Different sources of information made them change their mind and made them want to become more knowledgeable about it in order to further manage their online space.

An interesting observation was also made in terms of attitudes, expressed by the group of respondents with 'undecided' opinion. They have raised the question of discrimination by means of cybervetting in a sense that the practice may adversely affect people who are not registered in social networks or who do not provide a lot of information about themselves, because that may seem suspicious to the employer. So, even though the participants see the advantages of cybervetting, they also clearly see potential problems, which do not allow them to form an unambiguous attitude.

The last point that was addressed in the study was discovering the practices and actions that are undertaken once the respondents are aware of the possibility of being cybervetted. Those actions presented themselves in two main strategies – preventive and 'ex-post'. Preventive

strategy was used by most of the respondents, meaning that their initial awareness of potential pre-screening made them think carefully about what they post online in order not to get any problems in the future. 'Ex-post' strategy was used mostly in combination with the preventive one, however, it was also used separately by three respondents. 'Ex-post' in this case means that initially the respondents did not pay much attention to what was being posted, but then, once they saw it as inappropriate, aggressive, or did not agree with it anymore, they deleted it. So, when preventive and 'ex-post' strategies were combined, people mostly thought about what they were posting in the first place, but later refined their profiles even more by means of deleting some information. Another way of reacting to being cybervetted that was also noticed, but is not really a strategy, is evaluating employers by the candidates. It is mainly done in order to get some topics to discuss during the interview or, as it was mentioned in the previous literature on the topic (Ghoshray, 2013a), because one-sidedness of information (when only employers can get additional information on the employees) is not really appreciated by the job candidates.

By means of getting those separate conclusions and merging them together it was possible to answer the main research question. As long as it considered the differences between age groups in terms of their practices, which emerge as a response to cybervetting, it is quite noticeable that the age issues are rarely mentioned in the analysis. It may seem as an oversight of a researcher, however, apart from the age differences mentioned in terms of internet use there were no other patterns discovered. Despite the fact that participants of the study started using the internet and social networks at a different point of time, they still got knowledgeable about cybervetting at approximately the same time period, and their attitudes and actions did not really differ across age or gender (as it was mentioned in the sampling section, equal amount of men and women participated in order to enrich the data by varying opinions).

In a nutshell, current research deepens the understanding of job seekers' perspective on cybervetting, fulfilling the gap in the existing academic literature. It describes and explains the attitudes of job seekers towards a phenomenon of cybervetting in a previously unstudied Russian setting and covers a new aspect – actions, undertaken as a response to cybervetting. Those results were obtained by means of conducting in-depth semi-structured interviews, which are the most suitable tool for collecting relevant data about attitudes and practices of the respondents. What is more, employed scenarios of job-seeking procedures and stimulating creative thinking by means of offering respondents to come up with possible rules and regulations for using cybervetting demonstrated its efficiency. Even in the cases in which the respondents did not mention their attitudes explicitly, it was possible to formulate their opinions based on the

reactions that were observed during the scenarios. Moreover, while offering regulations to the practice they were implicitly indicating the aspects that they did not like about cybervetting.

However, there are certain limitations to the results obtained. The first is that the explored younger group is a bit too homogenous (with the younger age 22 and the older – 25), while the studied age gap was 18-35 years old. That is mainly explained by the fact that people who contacted me for participating in the research were distant acquaintances of my friends, who are more or less the same age. However, it is not an issue in the elder group, where the younger age is 36 and the oldest – 58, which is almost a pension age. The second limitation, to some extent, is the research qualitative design itself that does not provide opportunities for generalization. This also offers further directions for the research on the topic. In order to better understand the job seekers' attitudes towards cybervetting and practices emerged as a response to it on a bigger scale, I find quantitative methods suitable for generalizing the ideas, expressed in the current exploratory study. By means of conducting a survey and further data analysis it can be possible to see whether a negative attitude towards the phenomenon can be actually observed, which is suggested by the previous literature on the topic. Moreover, age differences that did not present themselves in the current sample might be visible on a bigger sample of a quantitative study.

Finally, the next logical step in the subsequent research on the topic could be comparing the attitudes and practices connected with cybervetting in the Russian reality and in a foreign one. The comparison should be based on historical and cultural background as well as discovered in this research practices. I, as a researcher, believe that in a similar vein to this study, other scholars could help broadening the understanding of the studied phenomenon through the lens of job candidates, as well as uncover other attitudes and practices that they may express and form.

References

Agre, P. E., & Rotenberg, M. (1998). *Technology and privacy: the new landscape*. San Diego: Mit Press.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey: Brooks/Cole Publishing Company.

Aronson, J. (1995). A pragmatic view of thematic analysis. *The Qualitative Report, 2*(1), 1-3. Retrieved from http://nsuworks.nova.edu/tqr/vol2/iss1/3

Arthur, C. (2012). Employers warned against demanding Facebook details from staff [Article]. Retrieved from https://www.theguardian.com/technology/2012/mar/26/employers-warned-facebook-login-details

Austin, L. (2003). Privacy and the question of technology. *Law and Philosophy*, *22*(2), 119-166.

Babbie, E. (2008). *The Basics of Social Research* (fourth edition). Belmont: Thomson Higher Education.

Bedareva, O. (2014). Social'nye seti mogut pogubit' vashu kar'eru [Social networks can destroy your career; Article]. Retrieved from http://www.e-xecutive.ru/career/labormarket/1922022-sotsialnye-seti-mogut-pogubit-vashu-kareru

Bennett, C. H., Brassard, G., Crépeau, C., & Maurer, U. M. (1995). Generalized privacy amplification. *Information Theory, IEEE Transactions on*, *41*(6), 1915-1923.

Berkelaar, B. L. (2014). Cybervetting, online information, and personnel selection new transparency expectations and the emergence of a digital social contract. *Management Communication Quarterly*, *28*(4), 779-506. http://doi.org/10.1177/0893318912439474

Berkelaar, B. L., & Buzzanell, P. M. (2014). Cybervetting, person-environment fit, and personnel selection: Employers' surveillance and sensemaking of job applicants' online information. *Journal of Applied Communication Research*, *42*(4), 456-476. http://doi.org/10.1177/0893318912439474

Boeije, H. (2010). *Analysis in qualitative research*. London: Sage.

Boyce, C., & Neale, P. (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input* (pp. 3-7). Watertown, MA: Pathfinder International.

Brandeis, L., & Warren, S. (2014). *The right to privacy*. Roden: RL Van Bruggen.

Cohen, C. F., & Cohen, M. E. (2007). On-duty and off-duty: Employee right to privacy and employer's right to control in the private sector. *Employee Responsibilities and Rights Journal*, *19*(4), 235-246. http://doi.org/10.1007/s10672-007-9050-2

Cranor, L. F. (1999). Internet privacy. *Communications of the ACM*, *42*(2), 28-38.

Craver, C. B. (2006). Privacy issues affecting employers, employees, and labor organizations. *Louisiana Law Review*, *66*(4), 1057-1078.

Crocker, D. (n.d.) Email history [Article]. Retrieved from http://www.livinginternet.com/e/ei.htm

DeAndrea, D. C., & Walther, J. B. (2011). Attributions for inconsistencies between online and offline self-presentations. *Communication Research*. http://doi.org/10.1177/0093650210385340

Depressed woman loses benefits over Facebook photos [News article]. (2009, November). Retrieved from http://www.cbc.ca/news/canada/montreal/depressed-woman-loses-benefits-over-facebook-photos-1.861843

DiCicco Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, *40*(4), 314-321.

Dunning, T. (2008). Improving causal inference: Strengths and limitations of natural experiments. *Political Research Quarterly*, *61*(2), 282–293.

Erving, G. (1959). *The presentation of self in everyday life*. Garden City, NY: Anchor.

Fichman, R. G., & Kemerer, C. F. (1999). The illusory diffusion of innovation: An examination of assimilation gaps. *Information Systems Research*, *10*(3), 255-275. http://doi.org/10.1287/isre.10.3.255

Finder, A. (2006). When a risqué online persona undermines a chance for a job. *New York Times*, *2*.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153-160. http://doi.org/10.1016/j.chb.2008.08.006

Fotografii v social'nyh setyah budut povodom dlya otkaza v kredite [Pictures in social networks will be the reason to reject a loan request; News article]. (2016, February). Retrieved from http://ren.tv/novosti/2016-02-29/fotografii-v-socialnyh-setyah-budut-povodom-dlya-otkaza-v-kredite

Galachieva, I. (2012) Elektronnaya perepiska kak dokazatel'stvo v grazhdanskom processe [Electronic correspondence as evidence in Civil Court; Blog post]. Retrieved from https://zakon.ru/blog/2012/1/18/elektronnaya_perepiska_kak_dokazatelstvo_v_grazhdanskom_processe

Ghoshray, S. (2013a). Employer surveillance versus employee privacy: The new reality of social media and workplace privacy. *Northern Kentucky Law Review*, *40*, 593-626.

Ghoshray, S. (2013b) The emerging reality of social media: Erosion of individual privacy through cyber-vetting and law's inability to catch up. *The John Marshall Review of Intellectual Property Law, 12,* 551-582.

Gosling, S. D., Augustine, A. A., Vazire, S., Holtzman, N., & Gaddis, S. (2011). Manifestations of personality in online social networks: Self-reported Facebook-related behaviors and observable profile information. *Cyberpsychology, Behavior, and Social Networking*, *14*(9), 483-488. http://doi.org/10.1089/cyber.2010.0087

Gould, E., & Belyakova, M. (2013) Social'nye seti kak instrument izucheniya psihologicheskogo portreta potrebitelya [Social networks as a tool of studying psychological portrait of a consumer; News article]. Retrieved from http://www.therunet.com/experts/926-sotsialnye-seti-kak-instrument-izucheniya-psihologicheskogo-portreta-potrebitelya

Grant, A., & Lewis. A. (2014) When is it OK for employers to monitor an employee's social media profiles? *Employers' Law, 14*(10), 17.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80). ACM.

Guscheva, N. M., Vatolina, E. A., Zelmanovich, G. V., Lukashina S. Y., Krylova M. D. (2013) *Internet v Rossii: Sostoyanie, tendencii i perspectivy razvitiya [Internet in Russia: State, tendencies and development perspectives]*. Moscow: Federal agency of printing and mass communications.

Hall, J. A., Pennington, N., & Lueders, A. (2013). Impression management and formation on Facebook: A lens model approach. *New Media & Society, 0*(0), 1-25. http://doi.org/10. 1177/1461444813495166

Hayes, B. L., & Cooley, S. J. (2013). Social media – striking the balance between employer interests and employee rights. *The Computer & Internet Lawyer, 30*(7), 1-6.

Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society*, 1-10.

Hughes, B. L., & Beer, J. S. (2013). Protecting the self: The effect of social-evaluative threat on neural representations of self. *Journal of Cognitive Neuroscience*, *25*(4), 613-622. http://doi.org/10.1162/jocn_a_00343

Hunt, C., & Bell, C. (2014). Employer monitoring of employee online activities outside the workplace: Not taking privacy seriously. *Canadian Lab. & Emp. LJ*, *18*, 411-458.

Infographic: Facebook VS the Stasi in numbers [Blog post: statistics]. (2014, July). Retrieved from http://charlieharvey.org.uk/page/facebook_vs_the_stasi

Internet users by country [Statistics]. (2016). Retrieved from http://www.internetlivestats.com/internet-users-by-country/

Joffe, H., & Yardley, L. (2004). Content and thematic analysis. In D. Marks & L. Yardley (Eds.), *Research methods for clinical and health psychology* (pp. 56-68). California: Sage.

John, L. (2015, October). My trebuem privatnosti v internete, no nashi deistviya govoryat ob obratnom [We require privacy on the internet, but our actions speak against it; News article]. Retrieved from http://hbr-russia.ru/biznes-i-obshchestvo/fenomeny/p16629/#ixzz49nbUB7ZZ

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. *The Oxford handbook of Internet psychology*, *4*(7), 235-250.

Jones, C., & Shao, B. (2011). The net generation and digital natives: Implications for higher education. York: Higher Education Academy. Retrieved from http://oro.open.ac.uk/30014/1/Jones

Jourard, S. M., & Lasakow, P. (1958). Some factors in self-disclosure. *The Journal of Abnormal and Social Psychology*, *56*(1), 91-98. http://doi.org/10.1037/h0043357

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59-68. http://doi.org/10.1016/j.bushor.2009.09.003

Katanova, L. (2009, May). Poisk, otbor i priem personala [Search, selection and hiring personnel, Article]. Retrieved from http://scholar.googleusercontent.com/scholar?q=cache:YbAVXrxzszUJ:scholar.google.com/+%D0%BA%D0%B0%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%B0+%D0%BF%D0%BE%D0%B8%D1%81%D0%BA+%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D0%B0&hl=en&as_sdt=0,5

Katz, E., Levin, M. L., & Hamilton, H. (1963). Traditions of research on the diffusion of innovation. *American Sociological Association*, *28*(2), 237–252.

Kluemper, D. H. (2013). Social network screening: Pitfalls, possibilities, and parallels in employment selection. *Advanced series in management*, *12*, 1-26.

Kovach, D., Kenneth, A., Jordan, J., Tansey, K., & Framiñan, E. (2000). The balance between employee privacy and employer interests. *Business and Society Review*, *105*(2), 289-298. http://doi.org/10.1111/0045-3609.00082

Legard, R., Keegan, J., & Ward, K. (2003). In-depth interviews. In J. Ritcher & J. Lewis (Eds.), *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (pp. 138-169). London: Sage.

Levinson, M. (2011, April). Social networks: New hotbed for hiring discrimination claims [Article]. Retrieved from http://www.computerworld.com/article/2507674/it-careers/social-networks--new-hotbed-for-hiring-discrimination-claims.html

Madden, M. (2007). *Digital Footprints: Online identity management and search in the age of transparency*. Washington, DC: Pew Internet & American Life Project.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355. http://doi.org/10.1287/isre.l040.0032

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer−Mediated Communication*, *9*(4). http://doi.org/10.1111/j.1083-6101.2004.tb00292.x.

Mikkelson, K. (2010). Cybervetting and Monitoring Employees' Online Activities: Assessing the Legal Risks for Employers. *Pub. Law*, *18*, 3-7.

Mitrou, L., & Karyda, M. (2006). Employees' privacy vs. employers' security: Can they be balanced? *Telematics and Informatics*, *23*(3), 164-178. http://doi.org/10.1016/j.tele.2005.07.003

Murakhovsky, A. (2014, October) 7 veschei, na kotorye rabotodatel' smotrit v resume [7 Things That an Employer Pays Attention to in Your CV; Blog post]. Retrieved from http://lifehacker.ru/2014/10/07/7-veshhej-na-kotorye-rabotodatel-smotrit-v-rezyume/

Murphy, D. E. (1999). KGB and MfS: Friendly enemies. *Intelligence and National Security*, *14*(3), 228-234. http://dx.doi.org/10.1080/02684529908432561

Nederhof, A. (1985) Methods of coping with social desirability bias. *European Journal of Social Psychology*, 15, 263-280.

Neuman, W. L. (2005). *Social research methods: Quantitative and qualitative approaches*. Boston, MA: Allyn and bacon.

O'Reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & Strategies*, *65*(1), 17-37.

O'Reilly, T., & Battelle, J. (2009). Web Squared : Web 2 . 0 Five Years On. *Proc of the 6th Annual Web*, *20*(1), 1–15. http://doi.org/10.1007/s00436-009-1524-8

Parker, R. B. (1973). Definition of privacy. In J. R. Potuto (Eds.), *Rutgers Law Review, 27* (pp.275-298). New Jersey: Rutgers University.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. US: SAGE Publications.

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Petrov, N., & Edelman, O. (2002). “Shpionazh” i “nasil’stvennaya smert” [“Espionage” and “violent death”]. *Logos, 4*(2), 33-46.

Ployhart, R. E., Ryan, A. M., & Bennett, M. (1999). Explanations for selection decisions: Applicants’ reactions to informational and sensitivity features of explanations. *Journal of Applied Psychology*, *84*(1), 87-106.

Prokofieva, E. (2009, November) Kak iskat’ rabotu cherez social’nye seti [How to look for a job through social networks; Blog post]. Retrieved from http://egraduate.ru/%D0%BF%D0%BE%D0%B8%D1%81%D0%BA-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%8B/howtofindjob/jobsearchchannels/jobsearchandsocialnets

Ramirez, A., Walther, J. B., Burgoon, J. K., & Sunnafrank, M. (2002). Information-seeking strategies, uncertainty, and computer-mediated communication. *Human Communication Research*, *28*(2), 213-228.

Robert M. O’Keefe, Gina O’Connor, H.-J. K. (1998). Early adopters of the Web as a retail medium – small company winners and losers. *European Journal of Marketing*, *32*(7/8), 629–643. http://doi.org/10.1108/03090569810224038

Rubenfeld, J. (1989). The right of privacy. *Harvard Law Review, 102*(4), 737-807. http://doi.org/10.2307/1341305

Sánchez Abril, P., Levin, A., & Del Riego, A. (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal*, *49*(1), 63-124.

Savchenko, E. (2012, May) Kto, kak i zachem sledit za vami v internete? [Who, how and why is anyone tracking you on social networks?; Blog post] Retrieved from http://www.k-istine.ru/safety/safety_savchenko.htm

Scott, C. R. (2004). Benefits and drawbacks of anonymous online communication: Legal challenges and communicative recommendations. *Free Speech Yearbook*, *41*(1), 127-141.

Shibutani, T. (1955). Reference groups as perspectives. *American Journal of Sociology,* 60(6), 562-569. Retrieved from http://www.jstor.org/stable/2771966

Social’nye seti i poisk raboty [Social networks and job search; Blog post]. (2015, October). Retrieved from http://jewspace.org/article/Socialnye-seti-i-poisk-raboty

Social’nye seti v Rossii: Cifry i trendy za fevral’ 2016 [Social networks in Russia: Numbers and trends in February 2016; Statistics]. (2016, April). Retrieved from http://br-analytics.ru/blog/socialnye-seti-v-rossii-cifry-i-trendy-za-fevral-2016-g/

Social'nye seti v Rossii, vesna 2015: Cifry, trendy i prognozy [Social networks in Russia, spring 2015: Numbers, trends, forecasts; Statistics]. (2015, June). Retrieved from http://br-analytics.ru/blog/socialnye-seti-v-rossii-vesna-2015-cifry-trendy-prognozy/

Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2013). Big Five Personality Traits Reflected in Job Applicants' Social Media Postings. *Cyberpsychology, Behavior, and Social Networking*, *16*(11), 800–805. http://doi.org/10.1089/cyber.2012.0163

Subrahmanyam, K., Reich, S. M., Waechter, N., & Espinoza, G. (2008). Online and offline social networks: Use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology*, *29*(6), 420-433. http://doi.org/10.1016/j.appdev.2008.07.003

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5), 557-570.

Treem, J. W., & Leonardi, P. M. (2012). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Communication Yearbook*, *36*, 143-189.

Trottier, D. (2012). Interpersonal surveillance on social media. *Canadian Journal of Communication*, *37*(2), 319-332. Retrieved from http://search.proquest.com/docview/1027767558?accountid=13598

Trottier, D., & Lyon, D. (2012). Key features of social media surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and Surveillance: The challenges of Web 2.0 and social media*, *16*. (pp. 89-105). New York: Routledge.

Tsvetkova, D. A. (2014) *Rol' social'nyh setei v professii HR manager [The role of social networks in the profession of HR manager]*. (Unpublished master's thesis). Retrieved from https://www.hse.ru/edu/vkr/125124386

Umarov, M. (June, 2010). Rabotodatel', popavshii v social'nuyu set' [Employer, stuck in social networks; Blog post]. Retrieved from http://www.forbes.ru/svoi-biznes-opinion/master-klass/51813-rabotodatel-popavshii-v-sotsialnuyu-set

Uvolen za lyubov' k Facebook: Kak pravil'no sovmeschat' rabotu i socseti [Fired for love to Facebook: How to combine work and social networks; News article]. (2016, March). Retrieved from http://www.aif.ru/society/web/uvolen_za_lyubov_k_facebook_kak_pravilno_sovmeshchat _rabotu_i_socseti

Van Dijck, J. (2013). 'You have one identity': Performing the self on Facebook and LinkedIn. *Media, Culture & Society*, *35*(2), 199-215. http://doi.org/10.1177/0163443712468605

Vazire, S., & Gosling, S. D. (2004). e-Perceptions: Personality impressions based on personal websites. *Journal of personality and social psychology*, *87*(1), 123-132. http://doi.org/10.1037/0022-3514.87.1.123.

Voida, A., Mynatt, E. D., Erickson, T., & Kellogg, W. A. (2004, April). Interviewing over instant messaging. *CHI'04 Extended Abstracts on Human factors in Computing Systems*, 1344-1347.

Walther, J. B. (2011). Theories of computer-mediated communication and interpersonal relations. In M. L. Knapp & J. A. Daly (Eds.), *The Sage Handbook of Interpersonal Communication* (4th edition; pp. 443–479). Thousand Oaks, CA: Sage Publications.

Ward, V. (2013, May) Children using internet from age of three, study finds [News article]. Retrieved from http://www.telegraph.co.uk/technology/internet/10029180/Children-using-internet-from-age-of-three-study-finds.html

Winer, B. J., Brown, D. R., & Michels, K. M. (1971). *Statistical principles in experimental design*. New York: McGraw-Hill.

Wittel, A. (2001). Toward a network sociality. *Theory, Culture & Society*, *18*(6), 51-76.

Wood, A. F., & Smith, M. J. (2004). *Online communication: Linking technology, identity, & culture*. New York: Routledge.

Yanisky-Ravid, S. (2014). To read or not to read: Privacy within social networks, the entitlement of employees to a virtual "Private zone", and the balloon theory. *American University Law Review, 64*(1), 53-107.

Zukowski, T., & Brown, I. (2007, October). Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 197-204). ACM.

Appendix A

Interview guide

Good afternoon! I am a student of Erasmus University and I am carrying out the research, which is targeted at understanding attitudes and practices connected to the job-seeking procedures and employer-employee relationships but we will discuss the exact phenomenon later. Our interview will last around one hour and I am going to make a recording for further processing of the research. However, none of your personal details mentioned during the interview will be used in the research.

Firstly, let me know some basic information about you.

Introduction

- Educational level
- Employment status
    - If the respondent currently has a job – how did he/she find a job; in which sector, company, for how long; possible to ask a few words about the relationships with the boss
    - If the respondent does not work – which channels of job-seeking is he/she using; if he/she mentions media – elaborate on it)
    - If he/she found a job with a help of his personal network or agencies, ask, if he/she has ever searched for a job on the internet
- Social media and internet use
    - When did you start using internet? Social media?
    - Nowadays: how often, which platforms, purposes of use
    - Have you ever posted something online that you have deleted afterwards? Due to which reasons? (Could you please describe the situation, if it is not sensitive?)

Part I

- Imagine the situation: you are applying for a job in your chosen sector. You have sent your CV and attended a personal interview with an employer. In couple of weeks you get a call/an e-mail from the company, saying that you are employed for the position. The company also informs you that they had a third step of evaluating your fit for the position by checking your profiles in different social networks. How would you react to this? However, mind that your private information like messages and passwords were not being checked.

- Imagine the same situation again. However, this time you get a call/an e-mail that you are not employed for the position. The company still informs you that the main reason for this is that they were evaluating your online space and that became a main reason. Will your attitude to the company's actions change? Overall, do you consider it a sufficient criterion fore rejection?
- Now imagine the following: the company hires/or rejects you, however it does not explicitly tell you about the fact that they were evaluating your social networks and based their decision on that. You get to know about it by accident from someone else – maybe your colleague or a friend. Is it important for you that the company informs you about the fact of checking your online information?

Part 2

As it may be clear by now, the phenomenon that interests me is cybervetting – employers' use of employees' online information for personnel selection. Online sources that are used by employers in this case are not usually used for professional tasks (like, for instance, LinkedIn). Employers in this case collect information from "…informal, non-institutional, online sources to inform personnel selection decisions without workers' specific knowledge, permission or opportunity for correction". Did you know about this phenomenon before? If yes, where/when/how you first learnt about it? 'If possible, can you provide a situation where this process occurred, either to you, or a colleague or friend, or in a more prominent case in the news'.

- If the topic of "privacy" was not touched upon by the respondent himself:
  - How do you understand the term "privacy" within social networks?
  - Are social media for you more of a private space or a public space?
  - What is the relation between cybervetting and privacy? Do those terms overlap?
- Do you think that the messages that you send online are private? While you are sending the messages, do you assume the probability that they can be seen by someone else except for the recipient? However, do you feel freer in expressing yourself in the messages rather than in your profile?
- There is a relatively new saying that I recently came across, which is: do not ever post/write something on the internet that you would not like to see on a first page of a newspaper. How can you interpret that and do you think it is right or wrong and why?

- (If the respondent is currently working) Do you think/know that your employer was using cybervetting while evaluating you as a candidate? How do/would you feel about it?

Part 3

- Let us take a closer look at present situation with your social media use. If I mention the word combination digital footprint, what comes to mind?
- Basically, the information that you post online can possibly remain online indefinitely and virtually anybody could get access to it. Those could also be your current/future employers. Are you thinking about it while managing your online space?
- If yes, are there any specific actions that you are taking in order to protect your personal information or even escape leaving a digital footprint? Any specific ways to create your online image? Which are those?
- How effective do you think those ways are? (e.g. can they actually protect your online information from your employer?) What may be the limits of those kind of protection?

Part 4

- There has recently been a case in Moscow that banks are considering checking online information about the borrowers in order to make a decision whether to give them credit. Have you heard about it? How would you react to such a practice?
- Cybervetting as a practice is becoming more and more used in different spheres, in personnel selection as well. If you had an opportunity, would you make any rules and/or restrictions for employers in terms of how they can use online information of candidates?
- Do you think that there are some certain positions that may require more attention towards the information that is found by means of cybervetting? (e.g. people in position of power, people working with vulnerable populations, public figures)

Conclusion

Thanks a lot for participating in the research. The topic of cybervetting is respectively new and has not yet been studied in Russia. However, I find this issue quite an important one. If you have any ideas or comments that can help me during this research, I will be happy to hear them.

Appendix B

Description of the respondents

#	Name of the respondent	Gen-der	Age	Education	Employment status	Profession
1	Alexandra	f	23	Medical University; Children's stomatology	Employed for 3 months	Children's stomatologist
2	Elena	f	53	St.-Petersburg State Financial and Economic University; Statistics, accounting and economic analysis	Unemployed, looking for a job	Recent position: chief accountant
3	Irina	f	24	Moscow State University; Politics	Internship	Marketing
4	Katerina	f	36	PR	Self-employed	Consultancy, marketing
5	Lenya	m	22	Higher School of Economics, Bachelor in Psychology; currently doing Master in Psychology	Unemployed; looking for a job	
6	Nataliya	f	50	PR and Advertisement	Unemployed; looking for a job	PR manager
7	Lena	f	25	Higher School of Economics; Master in Sociology	Employed for 9 months	Lecturer
8	Sveta	f	24	Russian State University for the Humanities; Juridical faculty	Unemployed; looking for a job	
9	Sasha	m	23	Moscow Financial University; Bachelor in Finance	Employed for 9 months	Banking (financial analyst)
10	Vladimir Sergeevich	m	44	Aviation Engineering	Employed for 4 months	IT specialist
11	Vitya	m	22	Higher School of Economics; Bachelor in History, undergraduate	Employed for 7 months	Courier
12	Evgeny	m	22	Higher School of Economics; Bachelor in Management	Employed for 9 months	Marketing assistant
13	Anton Alexandrovich	m	58	Polytechnic University, Faculty of Civil and Industrial Engineering	Employed for 4 months	Engineer
14	Sergey	m	41	Moscow State University; Faculty of Mechanics and Mathematics	Unemployed; looking for a job	Recent position: financial analyst