ATTITUDES OF HR PRACTITIONERS TOWARDS CYBERVETTING IN MONITORING EMPLOYEES' ACTIVITY

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

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

Purpose: The purpose of this article is to examine the HR practitioners' attitudes and approaches in big companies towards the use of cybervetting as a tool of monitoring the employees' activity in social media with the particular consideration of identified benefits, dangers and the influence of the respondents' seniority on the level of the acceptance of such a practice.

Design/methodology/approach: The survey test CAWI (n = 113) was applied among the representatives of big companies in the Lodz and Sielesia Provinces. The questionnaire covered the one- and multiple-choice questions and statements assessed with the use of 4-grade Likert scale and the responses were analyzed with the consideration of the respondents' seniority.

Findings: Almost 65.5% of respondents regards cybervetting as a significant support of employees' monitoring and the acceptance is growing with the seniority – from the objection of the people with the shortest seniority to the highest support of the most experienced ones. The indicated benefits include mainly protection of goodwill and identification of competitive actions and dangers – infringement of privacy and fall of trust.

Research limitations/implications: The limitation of the conducted research is its pilot nature, limited geographical scope and possible overrepresentation of digitally active people. Further research of quantitative and qualitative nature covering deepened interviews and case studies in wider differentiated sample is necessary.

Practical implications: The research emphasizes the need of clear lawful cybervetting policies which limit the risk of privacy infringement and trust fall and at the same time make it possible to protect the organization interests and reputation.

Originality/value: The paper provides empirical data about the managers' and HR specialists' attitudes towards the use of cybervetting in monitoring employees. It shows the differences in the perception of this practice depending on the seniority, indicating the necessity of balance between the organization interests and the protection and autonomy of employees.

Keywords: cybervetting, employees' monitoring, social media, human resource management, privacy.

Category of the paper: research paper.

1. Introduction

Monitoring work processes and the activity of employees in modern organizations exceeds the traditional methods (video monitoring or control of phone conversations). At present, the monitoring methods allow to record keystroke logging, archive the contents of chats, analyze the visited websites as well as to use cybervetting to monitor the activity of company members in social media. Almost 40% of employees in the USA claim that the employer monitors their activity in the workplace and the number of big companies supervising their employees in a digital way amounted to 60% (data of November 2022 – pandemic period). It is anticipated that this percentage will increase to 70% by the end of 2025 (McNutt, 2024). Additionally, the empirical analyses emphasize the significant popularity scale of social platforms in the everyday communication practices. More than a half of adult population in the United Stated (53%) admits that they use social media regularly as a source of gathering actual information (*Social Media and News Fact Sheet*, 2025)[1]. Additionally, according to the results of the research conducted by Pew Research Centre as many as 34% of employees admit that they use social media at work treating it as a break from professional duties (*Monitoring Employee Social Media Activity at Work*, 2025).

The purpose of this article is to examine the big companies HR managers', HR specialists', decision makers' attitudes and opinions towards using cybervetting as a tool of monitoring employees' activity in social media with the particular consideration of identified benefits, dangers and the influence of the respondents' seniority on the level of the acceptance of such a practice.

The answers to the following research questions may be helpful to perform the taken purpose:
- – RQ1. What is the level of support provided by cybervetting in the process of employees' monitoring declared by the managers and HR specialists in big companies?
- – RQ2. In which extent do the managers and HR specialists in big companies accept the use of cybervetting to monitor the employees' activity in social media?
- – RQ3. What benefits and dangers do the respondents attribute to the use of cybervetting towards the employees the most often?

The exploration of the above research questions will allow to recognize the real scope of support which cybervetting provides in the supervision of employees, to specify the level of organizational permission to monitor the activity in the social media and to identify the most often perceived benefits and dangers.

---

[1] What is interesting, the analyses show that Facebook and YouTube take a dominant position: respectively 38% of adult Americans declare that they use Facebook systematically and 35% indicates YouTube to gather current information. Much lower percentage of respondents use other social niedia regularly to gather current information, respectively: Instagram (20%), TikTok (20%) or X (12%). Even less people indicate: Reddit (9%), Nextdoor (6%), WhatsApp (5%), Threads (3%), Rumble (2%), Truth Social (2%) and Bluesky (2%) (*Social Media and News Fact Sheet*, 2025).

This paper is an extension of the previous publication of the authors in which the HR staff's awareness and attitudes towards cybervetting in recruitment processes were analyzed (Pytel-Kopczyńska, Niedbał, 2025). The current paper focuses on using this practice to monitor the employees' activity in the social media.

2. Cybervetting as a practice in employees' monitoring

Functioning of an organization strictly connected with the advance of technological and communication technologies resulted in the presence of the monitoring technology of the employee's activity not only in the workplace (monitoring of communication and productivity of employees with the use of artificial intelligence, gathering biometric data with the use of sensors, algorithmic employees' management in the context of productivity) (Vitak, Zimmer 2023) but also left the boundaries of organizational life by using cybervetting in the processes of monitoring the employees' activity in the social media (Rahat, Nadeem, 2025). The labor future is more and more connected with the common gathering of digital data coming from social platforms (Nguyen, Mateescu, 2019). Gathering new categories of data referring to the employees allows to specify the activities and personal features in a quantitative way, which could not be monitored in the working environment before, intensifying scale and dynamics of data accumulation process[2], blurring at the same time the border between the public and private zone and modifying the set of forces between employers and employees (Nguyen, Mateescu, 2019). The research conducted by the organization Gartner in 2018 showed that over half of big corporations (from 239 tested) uses the digital forms of monitoring covering among others cybervetting of employees' activity in social media (Wartzman, 2019).

The empirical analysis with the participation of 2006 peopled full-time employed in the United Stated and the United Kingdom (Burlee, 2024)[3] admitted in both cases that the digital methods are a dominant form of employees 'monitoring (50% of respondents experience the monitoring of electronic correspondence, chats led with the use of such tools as Gmail, Microsoft Teams or Slack the most often). The most visible difference is that the monitoring of the network and data is used in the U.S. 39% more often than in the UK. What is interesting,

---

[2] The pandemic strongly contributed to the increase in the quantity, scope and diversity of information gathered by employers. These data (so called digital footprint) constitute the basis to draw up employers' digital profiles and implement algorithms which order these data in specific categories and perform assumed analyses of connections between accumulated information (Leonardi, 2021).

[3] As it results from the empirical research (Burlee, 2024) numerous dangers and risks connected with digital monitoring of employees in the virtual space affect the mental health in a negative way (indications of almost 40% of respondents, respectively: U.K. 37.6%; U.S. 36.7%), lower job satisfaction (indications of three out of four surveyed, respectively: U.K 77.5%; U.S. 74.7%). Moreover, a significant conclusion drawn up from the analyses is perceiving the monitoring of employees' activity in the digital world as an unethical activity (respondents' indications, respectively: U.K. 70.6%; U.S. 59%).

only 30% of workers in the USA and 27% in the United Kingdom were formally informed about the active monitoring in the workplace.

The above issues constitute an important argument for the necessity to document practices concerning the use of cybervetting in an organization not only in respect to potential employees (in a recruitment process) but at first to the current employees in the process of monitoring their activity in the social platforms.

From the employer's point of view, there are a lot of justified reasons for implementing cybervetting to monitor employees, starting from the verification of submitting sensitive, confidential or covered with the company secret data to the confirmation of potential unlawful activity (Mikkelson, 2011). Whereas, from the employees' point of view, the use of unclear or inconsistent practice of cybervetting in the employees' monitoring process[4] may result in the feeling of injustice, lowering the engagement level, job satisfaction and trust towards the organization as well as the increase in stress and negative influence on mental condition (Akbulut et al., 2024; Mikkelson, 2011; McNutt, 2024; Burlee, 2024).

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 questions were divided into 4 sections: (I) experience and awareness about cybervetting, (II) legal and ethical aspects, (III) cybervetting in the context of

---

[4] The analysis of Secure Data Recovery Services of April 2022 covering 998 full-time employees in the United States indicates that over half of the surveyed is against the supervision at work. The main reason is the fall of job satisfaction and almost 60% assessed the supervision as unethical. Many employees were not certain whether they are monitored at all; only 30% were informed about it and 53% indicated the lack of transparency provided by the managerial staff. The increase in the transparency could cover among others the possibility to have an insight into monitoring data, which is expected by 25% of respondents. Moreover, one third of respondents regarded the supervision as harmful for mental condition and 45% indicated the infringement of privacy. Additional consequences cover the fall of trust, growth of stress and fall in productivity. What is really interesting, over 25% of respondents declares taking actions in order to avoid monitoring including manipulation of work indicators or engaging office space in such a way that they pretend being active (McNutt 2024). The analysis of the research results presented above shows that both practices of monitoring employees' activity as well as using cybervetting may contribute to the creation of false picture of a given entity. These actions may be directed on shaping the employee's image in order to create the impression of greater loyalty and productivity.

employees' monitoring, (IV) cybervetting and information tools and artificial intelligence (Artificial Intelligence – AI).

This paper constitutes the continuity of the research presented in the publication *Recruitment in the Digitalization and AI Era – Awareness and Attitudes of HR Practitioners Towards Cybervetting* (Pytel-Kopczyńska, Niedbał, 2025). Both texts are based on the results of the same research survey but due to the amount of the material, the analyses were divided into two complementary parts. Whereas the first paper focused on the awareness and attitudes of HR specialists and recruiters towards cybervetting in the recruitment processes – including the information sources, perceived risks of privacy infringement and possibilities of using artificial intelligence tools – this paper presents the analyses referring to the use of cybervetting to monitor the employees' activity in the social media with the particular consideration of assessed benefits and dangers and the influence of seniority on the level of acceptance.

4. Cybervetting in employees' monitoring – results of empirical research and discussion

The research sample consisted of 46.8% of respondents (n = 53) with the over 20 years of experience in recruitment, 26.6% of surveyed – persons with the experience of 11-20 years (n = 30). 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 (n = 15 each). In the research sample 54.0% of respondents (n = 61) represented the companies of the industry and 46.0% of respondents (n = 52) were from the sector of non-financial services.

The analysis of responses given by HR managers and specialists in big companies to the questions referring to the declared level of support which cybervetting provides in the process of monitoring the employees indicates generally positive assessment of this practice (Table 1).

Almost two thirds of respondents (65.5%) claimed that cybervetting may constitute a significant support in employees' monitoring whereas 25.7% gave the assessment '5' (very high support) and 39.8% - assessment '4'. These results suggest that the majority of respondents notices the real potential of this practice concerning the supervision over employees, independently of the fact whether it is used in their organizations or not.

It is worth noticing that the assessment of the usefulness of cybervetting is growing with the seniority of employees. In the group of employees with the seniority 11-20 as many as 73.3% regarded that cybervetting is a clear support in monitoring and among the people working over 20 years this percentage amounted to 79.3%.

Table 1.
The level of support provided by cybervetting in the process of monitoring the employees

In which extent, in your opinion, cybervetting may support the process of monitoring employees?*	Seniority				Total
	Up to 5 years (n = 15)	6-10 years (n = 15)	11-20 years (n = 30)	Over 20 years (n = 53)	Number of indications of all the respondents (%)
Level of support	Number of indications in a given group of respondents (Number of indications in a given group of respondents, %)				
5	6 (40,00)	-	9 (30,00)	14 (26,42)	25,66
4	2 (13,33)	2 (13,33)	13 (43,33)	28 (52,83)	39,82
3	7 (46,67)	9 (60,00)	7 (23,33)	9 (16,98)	28,32
2	-	4 (26,67)	1 (3,34)	-	4,43
1	-	-	-	2 (3,77)	1,77

* Assessment in the scale from 1 (no support) to 5 (very high support).

Source: own study.

It shows that the growing conviction that digital tools mat be useful in keeping organizational standards and control of employees' behavior. In the group with the lowest job experience (up to 5 years), the assessments were also positive but less unequivocal – 53.3% of indications were included in the values 4 or 5. The clearly more ambivalent attitude was observed among the respondents with the work experience of 6 -10 years. In this group the moderate assessments were dominant (60.0% indications at level 3) and there was relatively high percentage of low assessments (26.7% of indications at level 2). Only 13.3% in this group selected the assessment at the high level (4), which may show the increased caution about the control tools among people who are engaged in the team management processes but do not participate in shaping staff policy at the strategic level. The extremely low assessments (at level 1) appeared only in the group with the greatest job experience (over 20 years), which may suggest that part of the experienced employees do not have trust to the methods of digital supervision, especially if they disagree with the regarded privacy standards or employee's autonomy. Despite this fact, the percentage of this assessment was marginal and did not affect the general picture of high level of acceptance.

Summing up and at the same time referring to the research question RQ1 – cybervetting is perceived by managers and HR specialists as a practice which may support the monitoring of employees in a significant way. The level of declared support is growing together with the respondents' seniority and the highest indicators of approval were noticed in the group with the longest seniority. Although there are some differences in the assessments, the general picture is clearly beneficial – cybervetting seems to be a useful tool, worth considering in the modern practices of organizational supervision.

The next stage of the survey research was an attempt to identify the respondents' opinions about the justification to use cybervetting to monitor the employees' activity in social media (e.g. to protect the company image). There may be a discrepancy between the assessment of the usefulness of this practice and its acceptance – the respondents may perceive it as useful and declare a high level of support in the scope of monitoring the employees but due to various aspects (e.g. the ethical ones connected with the privacy or biding law) they may not accept it and be ready to implement it in their organization. The obtained results are presented in Figure 1.

The respondents' attitudes towards using cybervetting to monitor employees indicate clear differentiation depending on the seniority. The clearest objection was expressed by the employees with the smallest work experience – as many as 80% of people in the group up to 5 years regarded this practice as completely unacceptable and the next 13% declared the response "rather no". It shows the strong sensitivity of this group in the matter of privacy and protection of personal life in the digital area. Only 7% of respondents in this group supported the use of cybervetting fully. A different approach took the respondents with the job experience of 6-10 years among whom over half (54%) expressed the acceptance for monitoring. However, the exceeding part of this group (47%) were for the limited form – used only in specified cases. It can be assumed that these people start joining the responsibility for the image of an organization with the need to maintain moderation in using the control measures.
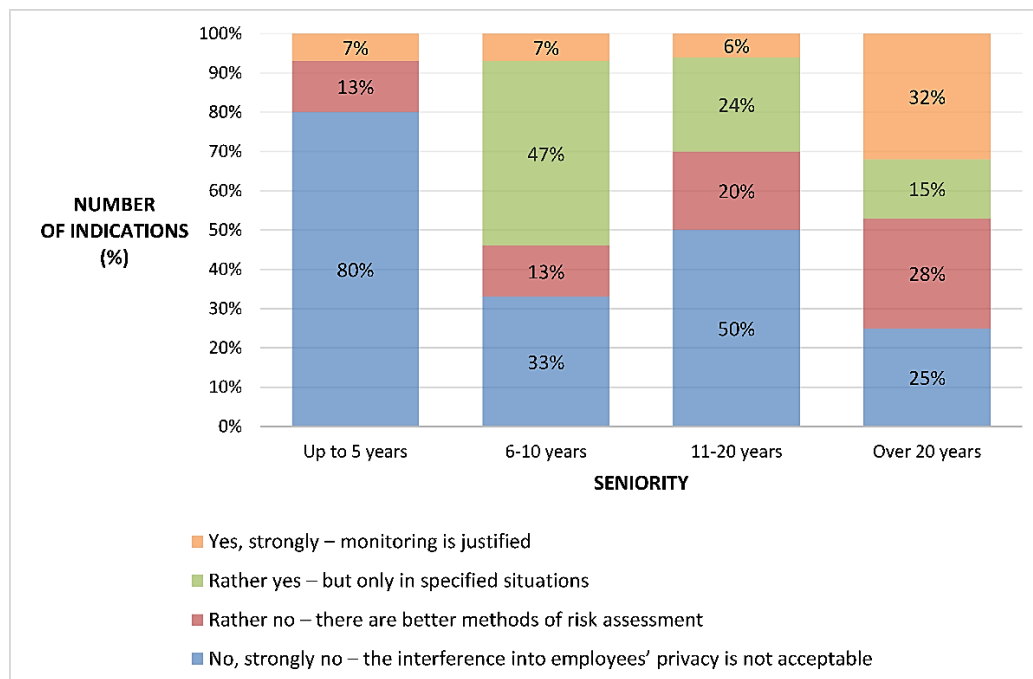

Figure 1. Monitoring the activity of employees in social media.

Source: own study.

Having worked for about ten years of seniority, in the group 11-20 years, the clear fall in acceptance is observed – as many as 70% of respondents rejected the use of cybervetting and half of them firmly. It may suggest stronger attachment to autonomy and greater experience in using alternative tools of the reputation risk assessment which do not interfere with a private

employees' activity directly. When it comes to employees with the work experience of over 20 years, the trend was partially reversed – almost one third (32%) declared the full support to the use of cybervetting and in total 47% were for any form of its implementation. Although some critical opinions appeared also in this group (28% of indications to the answer "rather no"), the increase in the readiness to accept this form of monitoring was visible. Probably it resulted from the stronger identification with the interest of an organization and greater awareness of risks connected with the employees' activity in the online public space.

Summing up, the opinions of managers and HR specialists in big companies about the importance of using cybervetting to monitor the employees are clearly polarized. Whereas, the people with low seniority clearly reject this practice and the employees with middle work experience show moderate acceptance, the ones with the longest work experience turn to be the most eager to regard cybervetting as the tool worth using. In the context of the research question RQ2 referring to the rate of acceptance of this practice, it is possible to notice that the acceptance of cybervetting among respondents is differentiated and conditional – depends on the seniority and the perception of relations between control and privacy. It is not possible to talk about the unanimous acceptance but about the segmentation of attitudes – from the clear objection through conditional acceptance to full support in selected professional groups.

The next two questions in the questionnaire referred to the identification of potential benefits (Figure 2) and risks (Figure 3) for the company arising from the use of cybervetting towards employees. Both had the form of multiple-choice questions (the respondents could choose more than one answer).
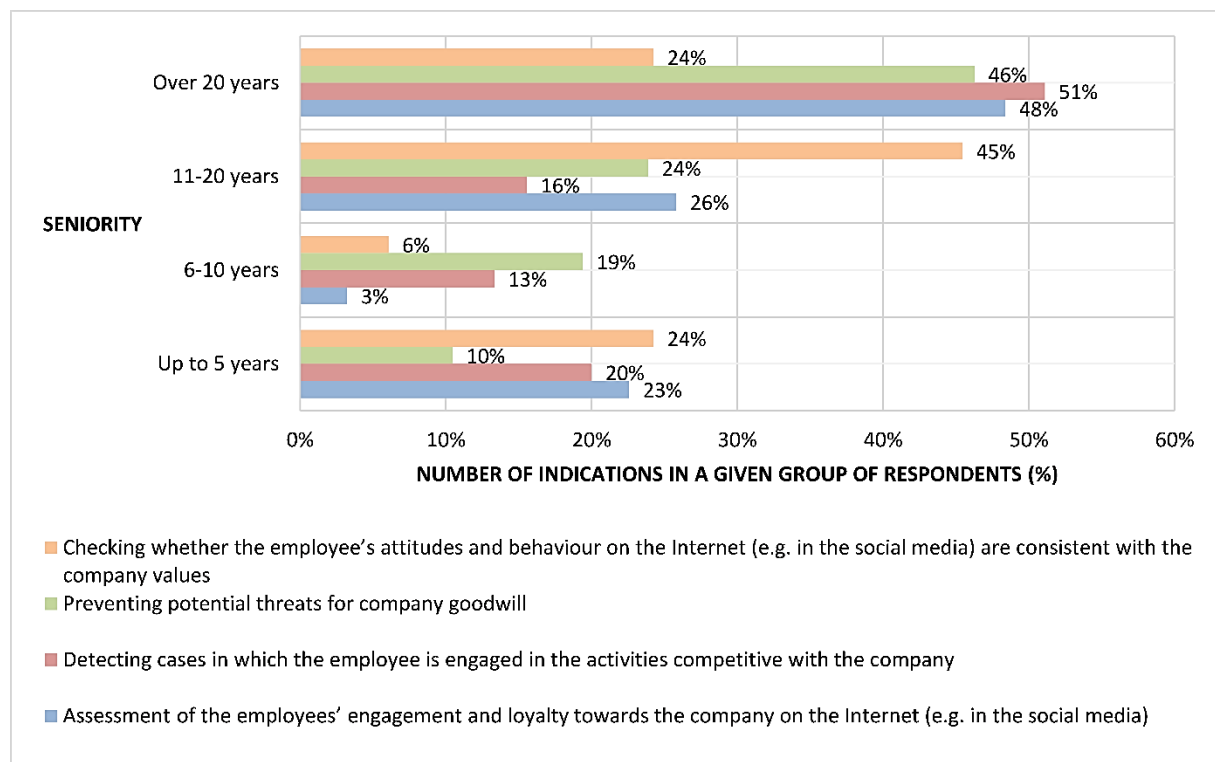

Figure 2. Benefits for the company arising from the use of cybervetting towards employees.

Source: own study.

The research results clearly show that the attitudes of managers and HR specialists towards the use of cybervetting to monitor the already employed workers are ambiguous – they see both particular benefits as well as significant threats arising from this practice (RQ3). On the one hand, cybervetting is perceived as a useful tool supporting the management in an organization, on the other hand - as an activity burdened with serious ethical, psychological and legal dangers.

When it comes to potential benefits, the possibility to prevent dangers for the company goodwill was the cybervetting function which the respondents chose most often. Such answer was chosen by 59.3% of all respondents whereas the highest percentage of indication was noticed in the group of respondents with the work experience over 20 years.
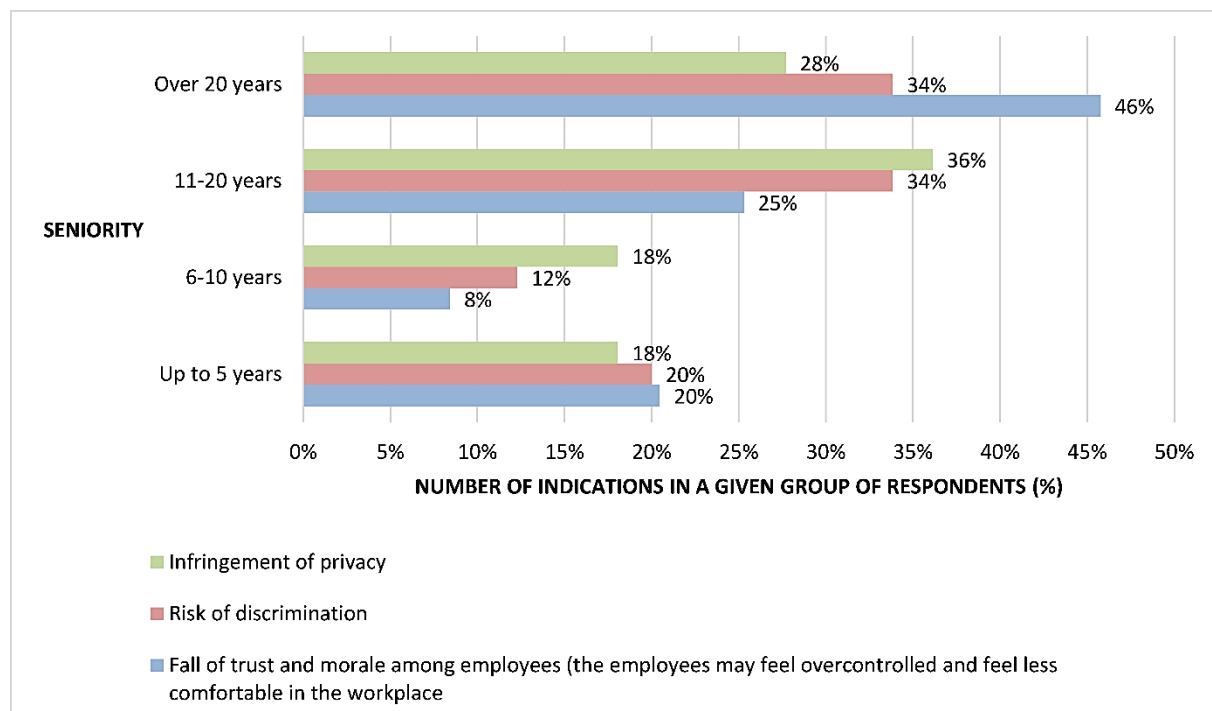

Figure 3. Dangers for companies arising from the use of cybervetting towards employees.
Source: own study.

This result suggests that people with the higher work experience appreciate the significance to protect the organization image in a particular way and are more sensitive to reputation risks connected with the employees' activity in the digital area. The possibility to identify the competitive actions taken by employees was the second most often selected aspect – it was indicated by 39.8% of respondents also mainly from the group with the longest work experience. Whereas 27.4% of respondents noticed the value of cybervetting in the assessment of employees' loyalty and engagement and 29.2% regarded that the analysis of activity on the network may be useful to check the cohesion of employee's attitudes with the organization values. The above results show that according to the respondents – especially the ones with the highest work experience -cybervetting may play the function of a tool supporting the control of organizational risks and cultural adaptation of the staff.

At the same time, the respondents' answers show the set of dangers which are clearly expressed. The worries which were indicated the most often referred to the infringement of privacy and fall in the morale among employees – both these dangers obtained 73.5% of indications. The infringement of privacy was often identified by people with the work experience of 11 – 20 years and over 20 years, which may indicate that they are sensitive to the border between professional and private life strongly. On the other hand, the fall in trust – interpreted as the possible effect of excessive control – was indicated by the respondents with the longest work experience. It may result from their attachment to the management model based on trust and autonomy. The risk of discrimination was the next significant danger (57.5% of indications. It was also perceived by the people with the longest work experience. It may show that they are more aware of the consequences arising from the subjective interpretation of contents published online and that they are more sensitive to the infringement of the rules of equal treatment.

Referring to the research question RQ3 formed in the introduction it is possible to claim that the respondents attribute to cybervetting towards employees both particular functions supporting the protection of the organization interests – especially when it comes to reputation, loyalty and consistence of attitudes with the company values – as well as significant dangers connected with the infringement of privacy, fall in trust and possibility of discrimination. In a consequence, cybervetting seems to be a tool with big potential but requiring a lot of caution, clear rules of use and sensitivity to ethical and social aspects.

The key element describing the rules of proceedings in the scope of cybervetting to monitor employees should be the standardized approach, performed both in the form of clearly formed internal use policies (Mikkelson, 2011) or by the set of consistent and transparent procedures to monitor the employees' online activity (Akbulut et al., 2024). The documents drawn up in this way should specify that the activity in the social media and online activities are monitored for business purposes and the improper use of digital tools may lead to disciplinary consequences including the dismissal from work. These documents should also specify which disclosures of confidential information referring to the employer are allowed and which are prohibited, should also forbid publishing false information about the employer, co-workers or customers. They should also indicate the person responsible in the organization for the issues connected with the use of social media and remind the employees about the necessity to maintain common sense and personal responsibility for the published contents. The organization should set boundaries of monitoring guaranteeing clearly that it is consistent with the binding provisions of law, justified, proportional, transparent and respects employees' rights (Mikkelson, 2011). These are the actions in order to eliminate or minimize dangers and generated numerous risks (prejudice, discrimination, infringement of privacy, infringements of labor agreement) referring to the practices of cybervetting towards employees of an organization.

5. Conclusion

Cybervetting constitutes a significant element of HR practices at present. The conducted research confirms that it is perceived by managers and HR specialists as a tool with big potential supporting the supervision over employees – especially in such areas as the protection of company goodwill, identification of risk behavior and assessment of the cultural adaptation. At the same time, the respondents express clearly dangers connected with this practice and in particular the infringement of privacy, fall of trust in the organization and risk of discrimination. The attitudes towards cybervetting turned out to be strongly differentiated depending on the seniority which may show the influence of work experience on the way of perceiving the border of available control.

The obtained results provide important indications for the management practice; however, they should be interpreted with the consideration of several important limitations. Firstly, the research was of a pilot nature and covered only big companies from two provinces (Lodz and Silesia), which limits the possibility to generalize the results to other regions. Secondly, the use of CAWI method may affect the composition of the sample – most probably the representant who were more active digitally gave their responses. Thirdly, although the differentiation of the seniority was considered, the impact of other significant factors such as taken position, level of responsibility in the organizational structure or the specific of company culture was not analyzed in this stage.

Taking the above into consideration, the presented results should be regarded as the preliminary picture of attitudes towards cybervetting which requires further deepened research – both quantitative as well as qualitative ones covering among others in-depth interviews and case studies.

References

1. Akbulut, Y., Sen, I.E.Y., Sahin, Y.L. (2024). Employer and employee perceptions of cybervetting as a selection method. *International Journal of Selection and Assessement*, *Vol. 32, Iss. 2*, pp. 292-308, doi: 10.1111/ijsa.12463

2. Burlee, T.J. (2024). Study Reveals the Prevalence and Impact of Work Surveillance. *Secure Data Recovery, Jun 10, 2024*. Retrieved from: https://www.securedatarecovery.com/blog/work-surveillance-prevalence-impact, 20.06.2025.

3. Leonardi, P.M. (2021). COVID-19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work. *Journal of Management Studies, Vol. 58, Iss. 1*, pp. 249-253, doi: 10.1111/joms.12648

4. Mateescu, A., Nguyen, A. (2019). Algorithmic Management in the Workplace. *Data & Society*, pp. 1-15. Retrieved from: https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf, 20.06.2025.

5. McNutt, K. (2024). Study finds 40% of employees suspect employer surveillance. *The Journal Record, September*. Retrieved from: https://journalrecord.com/2024/09/04/study-finds-40-of-employees-suspect-employer-surveillance/, 08.09.2025.

6. Mikkelson, K. (2011). Cybervetting and Monitoring Employees' Online Activities: Assessing the Legal Risks for Employers. *American Bar Association, Vol. 19, Iss. 2*. Retrieved from: https://www.americanbar.org/content/dam/aba/publications/public_lawyer/Cybervetting_and_Monitoring_Employees_PLS10.pdf, 20.06.2025

7. *Monitoring Employee Social Media Activity at Work*. Retrieved from: https://www.thehartford.com/business-insurance/strategy/workplace-privacy/social-media-monitoring, 04.09.2025.

8. Pytel-Kopczyńska, M., Niedbał, R. (2025). Recruitment in the digitalization and AI era – awareness and attitudes of HR practitioners towards cybervetting. *Scientific Papers of Silesian University of Technology – Organization and Management Series*, *Vol. 228*, pp. 531-542, doi: 10.29119/1641-3466.2025.228.30

9. Rahat, H., Nadeem, S. (2025). Social media as a workplace panopticon: The development and validation of social media monitoring by workplace contacts scale. *PLoS ONE, Vol. 20, Iss. 3, e0319429,* doi:10.1371/ journal.pone.0319429

10. *Social Media and News Fact Sheet*. Retrieved from: https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/, 27.08.2025.

11. Vitak, J., Zimmer, M. (2023). Surveillance and the future of work: exploring employees' attitudes toward monitoring in a post-COVID workplace. *Journal of Computer-Mediated Communication, Vol. 28, Iss. 4, zmad007,* doi:10.1093/jcmc/zmad007

12. Wartzman, R. (2019). *Workplace tracking is growing fast. Most workers don't seem very concerned.* Retrieved from: https://www.fastcompany.com/90318167/workplace-tracking-is-growing-fast-most-workers-dont-seem-very-concerned, 20.06. 2025.