Algorithmic Profiling in the Workplace: Employee Perceptions and Technostress

Magnus Ulvestad Paulsen[1,2] and Jefferson Seide Molléri[1][0000−0001−5629−5256]

[1] Ålesund Kommune, Ålesund, Norway
[2] Kristiania University College, Oslo, Norway
magnus.paulsen@gmail.com, jefferson.molleri@gmail.com

Abstract. Algorithmic profiling is becoming a common practice in workplaces, aimed at enhancing productivity and security. However, it raises concerns about employee privacy, algorithmic aversion, and technostress. This paper examines two cases of algorithmic profiling in a Norwegian municipality: a Security Awareness Program (SAT) tailored to employee behaviors and a User Behavior Analytics (UBA) system that monitors endpoint activities. Using technostress theory, we investigated how algorithmic profiling affects employee sentiments, focusing on privacy concerns, perceived invasiveness, and stress responses. Our mixed-method case study reveals concerns about algorithmic fairness and heightened stressors such as techno-overload and techno-insecurity. The findings suggest that while algorithmic profiling can enhance productivity, it also can induce technostress, particularly through techno-insecurity, techno-complexity, and techno-invasion. To mitigate these challenges, ethical implementation and transparency are critical. We also provide recommendations for organizational practices and future research directions.

Keywords: algorithmic profiling · workplace · public organization · perception · technostress

1 Introduction

Algorithmic profiling has become increasingly common in modern workplaces, driven by advancements in artificial intelligence (AI), machine learning (ML), and big data. These technologies enable organizations to collect and analyze large amounts of employee data, creating detailed profiles that guide decision-making on productivity and security [11, 12]. While these systems promise to enhance efficiency, they raise critical concerns about employee privacy, fairness, and well-being [5, 9].

This study focuses on how algorithmic profiling affects employee well-being, particularly through its potential to introduce or increase technostress - a form of stress induced by the use of digital technologies [1, 19]. As profiling systems monitor and evaluate employee behavior, perceptions of privacy invasion and lack of transparency can trigger stress responses, leading to negative outcomes such as distrust and anxiety. In some cases, this can culminate in what is known

as "chilling effects," where employees alter their behavior due to the perception of being constantly monitored [5].

Our research examines two algorithmic profiling initiatives in a mid-sized Norwegian municipality: a Security Awareness Program (SAT), which tailors employee training based on profiling data, and a User Behavior Analytics (UBA) system, which monitors employee activities for security purposes. By exploring how these profiling systems are perceived by employees, we provide insights into their broader implications for workplace well-being and the ethical considerations surrounding their implementation.

2 Background and Related Work

This section outlines concepts relevant to the research, setting the stage for understanding algorithmic profiling in the workplace.

2.1 Algorithmic Profiling

It refers to the use of algorithms to analyze large datasets, often containing personal information, to infer patterns and make predictions about individual characteristics, behaviors or preferences [10]. In the workplace, algorithmic profiling initiatives can include performance tracking, personalized training, or security monitoring [11, 12].

The adoption of these profiling tools is not without challenges. A growing body of literature highlights the dual-edged nature of algorithmic profiling in the workplace. On the one hand, it promises increased efficiency and more personalized employee support [11]; on the other, it often leads to unintended consequences, such as heightened feelings of surveillance and loss of autonomy [9]. Research has shown that employees may develop negative sentiments toward algorithmic profiling due to concerns over data transparency, trust, and bias [2, 12–14].

Moreover, if profiling tools are trained on biased data, there is a risk of reinforcing existing prejudices and producing discriminatory outcomes [3]. Moreover, algorithmic systems, while objective in theory, may lack the nuanced understanding required to interpret complex human behaviors and contextual factors affecting employee performance [2].

2.2 Chilling Effects

Closely tied to these concerns are the chilling effects identified in literature related to workplace surveillance. Büchi et al. [5] describe chilling effects as the self-moderating behavior employees may adopt when they know they are being monitored, even if their behavior is lawful or benign. In the context of algorithmic profiling, such effects may lead to reduced workplace engagement or a reluctance to use certain technologies. Furthermore, chilling effects can be exacerbated by a lack of transparency, where employees are unsure of how their behavioral data is being collected or used [18].

2.3 Technostress

Technostress refers to the stress caused by the use of digital technologies and has become a growing concern in modern workplaces. It is driven by factors (or stressors) such as 1. *techno-overload:* feeling forced to work faster and longer, 2. *techno-invasion:* always being reachable, 3. *techno-complexity:* the difficulty in understanding and using new technologies, 4. *techno-insecurity:* fear of job loss due to technology, and 5. *techno-uncertainty:* uncertainty caused by a changing technological landscape [1, 19].

Research has shown that technostress can negatively affect employee satisfaction, productivity, and health, especially in environments where data is collected for algorithmic profiling [6, 4]. In such environments, employees may feel overwhelmed by the complexity and perceived invasiveness of the profiling systems, leading to heightened stress levels [15, 17].

2.4 Research Gaps

Although extensive research have been conducted on algorithmic profiling and technostress individually, notable gaps remains on the intersection of these two domains. Technostress is still under-explored in the context of AI-driven profiling systems, particularly in how different types of profiling (e.g., security awareness, productivity tracking) affect stress levels [15, 9]. Moreover, few studies have examined the long-term effects or the role of organizational transparency in mitigating negative outcomes [5].

3 Methods

This study uses a mixed-methods case study approach [7, 20] combining both quantitative and qualitative data to offer statistical insights alongside a deeper contextual understanding of the phenomenon under investigation.

3.1 Research Questions

The overall goal of this study is to gain a deeper understanding of the interplay between employee perceptions towards profiling and privacy, and to explore if and how such technologies can contribute to technostress. Specifically, we intended to answer following questions:

RQ1 What are the employees' perceptions towards using algorithmic profiling in the workplace?
RQ2 How can the level of "invasiveness"/perceived privacy affect such perceptions?
RQ3 How do different algorithmic profiling initiatives (i.e. SAT and UBA) impact perceived technostress among employees?

3.2 Context of the Case Study

The case study was conducted in a mid-sized Norwegian municipality that had recently introduced two workplace initiatives involving algorithmic profiling. The first initiative is a **Security Awareness Program (SAT)**, which uses algorithmic profiling to tailor training and phishing tests based on individual employee behavior and knowledge. The system personalizes security training and adjusts the frequency of phishing tests depending on the employee's past performance.

The second initiative is a **User Behavior Analytics (UBA) system**, which continuously monitors employee activities across the municipality's digital infrastructure. The UBA system logs detailed data, including application usage, document access, and network behavior, to detect anomalies and potential security threats. While intended to enhance workplace security, some employees have expressed concerns that the system's detailed monitoring creates a sense of surveillance.

3.3 Data Collection

Data was collected from three sources to ensure triangulation:

Document Analysis: The municipality's strategies, policies, and data protection assessments were reviewed to gain insights into the organizational context and implementation of algorithmic profiling. This provided a foundational understanding of the ethical and practical considerations driving the use of profiling technologies.

Questionnaire: A structured survey was distributed to all employees, gathering quantitative data on demographics, pre-existing knowledge of algorithmic profiling, perceptions of invasiveness, and technostress. A total of 272 valid responses (out of 6233 invitations) were collected. This allowed for broad insight into the general perception towards algorithmic profiling, with a focus on identifying stressors linked to profiling technologies.

Interviews: In-depth semi-structured interviews were conducted with five employees to gain qualitative insights into their personal experiences and concerns regarding algorithmic profiling. The interviews were informed by the survey results, addressing effects that might not be fully captured in the quantitative responses. All the RQs were targeted by the interviews.

Survey and interview questions were designed based on constructs derived from literature on algorithmic profiling [5, 8, 18] and technostress [1, 19]. These constructs informed the development of 38 Likert scale survey questions targeting perceptions of privacy, trust, and technostress (see Appendix A), as well as open-ended questions to explore employee experiences via interviews. Each construct was addressed by multiple questions, exploring different dimensions of it. See supplementary materials [16] for details on the survey questionnaire, survey responses, interview guide, and informed consent forms[1].

[1] For access to the supplementary materials, visit the online repository at `https://doi.org/10.5281/zenodo.13950046`.

3.4 Data Analysis

The data analysis process was conducted in two phases:

Quantitative Analysis: Survey data was analyzed using statistical methods, including frequency analysis, correlation analysis, and regression analysis. Spearman's rho was used to assess the relationships between perceived invasiveness, privacy concerns, and levels of technostress. This helped to identify patterns in employee responses and the potential factors that contribute to algorithmic aversion.

Qualitative Analysis: Document and interview data were analyzed using a combination of inductive and deductive coding. The analysis focused on identifying common themes, such as feelings of surveillance, distrust in automated decision-making, and stress due to data collection practices. The coding process involved several iterations to ensure the accuracy and depth of the findings.

3.5 Research Validity and Reliability

To mitigate potential biases, the study incorporated triangulation by cross-referencing survey results with interview responses and document analysis. The use of multiple data collection methods also improves the internal validity of the findings. By integrating diverse data sources and methodologies, we could achieve a more comprehensive understanding of the phenomenon under study, reducing the likelihood of misinterpretation.

Although the organizational context may limit the generalizability of the findings, we sought to enhance external validity by ensuring the sample was representative of the broader employee population within the municipality. The survey participants closely reflect the overall demographics. Age, gender, and workplace distribution aligns well with the overall employee population. With regarding the organization sectors, the health sector was slightly underrepresented (it comprises nearly 50% of the workforce), while respondents from the 'organization' and 'society' sectors are slightly overrepresented.

4 Results

This section presents the key findings on employee perceptions of algorithmic profiling and their influence on technostress.

4.1 RQ1. Employee Perceptions of Algorithmic Profiling

Our survey included 18 questions based on five constructs: "Acceptance", "Privacy", "Trust", "Algorithm Aversion", and "Chilling Effects". A list of the survey questions and related constructs is provided in Appendix A and is also available in the supplementary material[1].

The results reveal mixed views on algorithmic profiling, as shown in Figure 1, and similar perception were identified across all demographic groups. Respondents generally agreed that data collection should be limited in scope and detail

(Accept4) and that algorithmic profiling should be used only when strictly necessary (Accept2). There were also elements of distrust in automated decision-making processes (Aversion2), particularly when employees felt that profiling technologies lacked transparency or fairness. There was notable disagreement with statements about privacy. Most participants disagreed with the notion that their privacy is unaffected by algorithmic profiling (Privacy1), given the current monitoring. Respondents also disagreed with the idea that there is no difference between collecting limited data and detailed data (Privacy3).

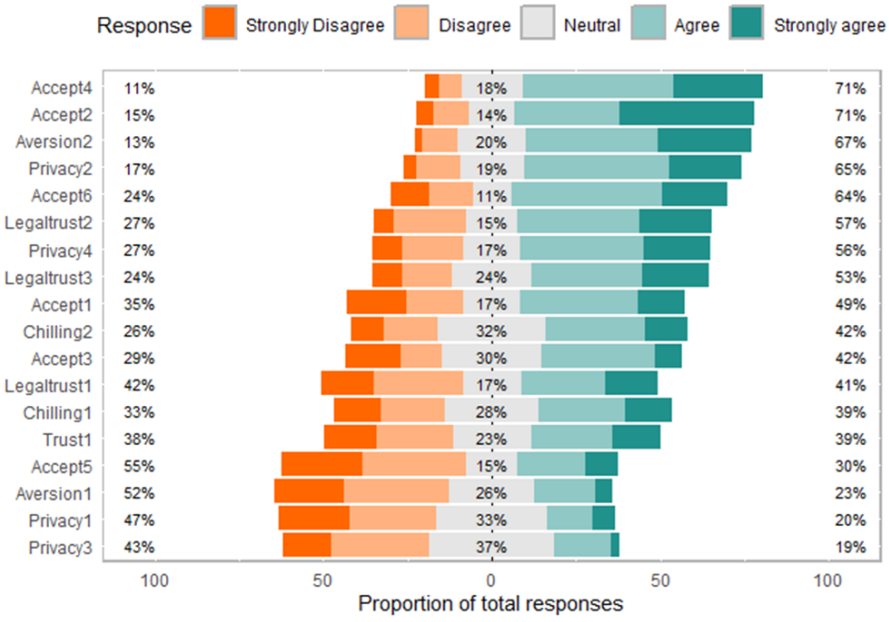

Fig. 1. Distribution of employee responses to Likert scale questions about algorithmic profiling. Constructs are detailed in Appendix A and supplementary material[1].

The qualitative analysis confirmed the mixed perceptions of algorithmic profiling. While some respondents saw potential benefits, such as improved efficiency and planning, concerns about surveillance, privacy invasion, and transparency were prevalent. As one interviewee mentioned, *"It feels uncomfortable knowing that everything I do on my work computer is potentially being monitored and used to judge my professional capabilities."*

Some interviewees feared that profiling could erode trust and lead to decisions being made solely based on data, without human oversight, with one participant expressing, *"The idea that a machine could decide my career trajectory based on data profiles is unsettling."* However, a few interviewees were optimistic, believing that profiling could help streamline work. Overall, there is a strong call for ethical guidelines and clear boundaries on data collection to prevent misuse.

Technostress We assessed this dimension through 20 survey items across four constructs: "Insecurity", "Complexity", "Security", and "Privacy" (see Appendix A for details). These questions were designed to retest key factors contributing to technostress, following the framework established by a previous study [1].

Our findings suggest that the overall level of perceived technostress within the organization is relatively low, with some variations. Most respondents scored low on all technostress factors, except for privacy concerns, which emerged as a potential source of stress. We also examined differences across the sectors in the organization, i.e. health, education, organizational, society, municipal enterprise, and others. An independent samples t-test revealed that job insecurity was higher in organizational sector compared to education or health services, while privacy concerns were consistently high across all sectors. Perceived technological complexity was most pronounced in health services.

Key Insights

- Mixed perceptions are consistent across all demographic groups.
- Perceptions are highly influenced by trust and concerns over privacy.
- There is a desire to balance data collection with individual benefits.
- Some level of distrust in automated decision-making processes.
- Fears of surveillance and workplace disruptions were common.

4.2 RQ2. The Influence of Perceived Invasiveness on Employee Perception

Statistical analysis of the survey data revealed a significant correlation between the perceived invasiveness and negative perceptions (Spearman's rho = 0.68, $p < 0.01$). Employees who felt that excessive amounts of personal data were being collected were more likely to report feelings of distrust.

Interviewees expressed concerns about the volume of data collected and the potential for misuse, along with uncertainty about how their data would be used. When employees lacked clarity on what data was collected and its purpose, they perceived the process as more invasive, which increased stress and led to feelings of being constantly monitored. As one interviewee stated, *"If a lot of information is collected, there's always a risk of it getting misplaced or misused"*. This perception of surveillance was reported by multiple of the interview subjects to have caused them to adapt and alter their behavior.

Both survey and interview data suggest that increased data collection amplifies concerns about privacy and surveillance. As a result, employees adopt a self-moderation behavior, or "chilling effects," where they become more cautious in their actions, which may disrupt normal work routines. For example, one participant shared, *"The logging makes you extra cautious about what you do"*. Transparency through clear communication and involvement emerged as a crucial factor in addressing these concerns.

Key Insights

- Amount of data collected significantly influences perceived "invasiveness" and privacy.
- This perception has impact on employee perception and stress levels.
- Risk of employees adjusting their actions due to feeling constantly monitored.

4.3 RQ3. Impact of Algorithmic Profiling Initiatives on Technostress

Security Awareness Program (SAT) The SAT, which tailors security training based on profiling data, was generally perceived more positively by employees compared to the purely analytical UBA system (as shown in Figure 2).

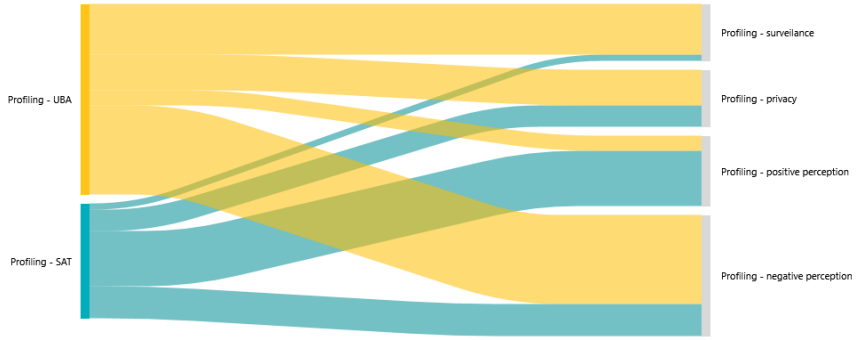

Fig. 2. Sankey diagram relating the algorithmics profiling initiatives SAT and UBA with employee perceptions and some of the key themes identified in the interviews.

Interviewees felt that the SAT improve their cybersecurity skills. The purpose of the tool may position it more as a support mechanism rather than a contributor to technostress. However, there was evidence of technostress linked to the following stressors:

- *Techno-complexity:* Employees unfamiliar with digital technologies reported frustration with the complexity of the training.
- *Techno-insecurity:* There was anxiety around the idea that the training system was tracking their performance and could be used for punitive measures. As one participant noted, *"If I keep getting low scores in security awareness, it feels like proof that I'm not competent in IT. It's demoralizing and could make me feel like I'm not valued or that my job could be at risk, even if my main skills lie elsewhere."*

- *Techno-invasion:* The gamification aspect of the training was seen as overwhelming, with employees feeling burdened by continuous new challenges.
- *Techno-uncertainty:* Employees expressed concern about their future career path, as weak results reinforced negative misconceptions of poor performance. One interviewee stated, *"If you find out you're the only one getting extra phishing tests, it could make you wonder if you're seen as a security risk. It's not a good feeling, especially if you start thinking your employer sees you as a weaker link compared to your colleagues".*

User Behavior Analytics (UBA) system In contrast to the SAT, the UBA system was perceived by many employees as intrusive, contributing significantly to technostress (see Figure 2, above). Interviews revealed that employees felt they were being excessively monitored, which led to negative feelings related to the following stressors:

- *Techno-insecurity:* Concerns were raised about the potential misuse of data to make decisions on employee performance or behaviour. One participant stated *"If the algorithms have any underlying biases or agendas, there's a risk that the profiling could categorize people unfairly, like judging someone's behavior based on what websites they visit. It feels like you can't fully control how you're perceived".*
- *Techno-invasion:* Employees frequently mentioned feeling "watched," leading to discomfort and a sense of invasion into their privacy. One interviewee shared: *"Knowing my online activity is being continuously analyzed makes me feel like I can't relax or take a break without it being noticed. The thought of being constantly monitored for security reasons starts to feel like an invasion of my personal space at work."*
- *Techno-overload:* The constant presence of the system led some employees to feel overwhelmed, with some expressing frustration at the amount of data being collected and analyzed.
- *Techno-uncertainty:* Employees were unclear about how the data collected by the UBA system would be used and whether it could impact their career trajectory, leading to increased stress and fear of unfair treatment. One interviewee shared *"(...) I also worry about how the data might paint a misleading picture of me, especially when I spend time researching topics that don't personally relate to me."*

Key Insights

- Less tech-savvy employees may feel overwhelmed by the system's complexity.
- Performance metrics can increase anxiety and create concerns about future career prospects.
- Constant surveillance increased feelings of invasion and discomfort.
- Fear of data being used for punitive actions raised concerns about job security.

5 Discussions

The results of this study indicate that algorithmic profiling can have both positive and negative effects on employees, depending on the context and the perceived level of invasiveness. Our findings aligns with prior studies [5, 18], which noted that algorithmic systems could induce chilling effects and impact trust when perceived as invasive.

The comparison of two distinct use cases within the same organizational context provides a nuanced understanding of how profiling technologies are perceived differently depending on their purpose and perceived level of invasiveness. While the SAT was largely seen as beneficial by employees, the UBA system was widely regarded as overly invasive, contributing significantly to technostress. This finding reinforces that algorithmic profiling, when applied transparently and ethically, can enhance workplace engagement, but it can also lead to adverse outcomes if perceived as a tool for constant surveillance.

The perceived invasiveness of these systems plays a critical role in shaping employee responses. Employees who feel that their privacy is being compromised by excessive data collection or monitoring are more likely to report negative perception and technostress. These results align with prior studies that suggest a link between perceived surveillance and stress in the workplace [1, 5, 9].

5.1 Theoretical Implications

This study provides important contributions to the understanding of Technostress Theory in the context of algorithmic profiling. While previous research has identified various sources of technostress, such as techno-overload and techno-complexity [1, 19], this study highlights the role of techno-insecurity and techno-invasion as central stressors specifically linked to algorithmic profiling. The introduction of profiling technologies in the workplace raises new concerns around privacy, transparency, and trust, suggesting that the established technostress constructs should be expanded to account for these unique stressors.

The findings also support the emerging view that algorithmic aversion is influenced by employees' trust in the system and the perceived transparency of data collection [13]. This study demonstrates that when employees feel uncertain or unaware of how their data is being used, their stress levels increase, reinforcing the importance of transparency as a moderator in the algorithmic profiling context.

5.2 Practical Implications

For practitioners, the results of this study highlights the importance of ethical and transparent implementation of algorithmic profiling. Related research [12, 14] highlighted a need for ethical governance to avoid potential misuse or discriminatory practices. To minimize negative perceptions and technostress, organizations must prioritize clear communication about the purposes of data collection and how it will be used. Employees need to understand what data is

being collected, why it is being collected, and how it benefits them. Transparency and involvement in decision-making processes can serve as key mitigating factors in reducing feelings of invasiveness.

Organizations should consider customization and flexibility in the implementation of profiling technologies. For example, the SAT was likely seen more positively because it is tailored to individual needs and allowed employees to engage at their own pace. On the other hand, the UBA system, which collected large amounts of data without clear communication of its purpose, led to feelings of surveillance and increased technostress. By allowing employees more control over how they interact with these systems, and by ensuring that profiling is implemented with respect to personal privacy, organizations can enhance the acceptance and effectiveness of these technologies.

Finally, organizations must recognize the psychological impact of constant monitoring on employee well-being. The study highlights the importance of maintaining a balance between security needs and employee trust. Profiling systems should be designed and implemented with a focus on ethical data use and privacy protections, ensuring that they do not undermine the mental health or job satisfaction of employees. Ethical guidelines and policies that address these concerns should be an integral part of any algorithmic profiling strategy.

5.3 Limitations and Future Research

While this study provides valuable insights, it is not without its limitations. The findings are based on a case study within a specific organizational context, which may limit the generalizability of the results to other industries or regions. Future research should consider conducting longitudinal studies or comparative analyses across different sectors to explore the long-term effects of algorithmic profiling on employee behavior and technostress.

Moreover, there is a need for further investigation into how demographic factors, such as age, technological literacy, and job role, influence employee responses to profiling technologies. Understanding these variations could help tailor profiling systems more effectively to individual needs, further reducing the risk of technostress.

6 Conclusions

Our research demonstrated that employees are more likely to experience negative emotions, such as distrust and discomfort, when they feel excessively monitored. Profiling systems like the Security Awareness Program, which offered clear benefits and tailored content, were met with more positive responses, whereas the User Behavior Analytics system, seen as overly intrusive, contributed significantly to technostress. This highlights the importance of balancing security needs with employee well-being and trust in the workplace.

From a theoretical standpoint, our study contributes to the evolving understanding of technostress. The findings suggest that future studies are needed to

better address the specific challenges posed by algorithmic profiling in modern workplaces. In practice, our results provide a clear mandate for organizations to adopt ethical and transparent approaches when implementing profiling technologies. By ensuring that employees are well-informed about how their data is being used and offering opportunities for involvement in decision-making processes, organizations can mitigate the negative impacts of profiling and foster a more trusting and productive work environment.

References

1. Ayyagari, R., Grover, V., Purvis, R.: Technostress: Technological antecedents and implications. MIS quarterly pp. 831–858 (2011)
2. Bankins, S., Ocampo, A.C., Marrone, M., Restubog, S.L.D., Woo, S.E.: A multilevel review of artificial intelligence in organizations: Implications for organizational behavior research and practice. Journal of Organizational Behavior **45**(2), 159–182 (2024)
3. Barocas, S., Selbst, A.D.: Big data's disparate impact. Calif. L. Rev. **104**, 671 (2016)
4. Becker, J., Berger, M., Gimpel, H., Lanzl, J., Regal, C.: Considering characteristic profiles of technologies at the digital workplace: The influence on technostress. In: ICIS (2020)
5. Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., Viljoen, S.: The chilling effects of algorithmic profiling: Mapping the issues. Computer law & security review **36**, 105367 (2020)
6. Cadieux, N., Fournier, P.L., Cadieux, J., Gingues, M.: New techno-stressors among knowledge professionals: The contribution of artificial intelligence and websites that misinform clients. International Journal of Electronic Commerce **25**(2), 136–153 (2021)
7. Creswell, J.W., Clark, V.L.P.: Designing and Conducting Mixed Methods Research. SAGE (2011)
8. Dietvorst, B.J., Simmons, J.P., Massey, C.: Algorithm aversion: people erroneously avoid algorithms after seeing them err. Journal of experimental psychology: General **144**(1), 114 (2015)
9. Giermindl, L.M., Strich, F., Christ, O., Leicht-Deobald, U., Redzepi, A.: The dark sides of people analytics: reviewing the perils for organisations and employees. European Journal of Information Systems **31**(3), 410–435 (2022)
10. Hildebrandt, M.: Defining profiling: A new type of knowledge? In: Profiling the European citizen: Cross-disciplinary perspectives, pp. 17–45. Springer (2008)
11. Holt, M., Lang, B., Sutton, S.G.: Potential employees' ethical perceptions of active monitoring: The dark side of data analytics. Journal of Information Systems **31**(2), 107–124 (2017)
12. Indiparambil, J.J.: Privacy and beyond: Socio-ethical concerns of 'on-the-job'surveillance. Asian Journal of Business Ethics **8**(1), 73–105 (2019)
13. Jussupow, E., Benbasat, I., Heinzl, A.: Why are we averse towards algorithms? a comprehensive literature review on algorithm aversion. In: Proceedings of the 28th European Conference on Information Systems (ECIS). An Online AIS Conference (June 15-17 2020)
14. Manokha, I.: The implications of digital employee monitoring and people analytics for power relations in the workplace. Surveillance and Society **18**(4) (2020)

15. Nisafani, A.S., Kiely, G., Mahony, C.: Workers' technostress: A review of its causes, strains, inhibitors, and impacts. Journal of Decision Systems **29**(sup1), 243–258 (2020)
16. Paulsen, M.U., Molléri, J.S.: Supplementary materials: Algorithmic profiling in the workplace (October 2024). https://doi.org/10.5281/zenodo.13950046, `https://doi.org/10.5281/zenodo.13950046`
17. Pflügner, K.: Technostress management at the workplace: A systematic literature review. Wirtschaftsinformatik 2022: Proceedings (Track 22: IS Adoption, Diffusion & Use) (2022)
18. Power, D.J., Heavin, C., O'Connor, Y.: Balancing privacy rights and surveillance analytics: a decision process guide. Journal of Business Analytics **4**(2), 155–170 (2021)
19. Tarafdar, M., Tu, Q., Ragu-Nathan, B.S., Ragu-Nathan, T.: The impact of technostress on role stress and productivity. Journal of management information systems **24**(1), 301–328 (2007)
20. Yin, R.K.: Case study research: Design and methods, vol. 5. SAGE (2009)

Appendix A Constructs and Descriptive Labels for Survey Items

Algorithmic Profiling Constructs

Accept1: I feel comfortable with my actions being monitored and logged in great detail, as long as the outcome provides me with a tangible benefit.
Accept2: I only want digital monitoring and algorithmic profiling to be used when strictly needed.
Accept3: I see algorithmic profiling as a good way to tailor work processes to my daily routine and level of competency.
Accept4: I perceive algorithmic profiling to be more acceptable if the data collected is limited in scope and detail.
Accept5: I have no problem with my employer collecting and analyzing detailed data about how I do my job.
Accept6: I understand that my employer might collect and analyze detailed data to improve efficiency or security.
Privacy1: I see no difference in collecting limited data or detailed data in relation to algorithmic profiling.
Privacy2: I perceive the use of algorithmic profiling at the workplace to erode my privacy.
Privacy3: My perception of privacy is unaffected by algorithmic profiling given the current level of logging at the workplace.
Privacy4: Knowing that many of my digital activities are logged makes me feel that I am under constant surveillance.
Trust1: I perceive the use of algorithmic profiling and monitoring as a consequence of a lack of trust.
LegalTrust1: I am confident that data collected by my employer will not be used for other than stated purposes.
LegalTrust2: I worry that data collected by my employer can be used for purposes beyond what was initially stated.

LegalTrust3: I am confident that my employer will comply with all relevant rules and regulations in using algorithmic profiling.
Aversion1: I generally trust algorithms to make fair and unbiased decisions.
Aversion2: Knowing that an algorithm rather than a human makes decisions impacts my perception of accuracy.
Chilling1: Knowing that my digital activities are being logged and profiled affects my behavior at the workplace.
Chilling2: Knowing that my digital activities are logged makes me more conscious about raising concerns or expressing my opinions.

Technostress Constructs

Techno-Invasion1: I fear that my use of ICT is less confidential than I would like.
Techno-Invasion2: I fear that information I exchange using ICT is not as protected as I would like.
Techno-Invasion3: I fear that malevolent outsiders can easily copy my identity due to ICT.
Techno-Invasion4: My personal information is too easily accessible due to ICT.
Techno-Invasion5: I fear that my personal data can easily be stolen online.
Techno-Complexity1: I often find it too complicated to accomplish a task using the ICT available to me at work.
Techno-Complexity2: I often need more time than expected to accomplish a task using ICT.
Techno-Complexity3: I feel that the ICT available to me at work are too confusing.
Techno-Complexity4: I often do not have enough time to keep up with new functionalities of ICT at work.
Techno-Complexity5: It would take me too long to figure out how to use ICT at work.
Techno-Insecurity1: I feel that my job is threatened due to ICT.
Techno-Insecurity2: I fear that I could be replaced due to the increasing standardization of work processes enabled by ICT.
Techno-Insecurity3: I cannot be optimistic about my long-term job security due to ICT automatization.
Techno-Insecurity4: I fear that I could be replaced by machines.
Techno-Insecurity5: I fear that digitalization will cost me my job.
Techno-Security1: I have to worry too often, whether I might download malicious programs.
Techno-Security2: I have to worry too often, whether I might receive malicious e-mails.
Techno-Security3: I fear that hackers might get access to company secrets through a mistake of mine.
Techno-Security4: I feel anxious when I get an e-mail from somebody that I do not know as it could be a malevolent attack.
Techno-Security5: E-Mails whose sender I do not know make me nervous.