Exploring the impact of AI monitoring on employee mental health and job satisfaction in remote work settings: ethical implications and governance strategies

Authored by **Sanchita Sanchita**, **Augusta Wood**, **Bisesh Shakya**

Douglas College

Abstract

Remote work models are increasingly more common in the modern workplace, as is the prevalence of workplace surveillance tools. This paper examines the impact of the emerging trend of AI-driven monitoring systems and their impact on remote workers. While these data-driven tools employ algorithms to study workers' behaviors as a means of boosting productivity and enhance worker engagement, they raise significant concerns about employee mental health, privacy, and job satisfaction. Continuous surveillance has been associated with increased stress and reduced autonomy, negatively impacting well-being. Additionally, the ethical implications of AI monitoring, including transparency and data privacy, are still underexplored. This study investigated issues related to the effects of AI monitoring in remote work settings using a mix of both primary and secondary data. This research aimed to identify current legal protections and recommended frameworks for AI governance. It determined current gaps in legal protections, both locally and globally. This was accompanied by primary research provided by interviewing qualified remote workers. Utilizing this mixed methodology, this research was able to devise an ethical framework for governance of AI-powered workplace surveillance tools with suggestions of actionable items.

Keywords

Artificial Intelligence (AI), Workplace Surveillance, Ethics and Governance, Worker Mental Health, Worker Job Satisfaction

Introduction

Since the COVID-19 pandemic, there have been significant increases in remote working trends. (Fathima and Kumar, 2024). Remote and hybrid work models have become increasingly prevalent across multiple industries. According to PayScale, an estimated 28% of the global workforce spent most or all their work hours from home in 2023 (PayScale, 2024). Many of organizations embracing these work models have sought means to monitor and analyze employees' behaviors and performance using data-driven technologies. These tools, which promise to boost productivity, improve time management, and increase accountability and transparency, are being built to include Artificial Intelligence (AI) and machine learning (ML) systems to handle the vast datasets more efficiently. According to a recent CNBC article, large enterprise companies such as "Walmart, Delta Air Lines, T-Mobile, Chevron, and Starbucks, as well as European brands including Nestle and AstraZeneca" currently utilize one AI-based workplace surveillance tool. (Field, 2024) The full extent of AI-powered surveillance has not been fully determined, as an emergent technology. However, a study conducted by Statistics Canada for 2024 into the use of AI technologies in the workplace indicated 6.1% of 10,173 respondent businesses and organizations in Canada had utilized AI tools in the last 12 months. (Bryan et al., 2024). Furthermore, of these respondents, 11.5% indicated plans to adopt software that uses AI in the next 12 months, indicating that use of the AI-powered software is going to increase over the next year. (Bryan et al., 2024).

The steady increase in the use of data-driven monitoring technologies has placed pressure on employees to perform under increasingly more invasive surveillance tools. This has been shown to impact the mental health and well-being of workers. Previous research has provided relevant information to this topic, such a method of classifying workplace surveillance tools based on functionality, what the impact of such tools are on workers, and what are the current and future legal, ethical, and governance concerns are. AI systems, particularly those integrated into remote worker monitoring tools, have prompted further ethical and legal concerns. These surveillance tools can include time management monitoring, performance monitoring, keystroke loggers, communication monitoring, task automation, security compliance, screen captures, and video and audio recordings. These systems collect employees' Personally Identifying Information (PII) and may include biometric data. Additionally, emotional AI is increasingly deployed to monitor employees' emotional states to optimize productivity, a trend accelerated by the COVID-19 pandemic. Businesses like IBM and Microsoft use emotional analytics not only for recruitment but also to assess employee well-being and engagement during remote work (Mantello & Ho, 2024). This raises ethical questions about workers' autonomy, privacy, and the consequences of continuous surveillance. Studies have shown that while AI monitoring systems can contribute to decision-making objectivity, they also carry risks such as increased stress, decreased autonomy, and erosion of human-centric management practices (Mantello & Ho, 2024; Banerjee et al., 2024).

Further, AI-powered mental health chatbots have emerged as tools to support employees, especially in managing mental health concerns like anxiety and depression (Banerjee et al., 2024). However, legal protections for workers are falling behind the progression of emergent technology trends in workplace surveillance, raising concerns related to privacy, data security, and the ethical use of employees' personal data. There is a lack of comprehensive regulatory frameworks and public engagement in the development and deployment of surveillance technologies, which may hinder their acceptance and effectiveness. (Fontes, et al., 2023). Employers should be cognizant of employees' need for data autonomy and ensure that any monitoring does not breach privacy laws, anti-discrimination laws or fair labor laws and practices. Addressing these issues is essential for creating governance frameworks that balance the benefits of AI monitoring with employees' mental well-being and job satisfaction. To address these concerns, this research seeks to discover the following. How does AI-powered remote work monitoring impact employee mental health and job satisfaction? What ethical concerns arise from the effects of AI surveillance on employee well-being? And what governance policies can be implemented to balance the benefits of AI monitoring with the need to protect employee mental health and job satisfaction?

To identify ethical concerns related to the psychological impact of AI monitoring in remote work, a thematic analysis of past research was conducted. The literary findings were organized based on common themes. The ethics and legality of remote worker monitoring tools was one key theme and studies discussing these concerns were selected, as addressing ethical concerns begin with a comprehensive understanding of the current legal landscape that may provide protections for workers, such as privacy laws. While this research paper will primarily focus its scope on Canadian legal protections, it does acknowledge that AI-governance is an increasingly global concern. Remote work is not restricted solely to local businesses and organizations but extends beyond country borders. Thus, in consideration of the development of an Ethical Framework, research was briefly conducted into the legal protections afforded to remote workers worldwide. Another theme that was selected was reviewing current governance methods for AI and remote monitoring technologies. Additionally, literature was reviewed with consideration into the theme of connections AI governance and the three key pillars of governance: corporate, IT, and data governance. Understanding AI Governance: AI governance encompasses the comprehensive set of rules, practices, and procedures that organizations employ to manage their AI systems. To better understand the types of software being reviewed, the research team selected research material that assessed and discussed these types of software. Finally, research that focused on the theme of workers' health and prosperity was added to our literature review, as the final research is focused on determining governances that promote worker well-being and job satisfaction.

Following the review of secondary literature, an analysis of primary research will be provided. This seeks to explore the impact of AI surveillance on the mental health and job satisfaction of remote workers. The data was gathered from interviews of qualified remote workers who are currently being monitored by AI-powered workplace surveillance software. The insights provided by remote workers provided additional data to identify gaps in governance and company policies that the development of an ethical governance framework directly addressed. The research utilized deductive analysis on the collected interview data to identify key issues that remote workers face with AI-based monitoring software and the analysis provided the research team with guidance on the development of an ethical governance framework. This proposed governance framework provides ways to minimize negative mental health effects while maintaining the benefits of AI-powered monitoring systems. The framework will be provided, along with actionable recommendations for companies who have implemented or may be considering the implementation of AI-based surveillance software. This research paper will then conclude with recommendations for future research.

Literature Review

This literature provides relevant information to the topics discussed within this paper and has been organized for clarity into the following themes: Ethics and legality in data-driven technologies, Impact on employees, and Current governances. This will be followed by a thorough discussion of Canada's current legal frameworks.

Ethics and legality in data-driven technologies:

In *From AI ethics principles to data science practice: A reflection and a gap analysis based on recent frameworks and practical experience*, researchers investigated the connections between AI governance and the three key pillars of governance: corporate, IT, and data governance. A well-established AI governance framework is crucial for aligning AI technologies with organizational objectives and ethical standards. Georgieva et al also stated that a well-established AI governance framework is crucial for aligning AI technologies with organizational objectives and ethical standards (Georgieva et al., 2022). This research focused primarily on the ethics of AI technologies overall. While this paper included the use of AI-powered monitoring technologies as part of a governance model, it did so without a specific focus on AI-powered surveillance technologies. This research concluded that "the solution lies not on one single framework that offers a simplified form of ethics" rather "we will need an entire landscape of methods, standards and procedures if we want to develop AI-based services for 'good'." (Georgieva et al., 2022).

Ethical and Legal Concerns of Artificial Intelligence in the Workplace: Examining Current Legislations in the United States attempts to analyze legal and ethical implications of AI-powered employee monitoring tools in the US workforce. Researchers reviewed both the ethics and legality of the use of AI in the workplace. In this paper, researchers provided several examples of past legal cases and specific statues that were used in understanding the current legal landscape of AI-powered surveillance tools. These often demonstrated how current laws fail to provide adequate protections for workers and may fail to meet the ethical needs of workers, such as transparency in managerial decisions. "Occupations like Uber driving exemplify how artificial intelligence's management applications intersect with the gig economy. In this scenario, oversight predominantly hinges on customer data and reviews, permitting implicit and explicit biases to influence workers' livelihoods without sufficient accountability." (Rudiyanto et al., 2023). The findings illustrated a need for employees to be fully informed of when they are being monitored with acceptable use policies and consent. It also concluded that employers should be cognizant of employees' need to be autonomous and ensure that any monitoring does not breach privacy laws, anti-discrimination laws or fair labor laws and practices.

In *Monitoring Mental Health: Legal and Ethical Considerations of Using Artificial Intelligence in Psychiatric Wards*, Solaiman, Malik, & Ghuloum explored the intricate balance between advancing healthcare through AI and adhering to stringent ethical and legal standards. They delved into the nuances

of patient consent, data privacy, and the legal ramifications of deploying AI in sensitive environments like psychiatric wards. This research explored how AI-power surveillance technologies can potentially improve monitoring and treatment in psychiatric settings, offering more personalized and timely interventions. The paper highlighted the beneficial outcomes of AI in monitoring patient behaviors and predicting psychiatric episodes. However, it also raised concerns about privacy, the potential for misuse, and the ethical implications of constant surveillance. "Given this sensitivity of data, clear guidelines are needed highlighting the laws that must be followed when handling such data in these and other scenarios." (Barry Solaiman et al., 2023). This research noted a deficiency in legal protections and ethical guidelines specific to the use of AI in psychiatric care, pointing to the need for more targeted policy development. While this did not relate specifically to employee surveillance, it reviews the ethics of AI-powered surveillance over mental health patients.

In *Artificial Intelligence and Employee Monitoring: Ethical Considerations and Best Practices*, Zimmerman & Fletcher (2023) analyzed the shift in employee perceptions towards workplace surveillance in the post-COVID-19 era. This paper proposed a comprehensive ethical framework for integrating AI into workplace monitoring. The analysis bridged the gap between theoretical ethics and practical implementation, advocated for a balanced approach that respects employee privacy while enhancing organizational transparency and accountability. The findings revealed how increased monitoring, especially in remote work settings, has diminished privacy and autonomy, potentially affecting worker satisfaction, organizational trust and creating power imbalances that could disproportionately impact vulnerable workers. (Zimmerman & Fletcher, 2023).

Impact on employees:

Data and Algorithms at Work: The case for Worker Technology Rights explores various data-driven technologies utilized by companies to address how these technologies may potentially harm workers. The case made statements concerning where US laws failed to protect workers' rights and recommended a set of principles that policymakers can use aimed at harm reduction. The case study also sourced some primary data from workers in various fields, providing anonymous statements from workers regarding perceived harms of data-driven technologies used in their workplace. This case study's determinations were that workers do not currently have enough legal protections in place for their defense. Workers should have additional rights for disclosure regarding when and where their data is being collected. They should have better access and control rights, and there should be more policies in place to protect against discrimination with data collection. This article provided a fair amount of insight into the potential harms of data-driven technologies in the workplace.

In *The Connected Workplace: Characteristics and Social Consequences of Work Surveillance in the Age of Datification, Sensorization, and Artificial Intelligence*, Mettler took an employee-centric stance to discuss the use of work surveillance tools in the modern workplace. Mettler gave a historical background on workplace surveillance and posited that many of these new technologies have arisen from a need to control workers. Mettler described three eras of workplace surveillance ending with the modern "connected workplace surveillance." (Mettler, 2023). Furthering this concept, Mettler broke down how connected workplace surveillance impacts workers' performance and even may have social consequences. For example, factory workers often experienced direct monitoring that measured their productivity on the assembly line, while remote software developers might encounter more subtle forms of oversight, like tracking their coding activities and the applications they used. Recognizing these differences was crucial in understanding how surveillance impacts various types of workers in distinct ways. Mettler stated this research sought to answer questions concerning the nature of workplace surveillance and how it impacted workers. Mettler provided a thematic analysis of previous works, basing research findings off of secondary data. This research gave further insights into workplace surveillance from a historical to modern context and briefly alluded to Taylorist management styles, another way to describe for Scientific Management Theory.

The swift shift to remote work due to the COVID-19 pandemic revealed critical elements impacting employee well-being, particularly in terms of job control and loneliness. In *Surviving remotely: How job control and loneliness during a forced shift to remote work impacted employee work behaviors and well-being* research indicated that employees who perceived they have more control over their work tend to experience reduced emotional exhaustion and a better balance between work and personal life. This highlighted the vital role that autonomy plays in remote work settings (Becker et al., 2021). However, the benefits of job control could differ based on individual preferences for separating work and home life. Becker's research highlighted that being under constant surveillance for extended periods can negatively impact both mental health and job satisfaction. This continuous monitoring created a stressful atmosphere that affected how employees felt about their work and overall well-being. For those who preferred a clear division, the advantages may not be as significant, suggesting a need for organizations to develop flexible policies that consider the diverse needs of their employees. This aligned with Becker's insights on the importance of autonomy but added another layer by considering the isolation experienced in remote work settings. The experience of isolation could differ greatly between blue-collar and white-collar workers. For example, white-collar employees working remotely often grappled with the challenge of distinguishing between their professional and personal lives. In contrast, blue-collar workers, who typically did not have the option to work remotely, encountered unique difficulties as they adjust to environments that involve increased monitoring.

In *Employee Surveillance Technologies: Prevalence, Classification, and Invasiveness,* Cousineau et al. seeks three main objectives: The research reviews literature regarding employee surveillance technology with the aim of determining the prevalence of it. It classifies the software, which are identified in the paper as "bossware." (Cousineau et al., 2023). Finally, it provides data to establish a means of defining how invasive these are.

In *Surveillance and the Future of Work: Exploring Employees' Attitudes Toward Monitoring in a Post-COVID Workplace* researchers indicated that while some employees accepted some level of monitoring as necessary for business continuity and safety, there was widespread concern over the extent and intrusiveness of these practices. This research found that increased workplace surveillance has been normalized due to the COVID-19 pandemic, affecting employee perceptions of privacy and autonomy. The study identified a gap in employer-employee communication regarding surveillance practices and a general lack of policies that balance organizational needs with employee privacy rights. "Our findings suggest that workers—especially women—are responding to shifts in informational norms that spark new concerns over the appropriateness of these data flows while working from home or after returning to traditional work environments." (Vitak & Zimmer, 2023). This research emphasized a gender gap and concerns about how these may be addressed.

In a study for the Communications Workers of America (CWA) union focused its scope on call center workers, *Making Call Center Jobs Better: The Relationship Between Management Practices and Worker Stress*. This report identified workplace stressors and sought means to provide a summary of best practices to increase worker well-being and job satisfaction. Using a comparative analysis on survey responses of call center workers, this report concluded that amongst the surveyed workers the majority reported high levels of stress. The study demonstrated that when monitoring is mainly aimed at enforcing discipline, it tends to increase stress levels and decrease job satisfaction among employees. On the other hand, when surveillance was focused on training and supporting workers, the negative impacts on mental health are less severe. This suggested that it is essential to adopt a more balanced approach to monitoring that considers the diverse needs of employees, particularly regarding their mental health and overall well-being. The report used comparative analysis on survey responses to identify several factors, job titles, education levels, employees' perceptions of monitoring technology, how the technology is used, workers' job satisfaction and stress levels, the impact of stress in their personal lives, along with salary and performance data. This report concluded that amongst the workers surveyed the majority reported high levels of stress. (Doellgast & O'Brady, 2020). An important finding was that companies that used monitoring to train employees, rather

than strictly as a means of discipline, had the lowest stress levels and the highest reported job satisfaction. The report recommended higher levels of training, providing workers with more flexibility, providing oversight, and ensuring that any technologies used are primarily error-free.

The Impact of AI on Workplace Dynamics: A Study of Surveillance and Employee Wellness, Morgan & Smith (2023) examined the psychological and professional impacts of AI-enhanced surveillance on employees. Their study identifies a correlation between increased surveillance and adverse effects on mental health, job satisfaction, and intra-organizational trust.

In the article, *The Impact of Remote Work on Employee Productivity and Satisfaction,* Fathima and Kumar examined the evolving dynamics of remote work, particularly how it affects employee performance, job satisfaction, and work-life balance. The study aimed to provide a balanced perspective on the benefits and challenges of working remotely by using a mixed-methods approach, gathering both quantitative data through surveys and qualitative insights via interviews. The research focused on understanding key questions such as how remote work influences productivity, the ways it impacts job satisfaction, and the specific challenges employees face while working from home. Though the study did not test specific hypotheses, it assumed that remote work could have both positive and negative outcomes depending on several factors, such as the level of managerial support and access to resources. To measure these variables, Fathima and Kumar utilized surveys that gathered data on productivity, job satisfaction, and work-life balance. Interviews provided additional context, revealing personal insights about employees' remote work experiences. The data analysis included statistical methods to explore correlations in the quantitative data and thematic analysis for the qualitative responses. The findings showed that while remote work offers increased flexibility and autonomy, which boosts productivity and job satisfaction for many, there are also downsides. Some employees struggled with blurred boundaries between work and personal life, feelings of isolation, and communication difficulties. These challenges varied significantly based on job role, organizational culture, and individual circumstances. Fathima and Kumar recommended that organizations reevaluate their remote work policies, placing greater emphasis on supporting employee well-being and ensuring that flexibility does not come at the expense of connection and communication. Their exploration of isolation and communication barriers offered a valuable lens through which it can examine how AI tools may affect these dynamics.

Current governances:

The link between AI governance and corporate governance was found to be significant, as the latter defines how organizations interact with various stakeholders. Corporate governance set forth the principles guiding the relationships between management, shareholders, and external parties (Cihon et al., 2021). As AI systems have gained autonomy, the necessity for accountability has become increasingly critical, particularly in contexts where AI decisions have substantial consequences for individuals. Therefore, aligning AI governance with corporate goals and acknowledging the broader societal impacts of AI has become essential. This was discussed in *Corporate Governance of Artificial Intelligence in the Public Interest*. Three specific examples were provided. “Google’s Project Maven shows that workers and the media can collaborate to be particularly successful in influencing management.” (Cihon et al., 2021). Second, law enforcement and the use of facial recognition “demonstrates that novel research, activism by nonprofits, and broad media coverage can build on each other to achieve change in corporate governance.” (Cihon et al., 2021). The third example offered insights into how “the publication of potentially harmful research shows management, workers, and industry consortia interacting to establish, implement, and share best practices for AI in the public interest.” (Cihon et al., 2021).

Connection to *Data Governance: Data Governance* demonstrated that data governance plays a pivotal role in AI governance, as AI systems heavily depend on data for their operations (Abraham et al., 2019). Effective data governance entailed treating data as a valuable resource and clarifying roles in decision-making. This study reflected primarily on two questions: “What are the building blocks of data governance? Where do we lack in knowledge about data governance?” (Abraham et al., 2019). The researchers

determined the AI governance must also consider the complex models and algorithms that underlie AI systems. This research was able to define “a conceptual framework for data governance comprising six dimensions: governance mechanisms, organizational scope, data scope, domain scope, antecedents, and consequences of data governance.” (Abraham et al., 2019).

AI-powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them discussed the potential for AI-powered surveillance systems to enhance public safety and health monitoring, emphasizing the importance of robust governance to address privacy concerns and public trust. “Adopting AI-powered surveillance systems expose populations to an increased risk of power imbalance, based on the enabling of access to privileged information on individuals' private lives collected within and feeding the systems to provide intel to public authorities.” It found that public support for surveillance technologies like facial recognition and contact tracing depended significantly on their implementation being transparent and regulated. The article pointed out a lack of comprehensive regulatory frameworks and public engagement in the development and deployment of surveillance technologies, which hindered their acceptance and effectiveness. (Fontes, et al., 2023).

In *Defining Organizational AI Governance*, researchers demonstrated that IT governance provided a structure for decision-making, and accountability related to technology use including AI. By leveraging existing IT governance frameworks, organizations could navigate the complexities associated with AI technologies, which were characterized by their adaptive and evolving nature (Mäntymäki et al., 2022). This paper explored how the topic of fairness within AI governance could be applied to a practicable governance. This study identified and explained “at least four necessary steps in developing AI governance towards a mature field” and those included a need to combine academic and “gray literature” for a more complete understanding of AI. (Mäntymäki et al., 2022). Secondarily, the paper stated that a need for “a more contextual under-standing of how organizations translate AI ethics principles to practice.” (Mäntymäki et al., 2022).

Key Findings from the Review of the Current Legal Landscape in Canada

Canada's current legal framework does not include comprehensive legislation specifically governing the ethical use of Artificial Intelligence (AI). While initiatives such as the Algorithmic Impact Assessment (AIA) (Government of Canada, 2021) and the Digital Charter (Government of Canada, 2019) have been introduced to address AI-related risks, there remains a lack of a standalone, enforceable law that clearly establishes ethical standards for transparency, accountability, and the mitigation of biases in AI systems. This absence of comprehensive regulation creates uncertainty regarding the ethical use of AI, particularly in workplace settings.

The regulation of algorithmic bias is also insufficient in Canada. The AIA focuses on identifying risks related to AI systems but lacks robust enforcement mechanisms to address algorithmic bias. Although the Canadian Human Rights Act (CHRA) (Government of Canada, 1985) protects against discrimination, it does not specifically target bias in AI, leaving a gap in regulations for monitoring and rectifying biases in AI systems, especially in high-risk sectors such as employment and law enforcement.

Privacy concerns raised by AI technologies are not adequately addressed by the Personal Information Protection and Electronic Documents Act (PIPEDA) (Government of Canada, 2000). While PIPEDA regulates the collection, use, and disclosure of personal data, it does not consider the complexities of AI, particularly regarding how machine learning algorithms process personal data. As a result, there is insufficient guidance on issues such as data ownership, consent, and privacy within AI-driven decision-making systems, potentially leading to violations of privacy rights in workplaces.

Despite the Digital Charter advocating for transparency in AI, there is no enforceable regulation that requires AI systems to be explainable. Many AI systems, particularly those based on deep learning, are often opaque, making their decision-making processes difficult to understand. While the AIA offers some

guidance on assessing AI systems' impacts, it does not mandate that these systems provide clear, understandable explanations, particularly in critical fields like employment and healthcare, where AI decisions can significantly affect individuals' lives.

Canada also lacks a centralized governing body to oversee the ethical implementation of AI systems. While the Pan-Canadian Artificial Intelligence Strategy (PCAIS) (Government of Canada, 2017) promotes research and innovation in AI, it does not provide a comprehensive governance structure for ensuring the ethical deployment of AI in practice. This decentralized governance approach results in inconsistent oversight and insufficient monitoring of AI's real-world effects, especially in high-risk environments such as hiring, criminal justice, and healthcare. Furthermore, existing laws do not clearly define liability when AI systems cause harm or discrimination, which leads to ambiguity regarding accountability among developers, employers, and government agencies.

Canada's AI regulations are largely domestic, limiting the country's ability to address global challenges posed by AI technologies. While the Digital Charter encourages international cooperation, Canada's national regulations do not effectively address the cross-border flow of data or establish global standards for AI ethics. As AI operates across borders, national policies alone are insufficient to tackle the global challenges associated with AI or to ensure consistent ethical standards across jurisdictions.

Current regulatory frameworks like the AIA primarily focus on identifying and assessing the risks of AI systems after they have been deployed, rather than preventing these risks during the development phase. This reactive approach means that AI systems may already be in use before potential risks are thoroughly evaluated or mitigated. There is a need for more proactive policies that ensure AI systems are designed and tested for ethical considerations, transparency, and fairness before they are implemented.

Finally, the use of AI in the workplace, especially for surveillance and performance monitoring, is not sufficiently addressed in Canada's existing legal frameworks. Although the CHRA prohibits discrimination, it does not specifically address the implications of AI-driven decision-making in employment contexts. Current laws do not require employers to obtain explicit consent from employees before introducing AI tools or to provide transparency regarding how these systems will be used in performance evaluations. Furthermore, employees lack legal avenues to challenge AI-generated decisions or to gain insight into the algorithms that influence workplace decisions.

Methodology

Research Design

A qualitative research design was employed to explore the effects of AI-enabled surveillance on employees' mental health and job satisfaction in remote work environments. This approach was chosen because it enables a deep understanding of participants' personal experiences, capturing their emotions, perceptions, and interactions with AI monitoring systems. The goal of this design was to provide a thorough examination of the psychological and ethical implications of AI surveillance, allowing for the exploration of participants' lived experiences.

Data Collection

Primary data were collected through semi-structured interviews with remote workers who had direct experience with AI-powered surveillance tools. This interview format was selected for its flexibility, as it allowed participants to provide detailed, open-ended responses while also giving the interviewer the ability to follow up on specific areas of interest. This approach ensured that the psychological and ethical effects of AI surveillance were explored in depth, generating rich insights.

The interviews were conducted online, which ensured accessibility for participants from various geographic locations, making the study more inclusive. This also allowed participants to share their experiences in a

setting that was familiar and relevant to their daily work, thereby enhancing the authenticity and context of the data collected.

Additionally, a literature review was conducted to contextualize the findings within the broader academic and professional discourse. The review focused on topics such as AI surveillance, workplace ethics, employee well-being, and job satisfaction. This provided a theoretical background against which the interview data could be interpreted and integrated into the existing body of research.

Sampling

Purposive sampling was used to select 12 participants who had direct experience with AI surveillance in remote work settings. This sampling method ensured that participants had firsthand knowledge of the topic and could offer relevant insights. The sample included individuals from diverse sectors and job roles, providing a variety of perspectives on the impacts of AI surveillance.

The sample size of 12 was deemed suitable for qualitative research, where the aim is to gain in-depth understanding rather than generalize the results to larger populations. Purposive sampling allowed for the selection of participants who could contribute meaningful and relevant data, ensuring that the study addressed the research objectives effectively.

Data Analysis

Thematic analysis was applied to examine the interview data. This method is commonly used in qualitative research to identify patterns and themes within the data. By using thematic analysis, the study identified key recurring themes such as the psychological effects of AI surveillance, including stress, anxiety, and changes in job satisfaction. Ethical concerns related to employee autonomy, data privacy, and trust in employers were also explored through this analysis.

Content analysis was used to develop governance recommendations, integrating insights from both the interview data and the literature review. This dual analysis approach helped create a framework that balances organizational goals with the well-being of employees, providing practical recommendations for managing AI surveillance in the workplace.

Ethical Considerations

Ethical guidelines were strictly followed throughout the research process. Participants were informed about the purpose of the study, their role, and their rights. Informed consent was obtained before any interviews took place, and participants were made aware that they could withdraw from the study at any time without penalty.

Confidentiality was a priority, and all participant data was anonymized. Security measures, including data encryption, were implemented to protect the sensitive information provided by participants. Mental health resources were offered to participants in case they experienced distress during the interview. These ethical considerations ensured the protection of participants' rights and well-being throughout the study.

Limitations & Future Research Opportunities

The study has several limitations. First, the purposive sampling method, while effective in selecting relevant participants, resulted in a small sample size of 12. This limits the ability to generalize the findings to larger populations or across different industries.

Second, the study relied on self-reported data, which may introduce biases such as social desirability or inaccurate recollection. Participants' responses were influenced by their own perceptions of AI surveillance, which may not always reflect the full scope of their experiences. Additionally, conducting interviews virtually may have limited the ability to observe non-verbal cues or detect subtle cultural differences in participants’ responses. Secondary research often was noted as being “worker-centric” and focused on

workers' experiences and views. This may have influenced researchers' viewpoint, although the research team attempted to remain partial and non-biased when considering ways to address ethical issues related to AI-powered surveillance technologies.

Due to the global reach of this study, remote workers were included from numerous countries including Brazil. Four participants did request the use of language translations services, as their primary language is Portuguese. Researchers used ChatGPT, an AI system, to translate the questionnaire from English to Portuguese. Prompts used during this were "translation the following into Portuguese" along with the interview questionnaire, and upon receipt, researchers used the prompt "translate the following into English" along with the participant's responses to review the data. See Appendix 1 for English Questionnaire, and Appendix 2 for Portuguese translation.

Despite these limitations, the study provides valuable insights into the psychological and ethical impacts of AI surveillance in remote work settings. The findings contribute to the growing body of research on the topic and offer a foundation for future research and policy recommendations. Future research recommendations of this study are the use of a practical application of this framework in comparison to workers who do not have clear guidance with AI-powered surveillance software to see if the use of the Seven Guiding Principles for the Ethical Use of AI-based Surveillance Software Governance Framework helps to alleviate the negative impacts of AI-powered surveillance software with workers.

Results and Discussion

Theme 1: Ethics and Legality in Data-Driven Technologies

Results:

The analysis of the primary data highlighted that employees' views on the ethical and legal aspects of AI-powered surveillance played a critical role in shaping their attitudes toward workplace monitoring. A recurring concern among participants was the lack of transparency regarding the extent of monitoring and the use of the data collected. Many employees expressed discomfort over the fact that they were unaware of how much data was being gathered, its specific purposes, or who had access to it. In several instances, participants voiced that although AI monitoring was a known factor, clear communication regarding its legal implications was often missing. This lack of transparency created an atmosphere of uncertainty, reinforcing the need for more clearly defined ethical standards and legal frameworks.

Supporting literature underscores this concern, with research by Georgieva et al. (2022) highlighting the tension between the development of surveillance technologies and the necessity for comprehensive ethical guidelines. Additionally, Rudiyanto et al. (2023) pointed out the deficiency of robust legal frameworks to adequately protect employees' privacy within the context of AI-powered surveillance systems. This gap in legal protection is consistent with the concerns raised by participants, who stressed the importance of clear regulations to govern the use of AI monitoring and safeguard personal data.

Discussion:

The findings from the primary data strongly suggest the need for greater attention to the ethical and legal aspects of AI-powered surveillance in the workplace. Employees are becoming increasingly aware of the data being collected but often lack insight into its scope, usage, and the legal protections available to them. As noted by Zimmerman & Fletcher (2023), this lack of transparency can create a sense of unease among employees, leading to diminished trust in their employers and the monitoring system itself.

Ethically, the issue centers around ensuring that AI surveillance is carried out fairly, transparently, and with respect for employees' privacy. Solaiman et al. (2023) emphasize that it is crucial for organizations to establish clear and transparent policies that govern data collection and usage. On the legal front, there is a

pressing need for comprehensive regulations that set boundaries on AI surveillance to protect employees from potential abuses.

In the Canadian context, the Personal Information Protection and Electronic Documents Act (PIPEDA) mandates transparency and consent regarding the handling of personal data. However, there are gaps in the application of these laws to AI surveillance tools, leaving certain aspects of employee privacy unprotected. In addition, existing legal frameworks may not fully address the unique challenges posed by AI monitoring, underscoring the need for specific regulations that account for the evolving nature of surveillance technologies in the workplace.

Theme 2: Impact on Employees

Results:

The psychological effects of AI-powered monitoring on employees emerged as another significant theme in both the interview data and the literature. The primary data indicated that many employees experienced heightened levels of stress, anxiety, and a general sense of being constantly observed. This contributed to lower job satisfaction. Numerous participants noted that while the intent of AI monitoring was to enhance productivity, it instead created pressure to maintain continuous performance, ultimately leading to burnout. As one participant expressed, “It feels like I’m always being watched, and it makes it harder to take a break or relax, even when I’m off the clock.”

In addition, several employees expressed frustration with the inaccuracy of AI tools in evaluating performance. For instance, one participant described how the system flagged minor lapses or moments of inattention, which negatively impacted their performance scores despite their overall productivity. This issue with AI’s accuracy in assessing human performance is consistent with the findings in the literature, such as those by Mettler (2023), who argued that AI monitoring systems often fail to capture the full complexity of human work, leading to incorrect assessments and added stress for employees.

Discussion:

The psychological toll of AI-powered surveillance is evident in the results, with employees reporting higher levels of stress, anxiety, and dissatisfaction due to the constant monitoring. These findings are in line with the broader literature, which indicates that constant surveillance can lead to adverse mental health outcomes, such as burnout and diminished motivation (Zimmerman & Fletcher, 2023). The fear of being perpetually observed can hinder employees' ability to relax or disengage from work, even outside working hours.

Moreover, the issue of AI accuracy in performance evaluation is a critical concern. Misrepresenting an employee's productivity can contribute to frustration, as employees may feel unfairly penalized for factors beyond their control. The literature also emphasizes the importance of ensuring that AI systems accurately reflect the nuances of human performance, as Becker et al. (2021) pointed out that misjudgments can exacerbate employee dissatisfaction and stress.

Given these findings, it is essential for organizations to balance the use of AI monitoring with consideration for employee well-being. Organizations should focus on using AI tools to support employees, rather than penalize them. AI can be a useful tool for providing feedback and identifying areas of improvement, but it should not be the sole determinant of an employee's performance or well-being.

In Canada, while the Canada Labour Code and PIPEDA provide some protections for workers, they do not fully address the complexities of AI-powered monitoring in remote work settings. As such, there are gaps in the legal framework that could leave employees vulnerable to the negative psychological impacts of such surveillance without sufficient safeguards or recourse.

Theme 3: Current Governance Practices

Results:

The governance of AI-powered monitoring systems was another key theme identified from both the interview data and the literature. Many employees expressed concern over the lack of clear governance regarding the use of AI surveillance in the workplace. While some acknowledged that AI tools had the potential to enhance productivity, they also highlighted the absence of clear policies on how these systems were implemented and governed. One participant remarked, "We were never told exactly what the AI is looking at, and there was no discussion about what data it's collecting."

Employees indicated that clearer governance policies would alleviate some of their concerns. Specifically, they emphasized the importance of having well-established guidelines surrounding data privacy, accuracy, and accountability to ensure that AI surveillance tools were used responsibly. This sentiment aligns with the findings in the literature, where Georgieva et al. (2022) stressed the need for comprehensive governance frameworks that ensure ethical and transparent use of AI technologies. However, as noted by Abraham et al. (2019), many organizations have yet to implement these frameworks, resulting in inconsistent and unclear governance practices.

Discussion:

The lack of clear governance surrounding AI-powered monitoring is a significant issue that needs to be addressed. The results from the primary data show that employees would feel more secure if there were clear, transparent policies governing the use of AI surveillance. Establishing a governance framework can help to clarify how data is collected, processed, and used, ensuring that employees understand their rights and the organization's responsibilities.

The literature supports the need for well-defined governance structures. Georgieva et al. (2022) argue that organizations must establish clear guidelines for the ethical use of AI monitoring systems to protect employees' privacy and ensure fairness in performance assessments. A transparent governance system would also include protocols for data protection, error correction, and accountability, which could foster trust between employees and employers.

In Canada, while PIPEDA and the Privacy Commissioner provide guidelines on data protection, there is a lack of specific legal frameworks governing the use of AI monitoring systems in the workplace. This creates a gap that leaves employees unprotected in cases where AI surveillance is used without adequate oversight. As a result, the development of comprehensive regulations that address the ethical and legal implications of AI monitoring in remote work settings is crucial.

Suggested Framework and Recommendations

Seven Guiding Principles for the Ethical Use of AI-based Surveillance Software Governance Framework:

Privacy, **Responsibility**, **Clarity**, **Autonomy**, **Transparency**, **Fairness**, **Trust**

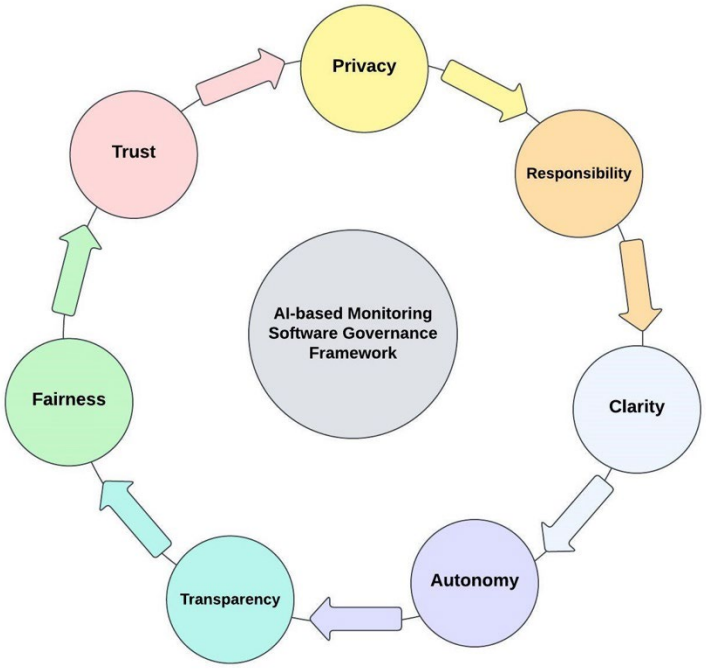

Figure 1.1: Seven Guiding Principles for the Ethical Use of AI-based Surveillance Software Governance Framework

Privacy: Use of AI-powered Surveillance should be limited to working hours, limited in scope to use only for systems owned and maintained by companies. Employers should consider all regional and specific laws pertaining to data privacy and ensure that data gathered is only of the employee and does not include employees' family or other household members.

Responsibility: Companies are responsible for safety and security in data gathering and storage to prevent any loss of employees' personal information. Companies should establish a time-to-deletion and ensure the safe destruction of personal data once employees separate. Employee data should not be provided to or sold to 3rd parties.

Clarity: Companies should provide clear, concise and easy-to-understand policies regarding AI-based surveillance software. Employees should be notified of its use, when it is used, how the data is gathered, and provided with information on the safe and secure storage of their data. Employees should give consent for its use and should be prompted to give consent for any changes to these established policies.

Autonomy: Companies should provide employees with the option to download a copy of their collected data, so that they might review what data has been gathered on them during working hours. Employees should be provided with a record of the full, secure deletion of their data once they have separated from the company, especially if terminated, to avoid concerns about data privacy once they are no longer employees.

Transparency: There should be transparency in how AI-based surveillance software is used regarding the assessment of employee behavior. All managerial decisions the utilize this data should allow employees to work with management for additional training opportunities should be provided if the data indicates any employee is failing to uphold company policies. AI-based surveillance software should not be used for disciplinary actions without providing employees with the opportunity to review and contest algorithmic-based decisions.

Fairness: There should be metrics to test all systems against biases. Using the current legal frameworks regarding the prevention of discrimination against workers with a focus on current laws, such Legislated Employment Equity Program (LEEP), including checks to prevent bias against those with disabilities.

Trust: All pillars should be accepted and agreed upon by both the company and the employees. Clear communication about data collection and storage policies should stress the importance of fostering trust for all employees. Companies should provide employees with the ability to notify any breeches of policies in a safe, anonymous way that protects against retaliation.

Actionable Recommendations:

The determinations that were discussed prior indicated a high need to inform employees of the full scope of data collection, usage, and storage. To ensure that employers meet recommendations for safe storage of data, researchers urge companies and organizations adopt compliancy standards such as the National Institute of Standards and Technology (NIST) SP 800-209, "Security Guidelines for Storage Infrastructure." (Chandramouli & Pinhas, 2020). The insurance of adherence to such standards allows for enhanced management and control over sensitive data. Such regulatory standards reduce the risk of data breaches, and any monetary losses associated with data breaches that may adversely impact businesses and organizations along with their employees.

Here are some Canadian Policies and recommendations for improvements:

Policy Name	**Current Scope/Limitations**	**Proposed Improvements with Steps**
Directive on Automated Decision-Making (ADM)	Limited to public-sector systems, leaving private-sector AI systems, like workplace monitoring, unregulated.	**Extension to Private Sector**: Expand the directive to cover private-sector applications of AI in workplaces. **Steps**: 1. Mandate risk assessments for AI systems before implementation. 2. Require organizations to document how AI systems affect employee mental health. 3. Introduce penalties for non-compliance and establish an independent monitoring body.
PIPEDA (Personal Information Protection and Electronic Documents Act)	Focuses on personal data use but lacks specific clauses for AI monitoring systems. Enforcement power is limited, leading to potential data misuse.	**AI-Specific Amendments**: Amend PIPEDA to include: 1. Mandatory employee consent before AI monitoring tools are implemented. 2. Restrictions on the type and amount of data collected. 3. Provisions for regular audits to ensure ethical AI use. 4. Enforceable penalties for misuse, including suspension of monitoring rights for repeat violations.
Pan-Canadian AI Strategy (PCAIS)	Primarily supports AI research and innovation, with no focus on	**Inclusion of Workplace AI Ethics**: 1. Fund research on the psychological impacts of AI monitoring.

	employee mental health or workplace AI ethics.	2. Develop a national certification program for ethical AI tools. 3. Provide tax incentives for businesses adopting certified ethical systems. 4. Host annual evaluations of certified AI tools to update standards.
Employment Standards Acts (Provincial)	Protects against traditional employment violations but fails to address the implications of AI monitoring on work-life balance and mental health.	**Work-Life Balance Provisions**: 1. Prohibit AI monitoring outside of working hours. 2. Enforce a "right to disconnect" policy. 3. Ban intrusive practices like webcam tracking without explicit justification. 4. Include clauses that allow employees to challenge decisions made by AI systems affecting their jobs.
Canadian Human Rights Act	Protects against discrimination but lacks proactive measures to address biases in AI systems, including in remote workplace monitoring.	**Anti-Bias Mandates for AI Tools**: 1. Require bias impact assessments before AI systems are deployed. 2. Mandate regular fairness audits of AI monitoring tools. 3. Establish an independent ombudsperson to address complaints related to AI bias. 4. Provide resources for employee training on their rights under these new regulations.
Workplace Safety Laws	Focused primarily on physical safety; psychological risks from AI monitoring are overlooked.	**Psychological Safety Enhancements**: 1. Include psychological risks as part of workplace safety laws. 2. Mandate biannual mental health surveys for employees working under AI monitoring. 3. Require stress management policies for workplaces using AI tools. 4. Impose fines for companies failing to address excessive stress or burnout linked to AI usage.

Conclusion

This study examined the influence of AI-powered monitoring on employee mental health and job satisfaction in remote work environments, with an emphasis on ethical, legal, and governance dimensions. The findings from both the interviews and existing scholarly research provide critical insights into how technology intersects with employee well-being and organizational practices.

The results reveal that ethical and legal considerations significantly shape employees' perceptions of workplace surveillance. Transparency, clear governance policies, and respect for privacy were identified as essential elements for addressing employee concerns about data collection and usage. The lack of comprehensive legal protections, as evidenced by gaps in Canadian regulations such as PIPEDA, highlights

the need for enhanced legislative measures to address the unique challenges posed by AI surveillance. These findings align with existing research, such as that by Georgieva et al. (2022) and Rudiyanto et al. (2023), which emphasize the tension between technological progress and the establishment of robust ethical standards.

Psychologically, AI monitoring has a notable impact on employees, often resulting in heightened stress, anxiety, and diminished job satisfaction. While these systems are designed to optimize productivity, they frequently lead to adverse effects due to the pressure of constant observation and inaccuracies in performance assessment. These insights are consistent with Zimmerman and Fletcher's (2023) assertion that persistent surveillance can undermine trust and motivation. Additionally, the study echoes concerns raised by Becker et al. (2021) about the inability of AI systems to fully comprehend the complexities of human labor, underscoring the need for thoughtful implementation strategies.

From a governance standpoint, the absence of well-defined policies exacerbates concerns among employees. Participants underscored the importance of frameworks that regulate data collection, storage, and usage while ensuring fairness and accountability. The proposed Seven Guiding Principles for Ethical AI Surveillance offer a structured approach to these issues, focusing on privacy, responsibility, clarity, autonomy, transparency, fairness, and trust. These principles build on theoretical perspectives, such as those outlined by Solaiman et al. (2023) and Georgieva et al. (2022), which advocate for ethical and transparent AI governance.

In addressing the research questions, the study provides a detailed understanding of how AI surveillance impacts employee well-being and workplace dynamics. The findings highlight the necessity of ethical practices, robust legal safeguards, and transparent governance to mitigate the negative consequences of monitoring while fostering a trust-based work environment. This synthesis of findings with existing literature underscores the importance of creating balanced strategies that support organizational goals without compromising employee mental health and job satisfaction.

This research offers valuable recommendations for organizations and policymakers, contributing to the ongoing discourse on AI surveillance. By developing robust governance models and regulatory frameworks, organizations can ensure the ethical and responsible use of AI technologies. Future studies could further refine these recommendations by exploring their application across diverse industries and organizational settings.

References

Fathima, M., & Kumar, B. N. S. (2024). The impact of remote work on employee productivity and satisfaction: Analyzing how remote work trends have affected various aspects of employee performance and well-being. *Educational Administration: Theory and Practice, 30*(5), 1323-1329. https://doi.org/10.53555/kuey.v30i5.3080

PayScale. (2024). Share of employees working primarily remotely worldwide 2015-2023. *Statista*. https://www.statista.com/statistics/1450450/employees-remote-work-share/

Field, H. (2024, February 10). *How Walmart, Delta, Chevron and Starbucks are Using AI to Monitor Employee Messages*. CNBC. https://www.cnbc.com/2024/02/09/ai-might-be-reading-your-slack-teams-messages-using-tech-from-aware.html

Bryan, V., Sood, S., & Johnston, C. (2024, June 20). *Analysis on Artificial Intelligence Use by Businesses in Canada, Second Quarter of 2024*. Statistics Canada. https://www150.statcan.gc.ca/n1/pub/11-621-m/11-621-m2024008-eng.htm

Mantello, P., & Ho, M.-T. (2024). Emotional AI and the future of wellbeing in the post-pandemic workplace. *AI & Society, 39*(3), 1883-1889. https://doi.org/10.1007/s00146-023-01639-8

Banerjee, S., Agarwal, A., & Bar, A. K. (2024). Securing well-being: Exploring security protocols and mitigating risks in AI-driven mental health chatbots for employees. *American Journal of Computer Science and Technology, 7*(1), 1-8. https://doi.org/10.11648/j.ajcst.20240701.11

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: Why we (might) need them and how we want them. *Technology in Society, 71*, 102137. https://doi.org/10.1016/j.techsoc.2022.102137

Mettler, T. (2023). The connected workplace: Characteristics and social consequences of work surveillance in the age of datification, sensorization, and artificial intelligence. *Journal of Information Technology, 39*(3), 547-567. https://doi.org/10.1177/02683962231202535

Mettler, T., & Naous, D. (2022). Beyond panoptic surveillance: On the ethical dilemmas of the connected workplace. *Proceedings of the Thirtieth European Conference on Information Systems (ECIS 2022)*, Timisoara, Romania. https://doi.org/10.1111/ecis.2022

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, 28*(4), zmad007. https://doi.org/10.1093/jcmc/zmad007

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49,* 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Becker, W., Belkin, L., Tuskey, S., & Conroy, S. (2022). Surviving remotely: How job control and loneliness during a forced shift to remote work impacted employee work behaviors and well-being. *Human Resource Management, 61*(1), 123-137. https://doi.org/10.1002/hrm.22102

Bernhardt, A., Kresge, L., & Suleiman, R. (2021). *Data and Algorithms at Work: The case for Worker Technology Rights*. UC Berkeley Labor Center. https://laborcenter.berkeley.edu/data-algorithms-at-work/

Cihon, P., Schuett, J., & Baum, S. D. (2021). Corporate governance of artificial intelligence in the public interest. *Information, 12*(7), 275. https://doi.org/10.3390/info12070275

Cousineau, L. S., Ollier-Malaterre, A., & Parent-Rocheleau, X. (2023). Employee surveillance technologies: Prevalence, classification, and invasiveness. *Surveillance & Society, 21*(4), 447-468. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

Doellgast, V., & O'Brady, S. (2019). *Making call center jobs better: The relationship between management practices and worker stress: Executive summary*. https://doi.org/10.13140/RG.2.2.27663.53923

Georgieva, I., Lazo, C., Timan, T., & van Veenstra, A. F. (2022). From AI ethics principles to data science practice: A reflection and a gap analysis based on recent frameworks and practical experience. *AI Ethics.* https://doi.org/10.1007/s43681-021-00127-3

Khogali, H. O., & Mekid, S. (2023). The blended future of automation and AI: Examining some long-term societal and ethical impact features. *Technology in Society, 73*, 102232. https://doi.org/10.1016/j.techsoc.2023.102232

Mäntymäki, M., Minkkinen, M., Birkstedt, T., Viljanen, M. Defining organizational AI governance. *Journal of Business Research, 144,* 33-42. https://doi.org/10.1007/s43681-022-00143-x

Rudiyanto, T., Kunda, H., Dunn, A., Shenderovskiy, S., & Gibson, R. (2023). Ethical and legal concerns of artificial intelligence in the workplace: Examining current legislations in the United States. *Lex Publica*, *10*(1), 84–100. https://doi.org/10.58829/lp.10.1.2023.84-100

Solaiman, B., Malik, A., & Ghuloum, S. (2023). Monitoring Mental Health: Legal and Ethical Considerations of Using Artificial Intelligence in Psychiatric Wards. *American Journal of Law & Medicine, 49*(2), 250-266. https://doi.org/10.1017/amj.2023.30

Chandramouli, R., Doron Pinhas, U.S. Department of Commerce, National Institute of Standards and Technology, & Continuity Software. (2020). Security guidelines for storage infrastructure. In National Institute of Standards and Technology, *NIST Special Publication 800-209*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-209

Government of Canada. (1985). *Canadian Human Rights Act*. Justice Laws Website. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/H-6/

Government of Canada. (2000). *Personal Information Protection and Electronic Documents Act*. Justice Laws Website. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Government of Canada. (2017). *Pan-Canadian Artificial Intelligence Strategy*. Innovation, Science and Economic Development Canada. Retrieved from https://ised-isde.canada.ca/site/ai-strategy/

Government of Canada. (2019). *Digital Charter Implementation Act*. Innovation, Science and Economic Development Canada. Retrieved from https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

Government of Canada. (2021). *Algorithmic Impact Assessment Toolkit*. Government of Canada. Retrieved from https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

Appendix 1: Questionnaire Used for Interviews

General Perception and Experience

1. Could you tell me a bit about your experience with AI monitoring tools in your remote work setup?
2. Did you know much about these tools before you started working remotely? How aware were you of their presence and purpose?
3. How has AI monitoring affected your daily work routine? Have you noticed any changes?

Mental Health and Job Satisfaction

4. Can you describe how the presence of AI monitoring at work affects your mental health? Could you share a bit more about how?
5. Are there any specific moments that come to mind where AI monitoring added to your stress or made you feel anxious?
6. Have you noticed any changes in your stress or anxiety levels due to AI monitoring? Explain your answer.
7. How does AI monitoring impact your work-life balance in a remote work setting?
8. Do you feel more, or less, motivated to perform your tasks when you know AI monitoring is in place?

Privacy and Trust

9. Has AI monitoring had any impact on your trust in the company or your managers?
10. Do you feel the monitoring process respects your privacy? Could you explain why or why not?
11. Are there any concerns you have about how the data collected from monitoring is used?

Ethical Considerations

12. Do you think your company's current AI monitoring practices are ethical? Why or why not?
13. What ethical questions do you feel arise from using AI to monitor remote work?
14. If you could make changes to improve the ethics of AI monitoring, what would you suggest?
15. How fair and transparent do you feel the company's AI monitoring policies are?

Trust and Organizational Relationship

16. Has the presence of AI monitoring affected how much you trust your organization or management?
17. What kinds of concerns might you have regarding how your data is collected and used through AI monitoring? What makes you feel that way?
18. How has AI monitoring influenced your relationship with supervisors or teammates, if at all?

Governance and Policies

19. How well do you feel you understand the company's policies on AI monitoring and how your data is used?

20. Do you think there are enough policies in place to protect employees from possible misuse of AI monitoring data?
21. What kind of strategies do you think could help manage AI monitoring tools responsibly in the workplace?
22. How might the governance around AI monitoring be improved to better support employees?

Recommendations and Future Perspectives

23. What advice would you give to companies thinking about using AI monitoring for remote workers?
24. How do you imagine AI monitoring might change for remote work in the future?
25. If you could change one thing about how data is collected and stored in your organization, what would it be?
26. How could companies strike a better balance between the benefits of AI monitoring and supporting employees' mental well-being?

Appendix 2: Questionnaire Used for Interviews Translated into Portuguese

Percepção Geral Experiência

1. Você poderia me contar um pouco sobre sua experiência com as ferramentas de monitoramento de IA no seu ambiente de trabalho remoto?
2. Você sabia muito sobre essas ferramentas antes de começar a trabalhar remotamente? O quão ciente você estava da presença e do propósito delas?
3. Como o monitoramento de IA afetou sua rotina diária de trabalho? Você notou algum mudança?

Saúde Mental Satisfação No Trabalho

4. Você poderia descrever como a presença do monitoramento de IA no trabalho afeta sua saúde mental? Poderia compartilhar um pouco mais sobre como isso acontece?
5. Existem momentos específicos que vêm à sua mente em que o monitoramento de IA aumentou seu estresse ou fez você se sentir ansioso?
6. Você notou alguma mudança nos seus níveis de estresse ou ansiedade devido ao monitoramento de IA? Explique sua resposta.
7. Como o monitoramento de IA afeta seu equilíbrio entre vida profissional e pessoal em um ambiente de trabalho remoto?
8. Você se sente mais ou menos motivado para realizar suas tarefas quando sabe que o monitoramento de IA está em vigor?

Privacide E Confiança

9. O monitoramento de IA teve algum impacto na sua confiança na empresa ou nos seus gestores?
10. Você sente que o processo de monitoramento respeita sua privacidade? Poderia explicar por que ou por que não?
11. Você tem alguma preocupação sobre como os dados coletados pelo monitoramento são utilizados?

Considerações Éticas

12. Você acha que as práticas atuais de monitoramento de IA da sua empresa são éticas? Por que ou por que não?
13. Quais questões éticas você acredita que surgem ao usar IA para monitorar o trabalho remoto?
14. Se você pudesse fazer mudanças para melhorar a ética do monitoramento de IA, o que sugeriria?
15. Quão justas e transparentes você acha que são as políticas de monitoramento de IA da empresa?

Confiança E Relacionamento Organizacional

16. A presença do monitoramento de IA afetou a sua confiança na sua organização ou na gestão?
17. Quais tipos de preocupações você poderia ter em relação a como seus dados são coletados e usados pelo monitoramento de IA? O que faz você se sentir assim?
18. Como o monitoramento de IA influenciou seu relacionamento com supervisores ou colegas de equipe, se é que influenciou?

Governança E Políticas

19. O quão bem você sente que entende as políticas da empresa sobre o monitoramento de IA e como seus dados são usados?
20. Você acha que existem políticas suficientes para proteger os funcionários contra o possível uso indevido dos dados de monitoramento de IA?
21. Que tipo de estratégias você acha que poderiam ajudar a gerenciar as ferramentas de monitoramento de IA de forma responsável no ambiente de trabalho?
22. Como a governança em torno do monitoramento de IA poderia ser aprimorada para apoiar melhor os funcionários?

Reconmendaçoes E Perspectivas Futuras

23. Que conselho você daria para as empresas que estão pensando em usar monitoramento de IA para trabalhadores remotos?
24. Como você imagina que o monitoramento de IA pode mudar para o trabalho remoto no futuro?
25. Se você pudesse mudar uma coisa sobre como os dados são coletados e armazenados em sua organização, o que seria?
26. Como as empresas poderiam encontrar um melhor equilíbrio entre os benefícios do monitoramento de IA e o apoio ao bem-estar mental dos funcionários?