SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 228

RECRUITMENT IN THE DIGITALIZATION AND AI ERA – AWARENESS AND ATTITUDES OF HR PRACTIONIONERS TOWARDS CYBERVETTING

Marzena PYTEL-KOPCZYŃSKA[1], Rafał NIEDBAŁ[2*]

[1] Czestochowa University of Technology, Faculty of Management; rafal.niedbal@pcz.pl, ORCID: 0000-0001-8850-8586
[2] Czestochowa University of Technology, Faculty of Management; marzena.pytel-kopczynska@pcz.pl, ORCID: 0000-0001-6898-8818
* Correspondence author

Purpose: The purpose of this paper is to determine to which extent the personal managers, HR specialists and recruiters of big companies in Lodz and Silesia Provinces are aware of the possibilities to use cybervetting including AI tools as an element of the recruitment process.
Design/methodology/approach: The survey test CAWI (n = 113) was applied. The questionnaire covered the one- and multiple choice questions and seven statements assessed with the use of 4-grade Likert scale and the responses were analysed with the consideration of the respondents' seniority.
Findings: About 40% of respondents have already been using or had direct knowledge about the application of cybervetting practices in their companies; Facebook, Instagram and LinkedIn are the most valuable data sources. The risks to infringe privacy and discrimination are perceived by personal managers, HR specialists and recruiters with the seniority up to 10 years more stronger whereas the persons with the seniority over 20 years regard the AI as helpful in the limitation of decision subjectivity.
Research limitations/implications: The limitation of the conducted research is its exploration nature which may make it difficult to generalize the results. Thus, it is recommended to cover wider, sector-differentiated sample in further research, and to use deepened interviews and case studies to analyse the cybervetting practices.
Practical implications: The research results lead to four recommendations for employers: (1) annual audit of social media review, (2) obtaining clear, voluntary agreements of candidates for such a verification, (3) providing them with a short training about digital identity and (4) providing 48-hour "right to comment" to the negative arrangements.
Originality/value: The paper provides empirical data about the awareness and attitudes of HR practitioners concerning cybervetting and AI tools, indicating the generation and experience differences, which extends the discussion about the employees' digital selection.
Keywords: cybervetting, recruitment, social media, artificial intelligence.
Category of the paper: research paper.

1. Introduction

Social Network Sites (SNS) have become a significant factor shaping the communication environment of modern societies, penetrating all aspects of human everyday life (Borcuch, Świerczyńska-Kaczor, 2013). This digital environment make in possible to the users to maintain wide network of social contacts in an unprecedented way by creating online profiles which enable to start contacts, interaction and communication, share everyday experiences (in a form of photos, texts, films) and consume the contents of other users of these digital applications (Hussenoeder, 2022). In the time the significant content of online social network sites together with autoprenentation of their users may become publicly available. Such contents may be also visible for potential future employees affecting the development of career path. This digital trace of potential interested parties of the recruitment process has become the focus of interest of entrepreneurs, decision makers, human resource specialists and recruiters using cybervetting in the HR process (Jacobson, Gruzd, 2022; Hedenus et al., 2021).

The purpose of this paper is the attempt to identify the personal managers', HR specialists', recruiters and decision makers' of big companies awareness concerning the employment process referring to the possibility to use cybervetting practices as a recruitment process element. The responses to the following research questions may be helpful to perform the research purpose:

- RQ1. Do the companies introduce cybervetting practices – understood as the analyses of publicly available information on the Internet for the needs of candidates' recruitment – and which types of the Internet sources may be the most useful in this process?
- RQ2. Can the implementation of cybervetting in the recruitment procedure be connected with the increase in the risk to infringe the candidates' privacy and the increase of prejudices and discrimination practices towards them?
- RQ3. Is the possibility to use information and artificial intelligence (AI) tools justified to analyse the publicly available information on the Internet about the job candidates during the recruitment process?

The exploration of the research questions above allows to specify the possibilities to apply the practice of digital verification of the job candidates.

2. Cybervetting as a practice in the recruitment process

Cyber verification of the job candidate is an economic practice which is widely used in the receruitment processes and consists in gathering and analysing data coming from widely available Internet sources, in particular from social media. It is a support for HR decision

makers in the optimisation of HR decisions referring to matching the candidate's profile to the needs and organizational culture of a given company (Berkelaar, Harrison, 2016). It is based on the implementation of information tools and sources, not connected with the institutional recruitment system, including social network sites, with the intention to obtain informal and personal data about the candidate which were not presented during the job interview (Holubek et al., 2024). In the subject literature the cybervetting events are focused on the prediction of candidates' personality[1] in the context of futute productivity in the work processes as well as their loyalty towards the organisation (Demir, Gunaydin, 2023). Cyber verification which is also sometimes called 'profiling' (McDonald, Thompson, 2026) is gaining popularity among HR decision makers in many geographical widths (Wilcox et al., 2022; Roulin, Liu, 2023). The analysis of digital identity of the potential employee in the context of verbal communication, non-verbal signals and other visual contents presented on the Internet enables to construct the applicant's profile and formulating assessments referring to their behaviour and personal features (Harrison, Budworth, 2015; Berkelaar, 2017). It suggests that the candidates' presence on the Internet may significantly affect their future career (Twes et al., 2020; Zang et al., 2020). The cyber verification is often performed at the beginning stage of the candidates' selection and it does not constitute the element of formal documentation and application procedures (Hartwell et al., 2022). The preliminary selection and candidate screening based on their profiles (physical appearance, hobby, opinions about current matters)[2], enables the fast and inexpensive background of a potential employee before inviting them to the proper job interview.

There are no exact statistical data precisely specifying the number of employers using the cyber verification as well as it is difficult the rate of their wideaspread in particular countries, sectors or branches of the economy. Despite this, as it results from the presentations prepared by Swedish independent organizations (e.g. Stockholm Chamber of Commerce), it is the practice widely used by employers (Backman, Hedenus, 2023). What interesting, the research conducted by American employers show that as many as 70% of them treat the social media as the tool supporting job candidate verification process (Walrave et al., 2022). In the American job market, both candidates and employers regard cyber verification as an integral and acceptable component of recruitment process. It means that a new digital social contract appears which reflects the significance of aware shaping of the image in the virtual space, apart from work place and time, increasing the employment prospects (Berkelaar, 2014).

[1] Although it may be assumed that the social media profiles present the ideal image of their authors, they often indicate the realistic presentation of their features. In particular, selfie- photos are reliable when it comes to presenting such personal features as agreeableness, diligence, neuroticism, openness (Qui et al., 2015).

[2] According to some recruiters, the most discouraging elements of candidates' profiles in SNS are: spelling and grammar mistakes in posts or tweets (45%); referrals to marihuana (40%); alcohol consumption (39%); political posts (30%) and pictures of body showing skin: 24% (*Recruiter Nation Report*, 2021).

It should be stressed that cyber verification as a multi-context practice arises some objections in the area of ethics, blurs the borders between professional and private life which may increase the risk of discriminating actions leading to social exclusion (Vosen, 2021). The implementation of tools based on artificial intelligence[3] in the preliminary recruitment stages may be a potential solution minimizing or eliminating the risk of wrong personal decisions and unethical practices. The use of AI enables to compare many candidates to the give job position by analysing not only application documents but also profiles and other publicly available digital data. AI may support recruiters' decision-making process when it comes to the assessment whether the declared competences are consistent with the workplace requirements, which allows to manage the information about candidates in an efficient way. The construction of ranking system assessing the candidates' adaptation to the working environment requirements which protects the private data from social media making only the aggregated assessment of potential employees' activity available according to the key criteria taken by the organization would be a significant prerequisite to implement AI technology to objectivate the cyber verification process (da Motta Veiga, Figueroa-Armijos, 2023).

3. Research method

The survey research was conducted with the use of the CAWI method (Computer Assisted Web Interview) in the period from November 2024 to March 2025. The questionnaire was presented to the big companies from the Lodz and Silesia Provinces, obtaining 113 complete responses. The participation in the research was voluntary and its results should be regarded as pilot observation. The respondents were managers and specialists dealing with employees' recruitment processes who represented big subjects of two key sectors of economy – industry and services (with the exclusion of financial institutions).

The research questionnaire consisted of 18 questions in total: 7 of one-choice questions, 4 multiple choice questions and 7 statements assessed with the use of even four-grade Likert scale without neutral point. The use of the scale without the mean value was aimed to make the respondents take a clear attitude limiting the possibility to choose the "safe" response which would not reflect their clear opinion. The questions in the questionnaire were preceded with the definitions of cybervetting and information tools used both in the process of candidates' selection as well as employees' monitoring. They were as follows (Berkelaar, Harrison, 2016; Jacobson, Gruzd, 2020; Laksanadjaja, Oviedo-Trespalacios, 2024):

[3] As the analyses performed by the Society of Human Resources Management in February 2022 shows as many as 79% of employers uses the solutions based on AI or automatizing technologies in the recruitment processes and selection of job candidates (Friedman, 2023).

- Cybervetting (i.e. so called cyber verification) is a practice to use the information available publicly on the Internet in order to assess job candidates or monitor employees. It covers search and analysis of data available in social media, discussion forum, blogs, branch services and other online platforms in order to obtain additional information about a person such as professional experience, competences as well as aspects which may affect recruitment or management decisions.
- Information tools supporting cybervetting and employees' monitoring are automatic systems used to: gather data, analysis of contents and behaviour, reporting and visualization, executing the security policies. In the context of the recruitment process, these tools support HR departments in minimizing the risk of employing the inappropriate worker, unifying and documenting "background check" process in the online environment. After the candidate employment, in the case of their actions undesirable for the company, the same or similar monitoring systems help the IT and human resources management departments protect the good company image and data.

Also the definition of AI tools used in cybervetting was precised in the contents of the invitation to fill in the survey questionnaire in order to eliminate the terminological ambiguities[4].

The empirical analysis in this paper is limited to the questions referring to the potential possibilities to use cybervetting in the employees recruitment process regarded in the context of seniority of persons responsible for this process. The separate deepended analysis of differences between sectors – covering the companies from sectors of industry and non-financial services will be presented in a separate publication.

4. Cyberveting – results of empirical research and discussion

The research sample consisted of 46.8% of respondents (53 persons) with the over 20 years of experience in recruitment, 26.6% of surveyed – persons with the experience of 11-20 years. The experience in the groups to 5 years and 6-10 years was represented by the same number of respondents – 13.3% of all tested (15 persons each). In the research sample 54.0% of

[4] AI tools in cybervetting cover the system components using machine learning or natural language processing to analyse and generate contents. The typical processing chain covers three layers: (1) module of data extraction – automatically downloads public posts, photos and metadata of candidates, using API (Application Programming Interface) platform or web-crawling; (2) machine learning models classifying texts and pictures, indicating among others hate speech, level of professionalism and calculating the indicators of risk and cultural matching; (3) generative modules based on big language models merging the analysis results into brief reports supporting recruitment decisions. According to EU AI Act, the presence of layers (2) and (3) classifies the cybervetting system as a high-risk solution in the employment field. The module of data extraction is subject to GDPR, especially the rules of source legality, minimization and limitation of the aim, which means that the gathered data may be used only for the clearly specified recruitment actions.

respondents (61 persons) represented the companies of the industry and 46.0% of respondents (52 persons) were from the sector of services (non-financial service companies).

The first question of the survey was to determine whether the practices based on the verification of information publicly available on the Internet (e.g. social media, branch portals) were used to assess job candidates in the present or previous job of the respondents dealing with recruitment. The results are presented in Table 1.

Table 1.
Using the cybervetting practices in the recruitment processes

Were the practices based on the verification of information publicly available on the Internet (e.g. social media, branch portals) used to assess job candidates in your present or previous job?	Seniority				Total (number of indications %)
	Up to 5 years (n = 15)	6-10 years (n = 15)	11-20 years (n = 30)	Over 20 years (n = 53)	
Yes, I used such practices myself	8	-	7	8	20.35
Yes, I have direct knowledge about using such practices in my company	-	-	7	14	18.59
Yes, I heard about single cases but I have not had contact with them personally	-	8	8	7	20.35
No, but I am aware of the possibility of using such practices	7	7	8	24	40.71
No, I am not aware of such practices	-	-	-	-	-

Source: own study.

Analysing the percentage of indications, the answer selected most often was "No, but I am aware of the possibility of using such practices" (40.71% of all respondents). The other responses should be assessed positively taking into consideration the awareness that the cybervetting practices are used in the recruitment processes or the experience of respondents in this area. It turns out that 20.35% of respondents used cybervetting personally, have direct knowledge about using it in their companies (18.59%) or at least heard about individual cases not having direct contact with them (20.35%). It should be also stressed that no person marked the response *I am not aware of such practices*.

According to the respondents, social media like Facebook (30.63% of all indications) and Instagram and LinkedIn – 25.09% and 22.14 of all responses – are the most useful, publicly available source of information in the cyber verification of job candidates (Figure 1). The questions about the source of information was a multiple-choice question. The very high position of Instagram – the photographic social service of hostic photos – was an interesting result in the research. It is worth emphasizing that the result was similar to the result of the social media platform LinkedIn. The last one is a professional social network site the main aim of which is to start and maintain professional contacts. Platform LinkedIn enables to create professional profiles, publish information about education, experiences, abilities and achievements as well as active job search and rectruitment of employees. LinkedIn is also used to create personal brand, share brand information, participate in subject groups and develop the contact networks in the business environment.

Referring to the research question RQ2 formed in the introduction, it is possible to state that the cybervetting practices are used in a relatively big part of tested companies – in total 40% of respondents used such practices or know about using them in their companies. Then the respondents regarded such social platforms as: Facebook, Instagram and LinkedIn as the most useful Internet sources of information about job candicates, which are publicly available.

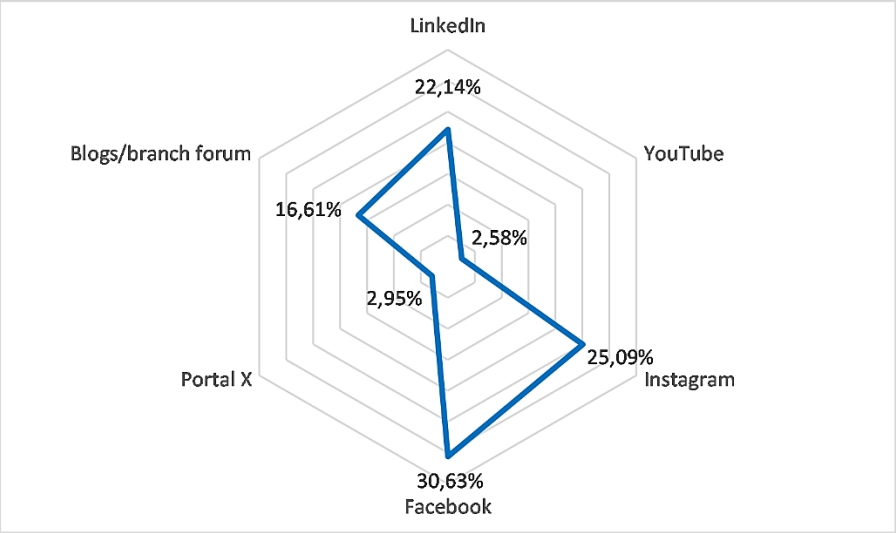

Figure 1. Internet sources used in the cyber verification of job candidates.

Source: own study.

However, the question arises which may be the reason for further research – whether the photos published by candidates, for example on the Instagram, play such an important role for the persons dealing with recruitment of employees in comparison to LinkedIn. To compare, the results of research conducted by Backman and Hedenus (2023) showed that American recruiters use the cyber verification process to obtain the most reliable image of candidates, their level of professionality and consistence of their virtual image with the norms of working environment and organizational culture. Moreover, this process is used to limit biases in personal decisions, to protect company reputation, to optimize the risk connected with it and also it satifies the curiosity and individual cognitive needs of HR decision makers. Human resource specialists obtain information about job candidates using various social network sites including: Facebook (68%), LinkedIn (65%), Twitter (48%), Instagram (46%) or YouTube (35%) (*Recruiter Nation Report*, 2021).

Two questions in the survey questionnaire referred to the existence of respondents' fears connected with the risk to infringe job candidates' privacy (Figure 2) and the possibity to create biases or discrimination in the recruitment process as a result of cybervettting (Figure 3). The possible answers in the first of these questions were" "low", "moderate", high" and "very high". The response selected most often among the respondents with the seniority over 5 years was the rensponse "moderate" and "high". The surveyed with the low seniority (up to 5 years) assessed the risk as "very high" (53% of respondents in this group) and "high" (47%).

The answer selected most often in the question *Do you think that using cybervetting may lead to create biases or discrimination in the employees' recruitment process* was "rather yes". As many as 87% of respondends from the group of job experience 6-10 years gave such an answer – and for other groups: 73% (seniorit 11-20 years), 62% (seniority up to 5 years), 45% (seniority over 20 years), respectively.

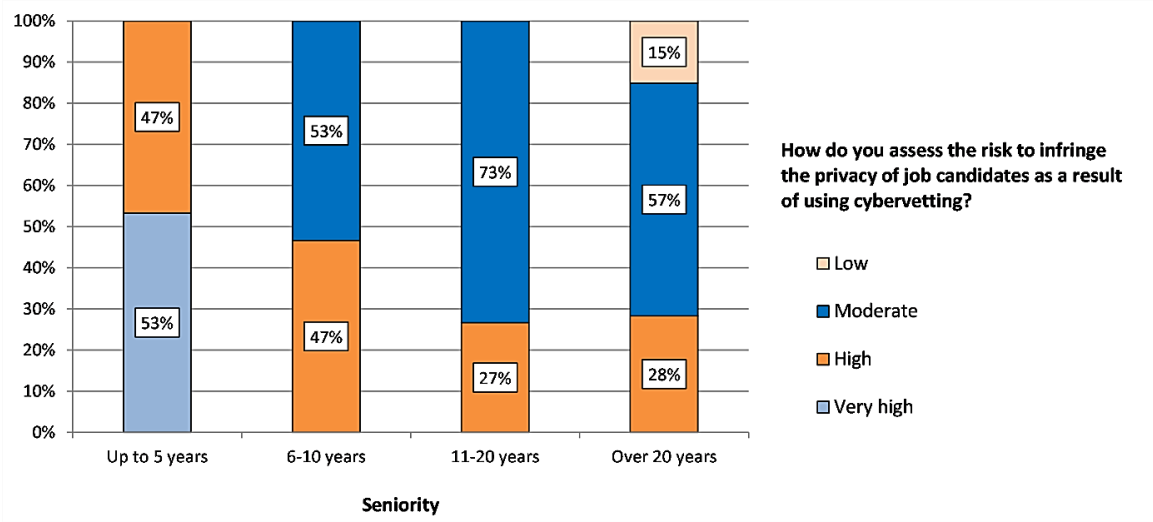

Figure 2. The risk to infringe the privacy of job candidates and using cybervetting.

Source: own study.

Thus, using cybervetting in the recruitment processes leads, according to the respondents, to the increase in the risk to infringe candidates' privacy as well as to the intensity of biases and discrimination towards them (which constitutes the answer to research question RQ2). The mentioned opinions are consisted with the results of the analyses of numerous researchers which connect directly the use of cybervetting with with the increase in the risk to infringe candidates' privacy and increased probability of discrimination and biased recruitment decisions (Backman, Hedebus, 2023; Walrave et al., 2022).

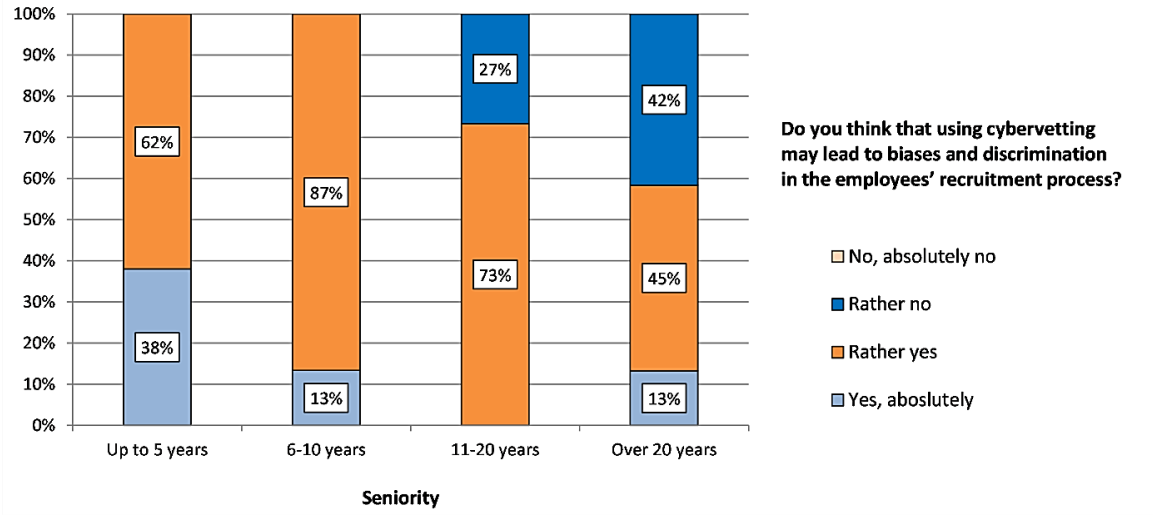

Figure 3. The existence of biases and discrimination in the recruitment process and using cybervettingu.

Source: own study.

The tendency may be observed that the respondents with lower experience of participation in recruitment processes in the company express greater fears concerning the risk to infringe the privacy of job candidates than the persons with higher experience. Such an observation should be also regarded as interesting as the just opposite result could be assumed – that the persons with high job experience would assess the risk as "very high" or "high". Moreover, the lower the job experience of the surveyed, the more they notice the negative effect of using cubervetting in a form of increased biases and discriminating practices towards job candidates.

The repondents were also asked to present their opinion towards the statement: *It is justified to use information tools and artificial intelligence (AI) technologies to analyse the data referring to candidates, including the information obtained from social media in the employees' recruitment process. Such an approach may support the identification of competences, assessment of cultural adaptation and preliminary selection of applicants, increasing the efficiency and accuracy of recruitment decisions* (Figure 4).

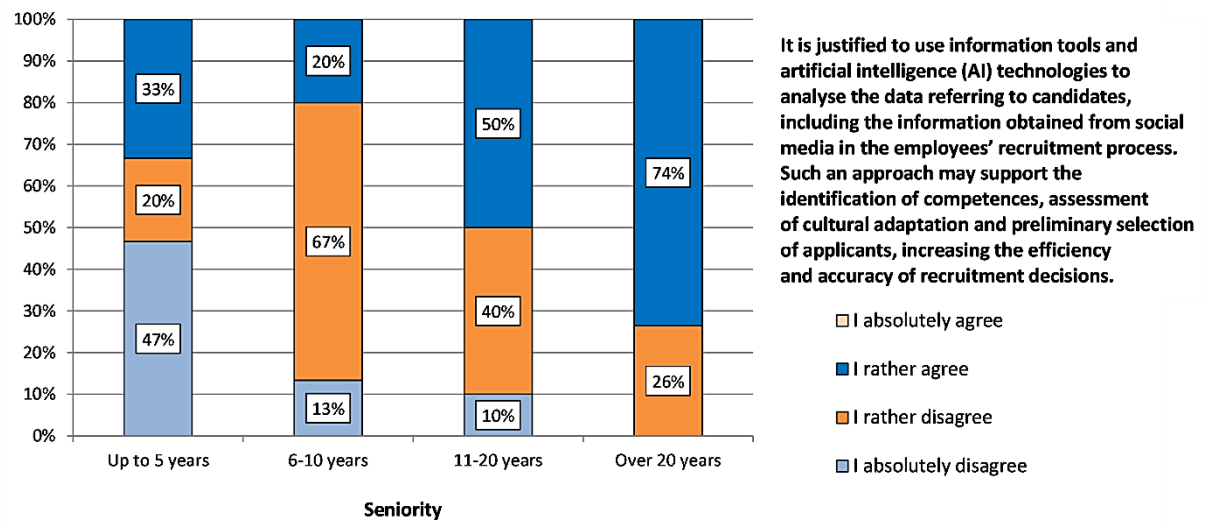

Figure 4. Use of AI tools in cybervetting and the employees' recruitment process.
Source: own study.

The 4-grade Likert scale in the scope from 1 ("I absolutely disagree") to 4 ("I absolutely agree") was used to the responses. The response indicated most often among the respondents with job experience over 20 years was "I rather agree" (74%), with the job experience 11-20 years – also "I rather agree" (50%), with job experience 6-10 years "I rather disagree" (67%) and with the job experience up to 5 years "I absolutely disagree". Summing up the indications "I absolutely disagree" and "I rather disagree" in particular groups of respondents (concerning the job experience), it can be observed that the most of such responses were given by the persons with lower job experience – 80% of responses in the group with the job experience 6-10 years and 67% in the group with the job experience up to 5 years. No respondent indicated the answer "I absolutely agree".

The response to the research question RQ3 is not unanimous and depends on the respondents' job experience. Persons with the low job experience (up to 10 years) claim that the use of such tools is justified. And also this time the unclear test results encourage to further thoughts and research – as the persons with the highest job experience (74% of tested in this group indicated the answer "I rather agree") declare the justification of using information tools and artificial intelligence technologies in cybervetting.

However, it should be emphasized that the inclusion of cyber verification supported by AI to the formal recruitment process and candidate selection may assist the companies with obtaining and gathering data in an aggregated form, aggregate data (e.g. by the mechanism of point assessments) at the same time being consistent with the regulations concerning privacy (da Motta Veiga, Figueroa-Armijos, 2023).

5. Operational recommendations

In order to provide responsible and lawful use of cyvervetting in social media – independently of the fact whether the profile analisys is run by a recruiter, compliance team or is supported by AI software – the organisations should apply four complementary operational practices: (1) The internal protocol of cybervetting audit should be created. At least once a year an interdisciplinary team covering HR, legal department and data protection officer should check which social sources are reviewed, which categories of information are subject to assessment and whether the selection criteria do not lead to discrimination or infringe the rules of minimizing data specified in GDPR. (2) Cybervetting has to be included in the standardized mechanism of aware consent: the candidate receives in the job announcement or application form the short, clear explanation that his public Internet activity may be analysed, in which scope and for which reason and further steps occur only after the clear confirmation of acceptance. (3) The companies should provide the candidates with synthetic education materials concerning digital identity – for example a short film or infographics – showing how the contents published in the net may be interpreted by the employer and which elements of the profile contribute to the assessment of cultural matching the most often. (4) The candidate should have the "right to comment" guaranteed, i.e. at least 48-hour time period to refer to any negative arrangements arising from cybervetting before the recruitment decision is taken; this practice limits the risk of wrong or contextually unjustified assessment.

The implementation of these four actions harmonises the cybervetting process with the indications of Personal Data Protection Office and the regulations of EU AI Act (*Regulation EU 2024/1689, Art. 6*).

6. Conclusion

The paper presents the analysis of the rate of using cybervetting practices in the employees' recruitment process of the bigh companies in the Lodz and Silesia Privinces. The survey research showed that about 40% of companies have already been using or are going to use the overview of candidates' social media, especially Facebook, Instagram and LinkedIn. The less experiences recruiters (the seniority under 5 years) express greater fears referring to privacy and the possibility of biases, whereas the most experienced ones (seniority over 20 years) perceive AI tools as a chance to limit the subjectivity of recruitment decisions.

The limitation of the conducted research is its exploration nature which may make it difficult to generate the results. Further research work should cover the sector differentiated sample as well as apply qualitative methods – in-depth interview and case studies – to examine how the recruiter attitudes change with time, to assess the efficiency of operational recommendations and to determine the longterm influence of cybervetting on candidates' trust to digital selection processes.

References

1. Backman, Ch., Hedenus, A. (2023). Professional talk on cybervetting: Accounting for a contested practice. *Acta Sociologica*, *Vol. 66, Iss. 1*, pp. 59-73.
2. Berkelaar, B.L. (2017). Different ways new information technologies influence conventional organizational practices and employment relationships: The case of cybervetting for personnel selection. *Human Relations*, *Vol. 70*, *Iss. 9*, pp. 1115-1140.
3. Berkelaar, B.L. (2014). Cybervetting, Online Information, and Personnel Selection: New Transparency Expectations and the Emergence of a Digital Social Contract. *Management Communication Quarterly*, *Vol. 28*, *Iss. 4*, pp. 479-506.
4. Berkelaar, B.L., Harrison, M.A. (2016). Cybervetting. In: *The International Encyclopedia of Organizational Communication* (pp. 1-7). New York, NY, USA: John Wiley & Sons.
5. Borcuch, A., Świerczyńska-Kaczor, U. (2013). Serwisy społecznościowe – jednostka i społeczeństwo na pograniczu świata rzeczywistego i świata wirtualnego. *Zeszyty Naukowe*. *Organizacja i Zarządzanie.* Politechnika Śląska, pp. 61-70.
6. da Motta Veiga, S.P., Figueroa-Armijos, M. (2022). Considering Artificial Intelligence in Hiring for Cybervetting Purposes. *Industrial and Organizational Psychology*, *Vol. 15*, *Iss. 3*.
7. Friedman, G.D. (2023). *Artificial intelligence is increasingly being used to make workplace decisions–but human intelligence remains vital*. Retrieved from:

https://fortune.com/2023/03/13/artificial-intelligence-make-workplace-decisions-human-intelligence-remains-vital-careers-tech-gary-friedman/, 14.05.2025.

8. Harrison, J.A., Budworth, M.-H. (2015). *Unintended consequences of a digital presence*. *Career Development International*, *Vol. 20*, *Iss. 4*, pp. 294-314.
9. Hartwell, C.J., Harrison et al. (2022). Structuring social media assessments in employee selection. *International Journal of Selection and Assessment, Vol. 30, Iss.* 5, pp. 330-343.
10. Hedenus, A., Backman, C. et al. (2021). Whom do you know? Recruiters' motives for assessing jobseekers' online networks. *International Journal of Human Resource Management*, *Vol. 32, Iss. 8*, pp. 1754-1777.
11. Hussenoeder, F.S. (2022). Social network sites as learning environments and their implications for mental health. *Frontiers in Digital Health*, *Vol. 4*, *939740*.
12. Jacobson, J., Gruzd, A. (2020). Cybervetting job applicants on social media: the new normal? *Ethics and Information Technology*, *Vol. 22*, pp. 175-195.
13. Laksanadjaja, F., Oviedo-Trespalacios, O. (2024). Uncovering the Web of Secrets Surrounding Employee Monitoring Software: A Content Analysis of Information Provided by Vendors. *Human Behavior and Emerging Technologies*, *7951911*.
14. Qiu, L., Lu, J. et al. (2015). What does your selfie say about you? *Computers in Human Behavior*, *Vol. 52*, pp. 443-449.
15. *Recruiter Nation Report* (2021). Agility: The Essential Ingredient for Recruiting Success. Retrieved from: https://www.jobvite.com/lp/2021-recruiter-nation-report/, 15.05.2025.
16. *Regulation (EU) 2024/1689, Article 6*: Classification Rules for High-Risk AI Systems, OJ L 2024/1689, 12 July 2024. Retrieved from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj, 05.07.2025.
17. Roulin, N., Liu, Z. (2023). Job seekers' attitudes toward cybervetting in China: Platform comparisons and relationships with social media posting habits and individual differences. *International Journal of Selection and Assessment*, *Vol. 31, Iss.* 2, pp. 347-354.
18. Tews, M.J., Stafford, K. et al. (2020). The effects of negative content in social networking profiles on perceptions of employment suitability. *International Journal of Selection and Assessment*, *Vol. 28, Iss.* 1, pp. 17-30.
19. Vosen, E. (2021). Social media screening and procedural justice: Towards fairer use of social media in selection. *Employee Responsibilities and Rights Journal, Vol. 33*, pp. 281-309.
20. Walrave, M., Van Ouytsel et al. (2022). Checked and Approved? Human Resources Managers' Uses of Social Media for Cybervetting. *Journal of Cybersecurity and Privacy*, *Vol. 2*, pp. 402-417.
21. Wilcox, A., Damarin, A.K. et al. (2022). Is cybervetting valuable? *Industrial and Organizational Psychology, Vol. 15, Iss. 3*, pp. 315-333.
22. Zhang, L., Van Iddekinge et al. (2020). What's on Job Seekers' Social Media Sites? A Content Analysis and Effects of Structure on Recruiter Judgments and Predictive Validity. *Journal Of Applied Psychology*, *Vol. 105, Iss. 12*, pp. 1530-1546.