

Privacy or Self-Censorship? Coping Strategies of Young Polish Job Candidates under Cybervetting

Ilona Pawełoszek*, Rafał Niedbał**

*Department of Management Information Systems, Czestochowa University of Technology, Częstochowa, Poland

**Department of Management Information Systems, Czestochowa University of Technology, Częstochowa, Poland; E-mail: rafal.niedbal@pcz.pl

Abstract **Purpose.** The article investigates how young adults in Poland (aged 18–30) adjust their self-presentation on social media in response to cybervetting. It compares two strategies—preventive profile privacy settings and reactive self-censorship—across professional and general platforms. It also explores whether the amount of time spent online correlates with the intensity of these actions.

Design/methodology/approach. An online survey (conducted March–April 2025) was completed by 126 respondents. Ordinal scales measured the level of profile privacy and frequency of self-censorship. Due to significant deviations from normal distribution, the Mann–Whitney U test was used. The relationship between time spent online and strategies was assessed using Spearman's correlation.

Findings. Users of professional platforms reported stricter privacy settings; self-censorship did not differ. Time spent online was not related to self-censorship but was slightly negatively correlated with privacy settings.

Research limitations/implications. Self-reported measures, simplified platform classification, non-random sampling, and lack of demographic subgroup analysis limit generalizability.

Originality/value. This is one of the first studies in Poland to compare preventive and reactive strategies toward cybervetting across platform types, combining impression management and context collapse theories. It shows that platform type, versus time online, drives privacy choices.

Keywords cybervetting, social media, talent acquisition, digital reputation management, online recruitment, technological transformation of HR.

JEL codes J24, M54, M15, O33

INTRODUCTION

With the widespread use of social media, the boundaries between private and professional life are becoming increasingly blurred. Content shared on platforms such as Facebook, LinkedIn, TikTok, or Instagram is increasingly drawing the attention of potential employers. This phenomenon, known as cybervetting, refers to the systematic use of social media content to assess job candidates during recruitment processes (Berkelaar, 2014; Jacobson & Gruzd, 2020). The use of new communication channels—especially social media—in organizations' interactions with their environment has been gaining growing attention from researchers (Zarzycka, Krasodomska & Dobija, 2021). Public activity in these channels has thus become one of the first and most easily accessible sources of information for recruiters engaging in cybervetting.

Although this practice raises numerous ethical concerns, it is becoming the “new normal” in the labor market—particularly in the case of young adults, who actively use multiple platforms and are often not fully aware of the consequences of their digital presence. However, even limited risk awareness tends to increase significantly once the prospect of employment becomes real (e.g., receiving an invitation to a job interview or advancing to the next stage of recruitment). As a result, candidates begin to perceive their social media profiles as publicly available curricula vitae and—often on an ad hoc basis—transform previously spontaneous online practices into a more strategic approach to content visibility management.

In response to this phenomenon, candidates adopt various coping strategies. Previous research has primarily focused on two key mechanisms: restricting profile visibility and selectively self-censoring content (Roulin and Levashina, 2016; Vitak and Kim, 2014). At the same time, new forms of both defensive and offensive behavior are emerging – from actively building a personal brand (so-called selfie-branding) to using algospeak to bypass automated moderation systems (Steen, Klug, & Yurechko, 2023).

*Corresponding author

Despite the growing number of publications, there is still a lack of studies that combine a broad theoretical context with an empirical analysis of specific self-presentation strategies employed by users across different types of social media platforms. This article aims to fill that gap by combining a review of recent research with an analysis of the behaviors of young adults in Poland ($N = 126$), focusing on profile visibility management and self-censorship. In particular, we are interested in how the type of social media platform—professional or general-purpose—affects the coping strategy adopted. The article also examines the relationship between the intensity of social media use and the tendency to hide or modify content.

The study addresses the following research questions:

RQ1. Does the type of social media platform influence candidates' coping strategies, such as profile privacy settings and self-censorship behavior?

RQ2. Is the self-reported daily time spent on social media (in hours) significantly related to (a) profile privacy level and (b) the frequency of content self-censorship—two main coping strategies in response to cybervetting?

This article attempts to integrate a current literature review with empirical data analysis to shed light on the diverse coping strategies young adults employ in response to cybervetting and their potential implications for employer branding practices and ethical considerations in recruitment.

LITERATURE REVIEW ON CANDIDATE STRATEGIES AND EMPLOYER PRACTICES IN THE CONTEXT OF CYBERVETTING

Candidate Coping Strategies in Response to Cybervetting

Candidates' strategies aimed at minimizing the risks associated with cybervetting primarily involve two complementary mechanisms. On the one hand, these strategies are rooted in Erving Goffman's classical theory of impression management; on the other, they align with the concept of context collapse described in the literature, understood as the necessity of simultaneous self-presentation to heterogeneous online audiences (Loh & Walsh, 2021).

The first mechanism is content self-censorship, which refers to reactive "cleaning" of one's profile by editing or deleting materials that might negatively affect one's professional image. A survey by *JDP* (2019) found that nearly half of respondents (46%) admitted to entering their own name into a search engine. Based on the results, they often decided to further limit the visibility of their social media profiles. The highest number of potentially compromising posts was found on Facebook.

Adjusting one's social media presence is not always about concealing information. In the context of shaping a professional image, 25% of respondents declared that they actively presented themselves on social media in a way intended to attract potential employers, through likes, publishing relevant content, or following industry-related materials.

Stoughton, Thompson and Meade (2013) found that a lower level of agreeableness significantly correlates with a higher frequency of *badmouthing* posts (i.e., critical comments about employers and coworkers). Meanwhile, posts related to substance use may be interpreted as manifestations of extraversion in online environments. From a human resources perspective, such content is considered potentially risky from the standpoint of recruiters.

The second mechanism, privacy settings, serves a preventive function, enabling users to consciously manage access to their information by limiting profile visibility or selectively sharing content. These actions align with the concept of boundary regulation, which posits that individuals control the disclosure of personal information by shaping the boundaries between private and public spheres in digital environments (Vitak and Kim, 2014). The tendency to use advanced privacy settings is strongly associated with digital competencies; Hargittai and Litt (2013) found that individuals with higher levels of internet skills are more likely to use extended visibility configuration options than those with lower technical proficiency.

In practice, both types of behavior – preventive and reactive – can be understood as elements of the online impression management cycle (Roulin and Levashina, 2016). A candidate first perceives signals suggesting that an employer may be reviewing their social media activity and subsequently decides either to post only neutral or professional content, or to act freely and later remove or restrict access to potentially undesirable posts. The choice of a particular approach depends, among other factors, on the nature of the platform. For example, content that disappears automatically after 24 hours may seem safer than content that remains permanently visible—as well as on personality traits, digital literacy, and the transparency of the organization's recruitment procedures.

Types of Social Media Platforms and Candidates' Self-Presentation Strategies

Previous research findings suggest a clear distinction: professionally oriented platforms (e.g., LinkedIn) tend to encourage users to proactively manage their privacy settings in advance (a preventive strategy), while general-purpose and entertainment

platforms (e.g., Facebook, YouTube) are more often associated with last-minute “clean-ups” of profiles just before submitting a job application (a reactive strategy). In turn, on platforms oriented toward entertainment and mass reach (e.g., TikTok, Instagram), users often focus on creatively building their visibility, aiming for viral reach [1]. This introduces a third approach, the exposure strategy.

Differences in privacy strategies stem from the nature of each platform. Services with a strong professional focus, such as LinkedIn, promote proactive image management and the accumulation of digital career capital – a resource that increases a candidate’s perceived value in the labor market (Berkelaar & Buzzanell, 2015). As a result, users carefully curate professional content rather than relying on later self-censorship.

A different pattern emerges on platforms dominated by entertainment content, such as Facebook or TikTok, where coping behaviors are more often reactive and occur only after content has been posted. A study by Roulin and Liu (2023), which examined three popular platforms in China (WeChat, QQ, and Sina Weibo), found that candidates’ attitudes toward cybervetting were negative across all platforms, although least negative for WeChat. These attitudes were linked to users’ content-sharing habits—those who posted more frequently had more positive attitudes. In addition, individual differences were observed: women expressed more negative attitudes, while extraverted individuals showed more positive ones.

A 2025 report by Zety (Escalera, 2025) indicates that 46% of Generation Z representatives obtained a job or internship thanks to content they published on TikTok. The authors of the report also emphasize that, for this generation, social media serves as a key space for establishing professional connections. This trend is further supported by Steinhardt (2024), who found that 41% of Gen Z respondents had made career decisions based on advice from TikTok, and 15% had received a job offer through the app. Instagram, in turn, supports what is known as selfie-branding [2]. Qiu, Lu, Yang, Qu and Zhu (2015), in their analysis of selfies posted on the Sina Weibo platform, found that specific visual features of the photos, even if unintentional, can reveal personality traits of the users. For example, higher levels of agreeableness were significantly associated with a lower likelihood of displaying posed facial expressions with pouted lips (commonly referred to as the duck face), suggesting a preference for a more polite and restrained self-presentation.

Subtle techniques of concealing content are also gaining traction, such as deliberate misspellings or the creation of neologisms (referred to as *algospeak*) that are intended to make it harder for algorithms and recruiters to detect potentially problematic material (Steen et al., 2023).

The boundaries between the three strategies—reactive, preventive, and exposure-oriented—are becoming increasingly blurred, as many platforms now combine multiple functions. Nevertheless, whether a platform is primarily used for professional networking, social interactions, or gaining reach through algorithmic amplification still largely determines which strategy a candidate adopts.

Employer Practices in Assessing Candidates via Social Media

According to Ruggs, Walker, Blanchard and Gur (2016), the growing use of social media in talent acquisition processes—from attracting candidates to initial screening—can facilitate the work of recruiters and enhance their understanding of applicants. However, it may also reinforce biases, particularly against individuals from minority groups. In the context of cybervetting, this means that informal profile reviews require transparent and fair criteria to avoid excluding valuable candidates.

Hoover, Rupp and McCauley (2025), in their article “Cybervetting Best Practices: An Integrative Framework for Developing, Validating, and Implementing Social Media Assessment for Personnel Selection,” offer guidelines for conducting reliable cybervetting. The authors adopt a technology-as-designed perspective, emphasizing that the platform’s architecture and professional character—not merely the content of a user’s profile—determine its suitability for candidate evaluation. They therefore recommend using highly structured and professional platforms (e.g., LinkedIn) and assessing only knowledge, skills, abilities (KSAs), and other characteristics relevant to the job position.

Tews, Stafford and Kudler (2019) found that three negative content categories in Facebook profiles—self-absorption, opinionatedness, and references to alcohol and drug use—significantly lowered candidate ratings. Among these, self-absorption had the strongest negative effect, likely because it suggests poor teamwork ability. Additionally, older recruiters tended to evaluate controversial opinions and substance-related content more harshly.

Additional context is provided by the study of Zhang et al. (2020), which demonstrated that Facebook profiles of job seekers often contain demographic information that, under U.S. labor law, should not be considered in hiring decisions (e.g., age, ethnicity, religion), as well as other non-job-related details such as sexual orientation or marital status. Various categories of content shared on social media—from demographic indicators and routinely assessed attributes (education, training, skills) to materials potentially viewed as problematic by employers (e.g., profanity, references to sexual behavior)—have been found to correlate with recruiters’ judgments about a candidate’s employability.

Walrave, Van Ouytsel, Diederer and Ponnet (2022) conducted interviews with HR managers from both the private and public sectors to investigate actual cybervetting practices. Respondents reported reviewing social media primarily to identify inconsistencies between online information and the content of CVs. Particular attention was paid to photos, especially those depicting private life, alcohol consumption, or the candidate's appearance. Images shared by third parties, rather than self-posted by the candidate, were perceived as more credible. In public institutions, alignment of political views with the role was occasionally mentioned as an additional criterion—something that was not observed in private companies.

An interview-based study with recruiters in Sweden demonstrated that the so-called “professional talk”—a discourse emphasizing objectivity and expert knowledge—serves to legitimize the practice of cybervetting (Backman & Hedenus, 2023). The interviewees relied on two recurring justificatory frames for reviewing candidates' social media profiles. First, they invoked the notion of “available information”, arguing that publicly accessible content may be used both legally and ethically, since it is the user's responsibility to manage what is published online. Second, they referred to the “relevant information” frame, asserting that they only consider content deemed professionally meaningful—such as indicators of unprofessional behavior. As a result, the boundary between the private and public spheres shifts in favor of the employer: privacy is reframed as the user's responsibility rather than a right. The authors emphasize that this rhetorical strategy is used by recruiters to normalize and defend cybervetting as a legitimate and professional practice.

Research on social media assessment (SMA) indicates that this method achieves reliability only when fully structured—that is, when it includes a clearly defined purpose, predefined competencies, standardized content coding criteria, and evaluator training, all elements familiar from structured interviews. Hartwell, Harrison, Chauhan, Levashina and Campion (2022) observe that although SMA is becoming a common selection tool, it is most often conducted informally, which undermines its reliability and validity and raises the risk of legal and ethical issues.

Similar conclusions are presented in Vosen's (2021) literature review: the lack of transparent rules intensifies subjective feelings of privacy violation and lowers candidates' acceptance of the selection process. The author emphasizes that structured elements—clear criteria, procedural consistency, and standardized rating scales—limit arbitrariness and enhance candidates' perceptions of fairness. Although most existing studies are theoretical or review-based, available evidence suggests that structuring SMA improves its reliability, validity, and user acceptance.

Artificial intelligence (AI) algorithms can also be applied in recruitment processes. However, according to Da Motta Veiga and Figueroa-Armijosa (2022), both candidates and recruiters generally perceive AI-driven social media analysis as unethical. In general, individual traits deemed undesirable or inappropriate by the algorithm, based solely on historical data, may lead to the disqualification of even highly competent candidates.

Nevertheless, the authors conditionally allow the use of AI for analyzing candidates' social media activity if the data is processed in an aggregated manner—for example, using a scoring system that evaluates overall fit with the role and organization, rather than searching for so-called “red flags” [3]. This approach would allow for more objective comparisons between applicants.

The authors also highlight two serious concerns related to AI in recruitment: (1) AI is created by humans, who are inherently biased, and the organizations they represent act in pursuit of their own goals and profits. (2) How authentic are candidates on social media in the first place?

Challenges Related to the Use of Technology in Cybervetting

A powerful influence mechanism used by social media platforms is the direct removal of unwanted content or users. According to Zaman and Chen (2024), a more extreme form of control over collective opinions over time is the phenomenon known as shadow banning – the stealthy restriction of a post's reach by platforms without notifying the user. The strength of this mechanism lies in the fact that it is nearly impossible to detect, even by policymakers or software engineering experts.

Previous research on candidates' coping behaviors has mainly focused on binary indicators (e.g., “post deleted – yes/no” or “profile private vs. public”). Still, an increasing number of examples show that these practices often take much subtler forms. Analyses of shadow banning reveal that some candidates attempt to diagnose their own visibility (e.g., by using additional test accounts) and modify hashtags, emojis, or keywords to bypass algorithmic filters. A study conducted by a team at the University of Michigan (Wadley, 2024), based on surveys and interviews with marginalized groups, provides a qualitative account of this practice—emphasizing that decreased visibility is often perceived as a form of systemic silencing.

The most contentious research gaps today concern the ethical and legal issues associated with the increasing use of AI tools in cybervetting. Several commercial solutions have already entered the market and are becoming subjects of empirical analysis. One such example is Yoono, a platform for fast, “intelligent” screening of candidates' public data [4]. The application processes only publicly available content and offers anonymized results, claiming full compliance with GDPR regulations (Yoono, 2024). A study by Hukkeri and Pol (2025) shows that the use of AI combined with social media data can improve the efficiency of pre-selection, shortening time-to-hire and enhancing candidate-job fit. However, the authors also identify significant challenges:

reduced human involvement in decision-making, the risk of algorithmic bias, and low procedural transparency. They emphasize the need for clear, legal, and audit frameworks to build candidate trust and safeguard privacy.

Similar conclusions are presented by Lacmanović and Skare (2025), who argue that systematic auditing of bias in recruitment algorithms supports algorithmic fairness and helps prevent discriminatory outcomes in hiring.

The importance of transparency in AI-based recruitment has also been highlighted by the United States Department of Justice (DOJ) and the Equal Employment Opportunity Commission (EEOC). Both institutions recommend that employers inform candidates when algorithms are being used and ensure the possibility of human appeal, especially in cases involving individuals with disabilities (Johnson, 2022).

In the European Union, Article 6 of the AI Act classifies AI tools used in recruitment—such as résumé scanners, candidate ranking systems, and algorithms that automatically target job ads to specific user groups—as high-risk systems (*Regulation (EU) 2024/1689, Art. 6*). The regulation on the use of AI in recruitment systems is scheduled to enter into force in 2026. From that point on, providers of AI systems used in recruitment, candidate selection, and workforce management will be required to register their systems in a centralized EU database maintained by the European Commission before placing them on the market or putting them into use. Additionally, they will be obliged to implement a systematic and documented risk management system throughout the AI system's lifecycle, identifying, analyzing, and mitigating potential risks related to safety, algorithmic errors, and bias, among others.

SELF-PRESENTATION STRATEGIES UNDER CYBERVETTING: SURVEY RESULTS

Research Method

The study employed a quantitative approach and was conducted via an online survey distributed among students from various universities in Poland. The sample consisted of 126 complete responses, collected on a voluntary and purposive basis between March and April 2025. Respondents represented different levels of higher education (engineering, bachelor's, and master's programs) and various academic disciplines. However, no subgroup analyses were conducted based on these factors. Participants were social media users aged 18 to 30, recruited primarily through university networks and social media channels. The questionnaire consisted of 18 questions in total, but this analysis focused on selected variables from the following four items:

- Social media platforms used (up to three most frequently used; Question 10).
- Profile privacy level (Question 17).
- Tendency to self-censor content (Question 18).
- Declared daily time spent on social media (in hours; Question 16).

Based on the responses, two main dependent variables were constructed:

- Profile privacy level (scale: 1 = private, 2 = partially private, 3 = public).
- Level of content self-censorship (scale: 1 = never, 2 = rarely, 3 = sometimes, 4 = often).

Due to the ordinal nature of the variables and significant deviations from normal distribution (Shapiro–Wilk test: $p < 0.000001$), non-parametric statistical methods were applied. The Mann–Whitney U test was used for group comparisons, while Spearman's rank correlation was used to analyze the relationship between time spent on social media and the levels of privacy and self-censorship. The study was anonymous, and data was analyzed in aggregate form without any personally identifiable information.

Analysis of Candidates' Coping Behaviors and the Type of Social Media Used

The analysis focused on two survey questions reflecting candidates' coping strategies in the face of potential cybervetting—that is, the possibility of recruiters searching their online presence.

Dependent variable 1: Content self-censorship

Question 18: *"How often do you edit or delete content that could look bad in front of an employer?"*

Scale: 1 = "Never", 2 = "Rarely", 3 = "Sometimes", 4 = "Often"

This variable is interpreted as an indicator of a reactive coping strategy in response to potential recruitment-related surveillance.

Dependent variable 2: Profile privacy

Question 17: *"Is your main personal profile currently..."*

Scale: 1 = "Private (visible only to friends)", 2 = "Partially private", 3 = "Fully public"

This variable reflects the degree of profile visibility management and intentional self-presentation.

To enable clearer comparisons of coping strategies, each respondent was assigned to one dominant type of social media platform. The classification was based on a functional hierarchy: individuals who reported using at least one professionally oriented platform (LinkedIn, X/Twitter, industry-specific forums) were classified into the professional platform group ($n = 44$). All other respondents—those who used only platforms such as TikTok, Instagram, Facebook, or YouTube—were assigned to the general-purpose platform group ($n = 82$), characterized by a more casual, social, and entertainment-oriented profile.

Due to the ordinal nature of the variables and the lack of normal distribution (confirmed by the Shapiro–Wilk test), the Mann–Whitney U test was applied to compare the two independent groups.

The results showed that users of professional platforms reported significantly higher levels of profile privacy than users of general-purpose platforms ($U = 1354$, $p = 0.011$). This finding supports the assumption that individuals active on professional platforms are more likely to employ preventive strategies, proactively restricting access to their information.

In contrast, no significant difference was found between the groups regarding content self-censorship ($U = 1698$, $p = 0.565$). This may suggest that behaviors such as editing or deleting posts are not directly related to the nature of the platform used but instead represent a general coping response to the prospect of being evaluated.

To illustrate the findings, boxplots were used to compare the distributions of responses, presented separately for each variable (Figure 1). Due to differences in response scale length (1–3 for profile privacy, 1–4 for self-censorship), the variables were plotted on separate axes to maintain interpretive clarity.

In addition, Table 1 presents the mean values of both variables in the two groups along with the statistical test results.

It is important to note that lower values on the privacy scale indicate higher levels of profile protection. Thus, the results show that users of professional platforms exhibit greater attention to privacy, whereas users of general-purpose platforms tend to keep their profiles more open.

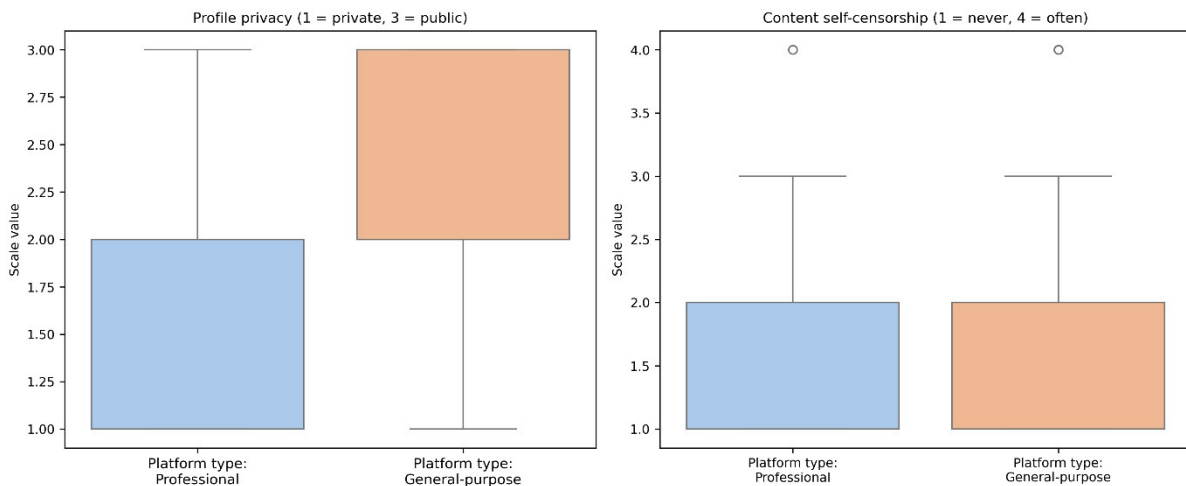


Figure 1. Comparison of coping behaviors (profile privacy and self-censorship) by type of social media platform used

Source: Own elaboration

Table 1. Average levels of profile privacy and self-censorship among users of professional vs. general-purpose platforms

Comparison Type	Variable	Mean – Professional Group	Mean – General-Purpose Group	p-value	Interpretation
Professional vs. General	Profile Privacy	1.77	2.10	0.011	Professional group -greater attention to privacy
Professional vs. General	Content Self-Censorship	1.82	1.90	0.565	No significant difference

Source: Own elaboration

These results also allow for a more in-depth interpretation of candidate behaviors through the lens of impression management and self-presentation theory. Users of professional platforms (e.g., LinkedIn, X, industry forums) report higher levels of profile privacy, which may reflect a greater concern with controlling their professional image. At the same time, they report less frequent content editing or deletion, suggesting a preventive strategy, setting high privacy levels in advance rather than reacting to specific threats. This indicates a more deliberate self-presentation strategy: these users publish content with their professional identity in mind, rather than correcting it retrospectively. This may indicate a higher level of impression management awareness in digital spaces, aligning with Goffman's theory and the concept of context collapse (Loh & Walsh, 2021).

By contrast, individuals who do not use professional platforms tend to have more open profiles but report slightly more frequent self-censorship behaviors, which may reflect a reactive coping strategy in response to perceived digital surveillance.

Conclusions from the Analysis of Coping Behaviors Related to Cybervetting

Based on the conducted analysis, the following conclusions can be drawn:

- 1 Users of professional platforms (LinkedIn, X/Twitter, industry-specific forums) more frequently maintain private profiles compared to users of general-purpose social media platforms. This may indicate a higher level of awareness regarding image management in a professional context. The difference was statistically significant ($p = 0.011$).
- 2 In terms of self-censorship—understood as deleting or modifying content that could negatively affect a candidate's evaluation—no significant differences were observed between the examined groups. This may suggest that such behavior is common and not necessarily dependent on the type of social media platform used.

Since respondents could use multiple types of platforms simultaneously, each person was assigned to one dominant category (professional or general-purpose), allowing for clearer statistical comparisons. It is also worth noting that the declared level of profile privacy may refer to multiple platforms simultaneously, and its interpretation depends on the technical capabilities of each service (e.g., limited privacy settings on LinkedIn).



Figure 2. Self-censorship vs. profile privacy level on social media platforms

Source: Own elaboration

To better visualize the relationship between profile privacy and the tendency to self-censor, a heatmap was prepared (Figure 2). The chart shows the number of respondents in each combination of the two variable categories. Two distinct patterns are noticeable:

- Among individuals with fully private profiles, the most common responses regarding self-censorship are “never” and “rarely.”
- None of the individuals with fully public profiles declared that they “often” edit or delete their posts.

This may suggest two contrasting approaches to online presence management: a preventive strategy (high privacy, lower need for self-censorship) and a full exposure strategy (low privacy and little to no post hoc correction).

Relationship Between Time Spent on Social Media and Levels of Self-Censorship and Profile Privacy

In the next stage of the analysis, we examined whether there is a relationship between the time spent on social media and users' engagement in protective behaviors, such as editing or deleting content that could be perceived negatively by potential employers (self-censorship), as well as their level of profile privacy.

The variable “time spent on social media” was coded as the number of hours declared by respondents. Before conducting correlation analysis, the Shapiro-Wilk test was used to assess the normality of this variable's distribution. The results were as follows:

- Test statistic = 0.861
- p-value < 0.000000002

Such a low p-value indicates a significant deviation from normal distribution. Therefore, to avoid assuming normality, Spearman's rank correlation was applied—a non-parametric method appropriate for data that is not normally distributed.

Spearman correlation results:

- Correlation between time spent on social media and level of self-censorship: $\rho = 0.04$, $p = 0.64$
- Correlation between time spent on social media and profile privacy: $\rho = -0.15$, $p = 0.05$

This means that no significant relationship was found between social media usage intensity and the tendency to self-censor. However, in the case of profile privacy, a weak negative correlation was observed at the threshold of statistical significance—the more time respondents spend on social media, the less private their profiles tend to be (Figure 3).

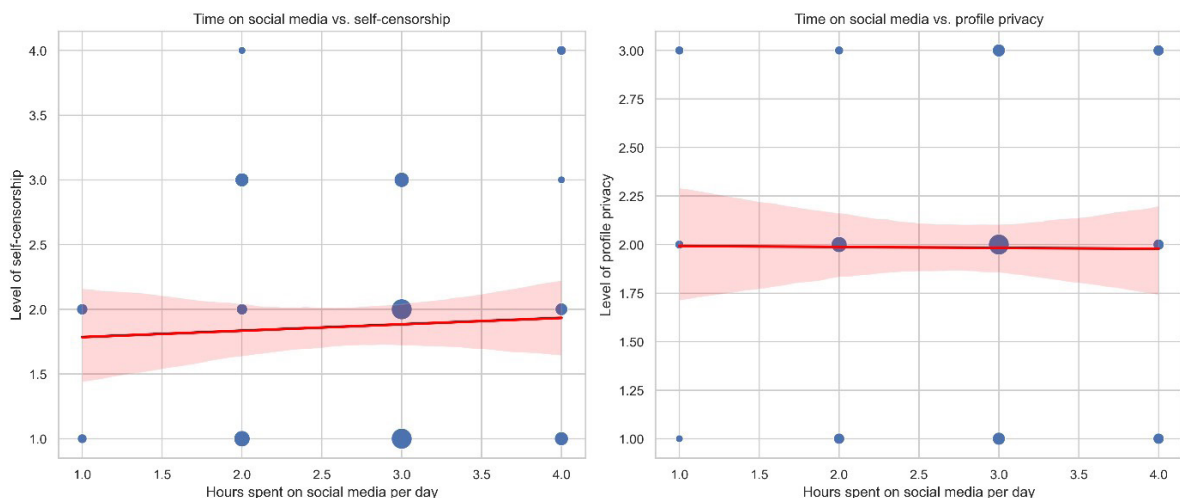


Figure 3. Relationship between time spent on social media and profile privacy, and between time spent on social media and level of self-censorship

Source: Own elaboration

A trend line has been added for illustration purposes only. Although linear regression was used for visualization, the actual analysis was performed using Spearman's correlation.

The scatter plots with the trend lines confirm the lack of significant relationships—the lines are nearly flat, indicating no clear connection between time spent on social media and levels of either self-censorship or profile privacy. The shaded area around each line represents the 95% confidence interval, illustrating the uncertainty of the trend estimate. The size of each point reflects the number of respondents who selected a given combination of values.

DISCUSSION

This article posed two research questions:

RQ1: Does the type of social media platform differentiate candidates' coping strategies, such as profile privacy level and tendency to self-censor?

RQ2: Is the declared daily time spent on social media (in hours) significantly related to (a) profile privacy level and (b) the declared frequency of self-censorship—the two main coping strategies in response to cybervetting?

In regard to the first question (RQ1), the results confirm that the type of social media platform used affects how young adults manage their online presence in the context of potential cybervetting. In particular, users of professional platforms (LinkedIn, X/Twitter, industry forums) reported higher levels of profile privacy, which suggests the use of a preventive strategy—consciously shaping the availability of information prior to publication.

In contrast, users of general-purpose social platforms (including entertainment and general-use services such as TikTok, Instagram, Facebook, or YouTube) did not significantly differ in terms of privacy or self-censorship. This may indicate a lower awareness of digital surveillance risks or reflect different usage patterns of those platforms.

The lack of significant differences in self-censorship levels between the two groups suggests that reactive coping strategies, such as editing or deleting content, are commonly employed regardless of platform function. This finding aligns with earlier research indicating that young candidates often engage in content management only in response to specific recruitment situations (JDP, 2019; Roulin & Levashina, 2016).

Regarding the second research question (RQ2)—the relationship between declared daily time spent on social media and the use of coping strategies—the analysis revealed no significant relationships with respect to self-censorship, and a weak negative correlation at the significance threshold in the case of profile privacy settings ($p = -0.15$, $p = 0.05$). This means that individuals who spend more time on social media reported slightly less frequent use of privacy restrictions on their profiles.

Although this effect is small, it may suggest a tendency toward greater openness among heavy users, perhaps due to habituation to constant online presence, increased comfort with public exposure, or a lower perception of cybervetting-related risks.

In the context of candidate selection based on social media content, several practical implications emerge from both the literature and the collected data. It can be inferred that candidates should not only remove photos depicting alcohol consumption or other behavior related to psychoactive substances, but also excessively egocentric or highly ideological posts, which—as previous research shows—negatively affect evaluations of professional suitability (Tews et al., 2019).

From the employer's perspective, standardizing content evaluation criteria and training individuals who conduct the screening may help reduce subjectivity and minimize the risk of bias related, for example, to the candidate's age or views (Vosen, 2021; Walrave et al., 2022).

CONCLUSIONS AND DIRECTIONS FOR FUTURE RESEARCH

The results of the conducted study provide valuable insights from both theoretical and practical perspectives. Most importantly, they show that young adults adopt diverse coping strategies in response to cybervetting, depending on the nature of the social media platforms they use. Users of professionally oriented platforms more frequently demonstrate higher concern for privacy and employ preventive strategies, which may be interpreted as a sign of greater self-presentation awareness in the recruitment context.

From the perspective of employer branding, these findings confirm that the growing awareness of young candidates regarding their digital presence can influence how they shape their online image. Employers, when designing recruitment strategies, should take into account that candidates are increasingly managing their digital identity, not only by hiding information but also by selectively exposing it.

At the same time, the study did not confirm some of the anticipated relationships—for example, the intensity of social media use was not significantly associated with the application of coping strategies. This may indicate a need for further analyses—including qualitative research—to better understand the motivations and intentions behind specific user practices.

One of the limitations of this study is the use of self-report scales—respondents may have underreported their level of exposure or overestimated their coping efforts. Additionally, in the initial pilot phase, users of different platform types were analyzed separately. However, due to overlapping groups and unequal sizes, each respondent was ultimately assigned to a single dominant category, which allowed for a clearer comparative analysis.

Another limitation is the purposeful sampling of 126 students, which restricts the generalizability of the findings to the entire population of young adults in Poland. Although demographic data (e.g., level and field of study) were collected, the variation in responses based on these variables was not analyzed, potentially obscuring significant differences in coping strategies.

Future research should consider qualitative approaches that could reveal more subtle mechanisms of digital self-presentation management, such as the use of algospeak, account rotation, or deliberate content “banalization.”

Notes

- 1 “Viral reach” refers to the phenomenon in which user-generated content spreads rapidly and widely across the internet, gaining significant popularity in a short period of time - most often due to the algorithms of social media platforms such as TikTok or Instagram.
- 2 “Selfie-branding” refers to the strategic use of selfies, self-portrait photographs posted by users, to build and reinforce one’s personal brand on social media. It is not merely about showing one’s face, but about consciously crafting an image (e.g., lifestyle, skills, values) through a series of visually consistent and appealing photos, especially on platforms like Instagram.
- 3 In the context of recruitment, “red flags” refer to warning signs in a candidate’s online behavior that may lead to disqualification from further consideration. These include vulgar or aggressive language, hate speech, content promoting discrimination, extremism, or violence, as well as posts showing excessive alcohol or substance use. Red flags may also include offensive comments about former employers or evidence of unethical conduct, such as lying or plagiarism. Essentially, they represent any element of a candidate’s digital footprint that suggests their employment could pose reputational, cultural, or legal risks to the organization.
- 4 A SaaS-based candidate screening tool used in recruitment processes. Yoono generates intelligent reports on potential employees using AI-driven software.

REFERENCES

- Loh, J.M.I., & Walsh, M.J. (2021). Social media context collapse: The consequential differences between context collusion versus context collision. *Social Media + Society*, 7(3). <https://doi.org/10.1177/20563051211041646>.
- Backman, C., & Hedenus, A. (2023). Professional talk on cybervetting: Accounting for a contested practice. *Acta Sociologica*, 66(1), 59–73. <https://doi.org/10.1177/00016993221088741>.
- 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), 479–506. <https://doi.org/10.1177/0893318914541966>.
- Berkelaar, B.L., & Buzzanell, P.M. (2015). Online employment screening and digital career capital: Exploring employers’ use of online information for personnel selection. *Management Communication Quarterly*, 29(1), 84–113. <https://doi.org/10.1177/0893318914554657>.
- Da Motta Veiga, S.P., & Figueroa-Armijos, M. (2022). Considering artificial intelligence in hiring for cybervetting purposes. *Industrial and Organizational Psychology*, 15(3). <https://doi.org/10.1017/iop.2022.54>.
- Escalera, J. (2025). *Zety’s 2025 Gen Z career trends report: 46% of Gen Z has secured jobs through TikTok*. Retrieved June 12, 2025, from <https://zety.com/blog/genz-career-trends-report> zety.com
- Hargittai, E., & Litt, E. (2013). New strategies for employment? Internet skills and online privacy practices during people’s job search. *IEEE Security & Privacy*, 11(3), 38–45. <https://doi.org/10.1109/MSP.2013.64>.
- Hartwell, C.J., Harrison, J.T., Chauhan, R.S., Levashina, J., & Campion, M.A. (2022). Structuring social media assessments in employee selection. *International Journal of Selection and Assessment*, 30(5), 330–343. <https://doi.org/10.1111/ijsa.12384>.

- Hoover, A.N., Rupp, D.E., & McCauley, R. (2025). Cybervetting best practices: An integrative framework for developing, validating, and implementing social media assessment for personnel selection. *Employee Responsibilities and Rights Journal*. <https://doi.org/10.1007/s10672-025-09538-4>.
- Hukkeri, P., & Pol, S. (2025). The impact of AI and social media integration on recruitment strategies: Opportunities and challenge. *IOSR Journal Of Humanities and Social Science (IOSR-JHSS)*, 30(5), 30–35. Retrieved July 2, 2025, from <https://www.iosrjournals.org/iosr-jhss/papers/Vol.30-Issue5/Ser-3/F3005033035.pdf>
- Jacobson, J., & Gruzdz, A. (2020). Cybervetting job applicants on social media: The new normal? *Ethics and Information Technology*, 22, 175–195. <https://doi.org/10.1007/s10676-020-09526-2>.
- JDP. (2019). *Study: How job seekers curate their social presence*. Retrieved June 27, 2025, from <https://www.jdp.com/blog/job-search-social-media-study-2019>
- Johnson, K. (2022). *Feds warn employers against discriminatory hiring algorithms*. Retrieved June 25, 2025, from <https://www.wired.com/story/ai-hiring-bias-doj-eccc-guidance/>
- Lacmanović, S., & Skare, M. (2025). Artificial intelligence bias auditing—current approaches, challenges and lessons from practice. *Review of Accounting & Finance*, 24(3), 375–400. <https://doi.org/10.1108/RAF-01-2025-0006>.
- Qiu, L., Lu, J., Yang, S., Qu, W., & Zhu, T. (2015). What does your selfie say about you? *Computers in Human Behavior*, 52, 443–449. <https://doi.org/10.1016/j.chb.2015.06.032>.
- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 12 July 2024, Classification rules for high-risk AI systems (Art. 6). *Official Journal of the European Union*, L 1689. Retrieved July 2, 2025, from <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Roulin, N., & Levashina, J. (2016). Impression management and social media profiles. In R., Landers, & G., Schmidt (Eds.), *Social media in employee selection and recruitment*. Cham: Springer. https://doi.org/10.1007/978-3-319-29989-1_11.
- 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*, 31(2), 347–354. <https://doi.org/10.1111/ijsa.12424>.
- Ruggs, E.N., Walker, S.S., Blanchard, A., & Gur, S. (2016). Online exclusion: Biases that may arise when using social media in talent acquisition. In R. Landers & G. Schmidt, (Eds.), *Social media in employee selection and recruitment*. Cham: Springer. https://doi.org/10.1007/978-3-319-29989-1_14.
- Steen, E., Yurechko, K., & Klug, D. (2023). You can (not) say what you want: Using algospeak to contest and evade algorithmic content moderation on TikTok. *Social Media + Society*, 9(3). <https://doi.org/10.1177/20563051231194586>.
- Steinhardt, S.J. (2024). Younger generations use TikTok as a career tool. *NextGen Blog (NYSSCPA)*. Retrieved June 28, 2025, from <https://www.nysscpa.org/article-content/younger-generations-use-tiktok-as-a-career-tool-060524>
- 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. <https://doi.org/10.1089/cyber.2012.0163>.
- Tews, M.J., Stafford, K., & Kudler, E.P. (2020). The effects of negative content in social networking profiles on perceptions of employment suitability. *International Journal of Selection and Assessment*, 28(1), 17–30. <https://doi.org/10.1111/ijsa.12277>.
- Vitak, J., & Kim, J. (2014). You can't block people offline. *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*. Retrieved June 25, 2025, from <https://doi.org/10.1145/2531602.2531672>
- Vosen, E. (2021). Social media screening and procedural justice: Towards fairer use of social media in selection. *Employee Responsibilities and Rights Journal*, 33, 281–309. <https://doi.org/10.1007/s10672-021-09372-4>.
- Wadley, J. (2024). Study looks at 'shadowbanning' of marginalized social media users. Retrieved June 27, 2025, from <https://record.umich.edu/articles/study-looks-at-shadowbanning-of-marginalized-social-media-users/>
- Walrave, M., Van Ouytsel, J., Diederer, K., & Ponnet, K. (2022). Checked and approved? Human resources managers' uses of social media for cybervetting. *Journal of Cybersecurity and Privacy*, 2, 402–417. <https://doi.org/10.3390/jcp2020021>.
- Yoono. (2024) *The Complete Guide to GDPR in Recruitment*. Retrieved June 12, 2025, from <https://www.gdpreu.org/yoono-the-complete-guide-to-gdpr-in-recruitment/>
- Zaman, T., Chen, Y.S. (2024). *How Shadow Banning Can Silently Shift Opinion Online*. Retrieved June 12, 2025, from <https://insights.som.yale.edu/insights/how-shadow-banning-can-silently-shift-opinion-online>
- Zarzycka, E., Krasodomska, J., & Dobija, D. (2021). Stakeholder engagement in corporate social practices and non-financial disclosures: A systematic literature review. *Central European Management Journal*, 29(1), 112–135. <https://doi.org/10.7206/cemj.2658-0845.43>.
- Zhang, L., Van Iddekinge, C.H., Arnold, J.D., Roth, P.L., Lievens, F., Lanivich, S.E., & Jordan, S.L. (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*, 105(12), 1530–1546. <https://psycnet.apa.org/doi/10.1037/apl0000490>.