Original Research Paper

Challenges and Opportunities of Electronic Workplace Surveillance in the Public Sector in Zimbabwe

Simbarashe Tongai[1], Farai Ncube[1], Mildred Mahapa[2]

[1] *Department of Human Resource Management, Faculty of Social Sciences, Midlands State University Zimbabwe. Zimbabwe.*

[2] *Department of Business Administration, Faculty of Social Sciences, National University of Lesotho. Lesotho.*

Abstract: Workplace surveillance is taking the world of work by storm and is becoming the flavour of the moment as a form of scientific supervision. This study sought to unpack the challenges and opportunities of electronic workplace surveillance systems in a selected Public Sector Organisation in Zimbabwe. The study adopted qualitative research using a sample size of twenty-one participants drawn from a population of 105 employees. Primary data was collected through semi-structured questionnaires and interviews, and secondary data was gathered using company records. Findings revealed various forms of surveillance including but not limited to the use of closed-circuit television (CCTV), biometric logging, vehicle tracking, telephone tapping email, and internet monitoring. Opportunities identified centered on the possibility to increase productivity, enhancing security, curbing abuse of organizational resources, and curbing sexual harassment and bullying at the workplace. Challenges identified were the invasion of privacy, the perpetuation of power dynamics, exertion of stress, emotional labour, the killing of innovation spirit, and erosion of trust between employees and employer. The researchers recommend crafting a robust surveillance policy that clears set guidelines, and parameters and provide remedial pathways in the public sector.

Keywords: Challenges, Workplace Surveillance, Opportunities.

1. Introduction

The introduction of an artificial eye through various forms of electronic surveillance was motivated by the need to eliminate laziness and manage resource utilization, activities, and behaviours of employees at the workplace [1]. The possibilities for employee monitoring have expanded and strengthened in recent years due to changes in the technologies available, managerial culture, and new organizational structures. Monitoring and data collecting are integrated more and more as the foundation for management, surveillance, and performance assessment [2].

With the advent of the Personal Computer (PC) and the digitization of data near the end of the 20th century, societal monitoring has changed and reached previously unimaginable heights, both technically and practically. The workplace is likewise subject to increasing levels of surveillance. All ranks of employees are increasingly being monitored closely. Even though the surveillance is disguised as performance monitoring and annual reviews, it still requires some sort of surveillance [1].

Globally, the question of monitoring employees' behavior at work is delicate and frequently divisive [3]. Electronic monitoring is typically used by employers to ensure the safety of their workers and properties [2]. Cameras are typically used to record the behavior of both staff and visitors to their buildings. Employers who wish to make sure that workers don't squander time at work primarily rely on workplace surveillance [4]. According to Fernandez and Gallardo-Gallardo [4], the capitalist economy uses workplace surveillance more frequently than other economic systems. "Any gathering and processing of information, whether personally identifiable or not, for the purpose of influencing and managing persons whose data have been gathered" is what is meant by surveillance [5]. A surveillance act requires the deliberate collecting of data about something or someone. Following a reasonable and systematic analysis of such information, the results are subsequently used to modify the initial surveillance target's behavior. Data must be gathered, analyzed, and then applied in a process of influence on the original data target for a phenomenon to qualify as surveillance. There is always a power play involved in surveillance (ibid).

Employee monitoring acts, according to Bryant [6], include keeping an eye on internet links, going over emails, using the phone, keeping track of computer files and reviewing them, recording employee job performance on video, listening to voicemails, and using video surveillance for security reasons. Dahlqvist and Matsson [7] pointed out that EPM systems are designed to give businesses access to their workers' computers and phones so they can keep tabs on how much time is spent online and increase productivity. Due to this contradiction, employers must build a security mechanism for every data they collect in order to prevent the theft of sensitive data, especially from sources outside the organization [8].

The main goal of any business venture is to make profits. That low productivity and faulty operational measures can ruin this goal is no breaking news. It is common to find workers chit-chatting during working hours leading to low productivity [2].

Global employee surveillance intensified as a result of the COVID 19 epidemic [1]. Others required workers to report their travel destinations while off the job. Surveys in Norway and the UK also showed a rise in employee anxiety over digital surveillance [1]. In South Africa, the Surveillance Device Act of 1994, which was further updated in 1999, contains rules regarding workplace surveillance [9]. The Act permits businesses to keep an eye on how their staff members are acting and behaving while they go about their everyday tasks in an effort to cut down on theft and social loafing.

In Egypt, any e-mail and internet monitoring carried out by the employer is legal as long as the monitored devices are owned by the employer and the employees are given advance notice [1]. While it is sometimes prohibited to monitor personal emails and the internet, it is acceptable to videotape employees at work as long as they are made aware of the monitoring and given advance notice. However, employees criticized the violation of privacy and saw surveillance as a blatant indication of mistrust on the part of management and employers [10].

In Zimbabwe, workplace surveillance policies are still in its infant stages. However, employers are guided by their specific Employment Codes and ILO ratified conventions. The surveillance cameras were put in place after it was noted that the Beitbridge border post was the most porous border post in Zimbabwe [4]. People were seen entering and leaving the border post without proper searches and declarations. Corruption and bribery were a common thing at the border post. After the adoption of such a technology the surveillance cameras managed to detect several criminal activities committed by ZIMRA employees, security agencies as well as from civil servants particularly from Immigration [10]. The introduction of workplace surveillance brought some sanity to the border post.

2. Literature Review

Electronic surveillance is the practice of secretly or openly filming, listening to, or observing someone in real time [1]. It generally entails watching the workspace and employees' actions or covertly listening to employees [2]. Electronic devices such as cameras, wiretaps, computers, and microphones are used to observe or monitor. Employers primarily employ workplace monitoring to encourage high production, manage resource usage, prevent theft, and guarantee workers' safety [2]. Electronic surveillance is often carried out covertly and does not obstruct a person's regular activities. Typically, a surveillance activity entails one or more people employing cameras, long-range microphones, listening devices, as well as keeping an eye on cell, workplace, and home phone services to observe and record the acts of another person (ibid). The expression "big brother is watching" is not new among staff members and suggests that a location is being watched. Most enterprises around the world have adopted electronic surveillance systems, making them more productive and streamlining processes [11]. Power is usually used during surveillance [11]. Over the past 20 years, technological improvements have increased the usage of workplace surveillance, freeing supervisors from the burden of manually observing and documenting employee behavior [8]. With the development of technologies, workplace surveillance and monitoring has changed, posing a growing number of opportunities, risks, and ethical dilemmas [12]. A surveillance act requires the deliberate collecting of data about something or someone. The results of that study are then used to modify the behavior of the initial target of surveillance after being rationally and systemically analyzed [5].

2.1. Technology Acceptance Model

The information systems (IS) community has been interested in how people accept technology for more than 20 years [13]. Lack of user acceptance is a major obstacle to the adoption of new information systems [14]. The theory asserts that, firms face challenges when users reject information systems that are recommended to improve organizational performance. Technology Acceptance Model (TAM) assumes that the user perceptions of the system, users' behavioural intentions, perceived utility, and perceived usability will influence whether a new IS is accepted [15]. Accessibility to the system, self-efficacy, and subjective norms are additional factors that affect system adoption [16]. The implementation of electronic surveillance is frequently met with resistance, as with any transition process. Other academics maintain that individuals - not organizations - are the ones who bring about change, therefore it starts and ends with people. The methodology was useful in this study because it provided an explanation for why new technologies, like the adoption of electronic monitoring systems in organizations, are commonly met with opposition. The model was essential to the study because it clarifies why employees usually embrace new technology at work more slowly than anticipated. The model is particularly important since it suggests potential factors that could determine whether new technologies are accepted, which organizations can use as a foundation and then strengthen when introducing new technologies. The approach is essential to this research as it makes evident the value of education and knowledge-sharing whenever new technologies are introduced. In order to minimize user resistance and discomfort when introducing new systems and technologies, the model also highlights the importance of careful planning.

2.2. Rationale of Electronic Workplace Surveillance

Electronic employment surveillance is used by many businesses for a variety of reasons. The use of electronic surveillance is still a contentious topic, both at work and elsewhere. Businesses utilize electronic surveillance for three purposes: to preserve productivity and monitor how employees use resources; to protect trade secrets; and to give proof in the event of a legal dispute [1]. As a result, they employ it to control risk, quality, and cost. The managers' concern that workers spend the majority of their working hours on social networking sites, responding to personal emails, shopping, or even playing online games, which has a detrimental impact on their productivity at work, has led to the need to implement surveillance in the workplace [12]. While some companies check that cash has been handled properly, the bulk watch employee arrival times. Some businesses keep tabs on the correctness and effectiveness of their workers' work. This kind of monitoring is considered as a necessary for business, and the majority of firms would view it as utterly insane to not do such inspections [3]. However, a surprising percentage of businesses continue to improperly monitor how employees use their computers, which can be a very expensive oversight [16].

The need for employee monitoring software increased as a result of the epidemic, which forced millions of individuals to work remotely. When compared to 2019, the demand for personnel monitoring software surged globally by 108% in April and by 70% in May of 2020 [17]. When compared to searches made the year before, search engine queries for "How to monitor employees working from home" grew by 1,705 percent in April and by 652 percent in May 2020. Additionally, substantial spikes in sales inquiries were recorded by providers of employee surveillance software. Teramind had expanded by 169 percent, Desk Time by 333 percent, and KickIdler by 139 percent. Time Doctor, for instance, recorded growth of 202 percent in April 2020 compared to the prior year.

The main methods employed were communication screening, desktop monitoring, occasionally through camera, and social media monitoring. The BBC then revealed in 2021 that Tele performance, a large provider of contact centers, occasionally used webcams to snap pictures of staff at their workstations [17], which was deemed needless and excessive in the setting of the home [14].

2.3. Challenges of Electronic Workplace Surveillance

Since the early 1980s, when a multidisciplinary report titled The Electronic Supervisor: New Technologies, New Tensions, which was commissioned by the US Congress Office of Technology Assessment, examined its potentially negative effects, the risks of electronic surveillance in the workplace have been discussed [1]. Employees that are subjected to excessive surveillance at work suffer from increased stress, identity loss, and privacy difficulties [18]. The risks of electronic surveillance in the workplace have been discussed since the early 1980s, when a multidisciplinary report titled The Electronic Supervisor: New Technologies, New Tensions, which was commissioned by the US Congress Office of Technology Assessment, examined its potentially negative effects [1]. Employees that operate under constant monitoring experience higher levels of stress, identity theft, and privacy issues [18]. The aforementioned assertion can imply that employees are apprehensive about the system. When this happens, even if an employee was late for a valid reason, they may still face repercussions. The high job expectations connected with workplace surveillance have required employees to work incredibly hard. As a result, working under pressure at work becomes the norm, which raises the risk of stress [6]. Early research demonstrated its impact on employee stress levels. Electronic surveillance is most stressful when it does not represent employee efforts accurately, employees cannot challenge its results, it is applied to inappropriate tasks which are difficult to measure and employees have no say in its onset [1].

Employers use workplace surveillance to illegally access the intellectual property [6]. This frequently occurs when newly hired employees utilize their own computers at work. As a result, when their bosses keep an eye on how their workers use their computers, it's conceivable that they will sneak access to and utilize the employees' private information. In developing nations where the availability of tools of the trade is poor and workers may wind up carrying their own tools to work, the trend of having a high employee-to-computer ratio may be more common. These patterns suggest that workers view workplace surveillance as a management tool designed to protect their employers at their expense.

Employees believe that "privacy is a fundamental human right" [9]. Because this freedom is guaranteed by the constitution, they feel that anyone, even their employers, has the right to restrict it. The fact that employers verify everything without discriminating between official and private communications is the main source of concern for employees. Because their emails are their property and not the employers', employees object to measures like having the content of their emails verified [9]. Consequently, the later has no right to read their emails. This means that workplace surveillance especially through electronic means is an unnecessary invasion of employees' privacy.

. Employee privacy can be compromised if employees do not authorise the disclosure of their information and it is broadcast to unknown third parties [1]. Like all surveillance technologies, employee surveillance technologies can exhibit 'function creep.' This occurs when surveillance technologies yield more information than intended and management needs to avoid the temptation to extend surveillance practice without consulting employees first. Further, if employees realize their actions and communications are surveilled, innovation may be reduced if they are worried about monitoring and judgement [1]. When the obvious purpose of surveillance equipment is to monitor employee presence and performance, employees are more likely to see it as intrusive (ibid). Knowing that one is continuously being filmed might easily breed mistrust among co-workers, especially if it's obvious that the employer doesn't think that the employees are capable of working independently.

This anger can eventually produce issues for a company. Employers who disregard privacy pay a hidden price [1].

Low employee motivation is a result of the constant monitoring at work [13]. Employees grow disenchanted with their jobs as technology like computers acquire supervisory roles in the monitoring process. The majority of employees believe that being monitored at work turns them into tools that they are responsible for [13]. Computer-based performance reviews are unbalanced because they ignore other facets of an employee's performance, like their interactions with co-workers or their emotional health. Additionally, these reports prevent the personnel from defending their mistakes. In certain instances, workplace surveillance results in assessments based more on perception than actual information [5]. For instance, co-workers may exploit information gleaned from an employee via wiretaps against them. As a result, assessments based on this information can produce inaccurate findings.

Exacting surveillance also strongly communicates to employees the types of behaviours the company values or expects [1]. According to research, employees would give monitored jobs and the behaviours that monitoring promotes more attention since they are seen as more important or useful than non-monitored ones. Finally, overzealous surveillance occasionally results in the actions it was intended to curtail. Employees are likely to strive to evade and manipulate the limitations of when, where, and how they are measured if they believe that monitoring activities are intensification and extension of control. The emergence of counter-institutional websites, also referred to as "gripe" or "sucks" sites, which enable disgruntled workers and customers to post about their experiences—a form of electronic surveillance by employees over their employers that facilitates collective organization—is another development in worker resistance. Currently, there are approximately 7000 corporate-focused websites that use the word "sucks" or "sux" (ibid). It is challenging to become radicalized since technological surveillance is so pervasive [1]. Using irony and emphasizing how local monitoring regimes become contentious in the micro-dynamics of daily work life, Graham Sewell and James Barker have made headway in addressing this issue (ibid).

Electronic monitoring at work serves to maintain existing disparities and, as a result, reflects larger dynamics of power dynamics and social structure [4]. Any form of monitoring, according to Michel Foucault, has "circuits of profit" that favour the owners. As a result, the owners of capital benefit the most from electronic surveillance used at work. It is disproportionately applied against people who are minorities or women who are at the bottom of the organization. More powerful people are shielded from such scrutiny (ibid). Some claim it marks a return to the old-style technical control of work and has sparked a new wave of deskilling in the service industry (ibid). It keeps bringing up human rights issues. New automated workplace surveillance technologies that concentrate on physical features of the human body as well as those that blur the lines between work and non-work life raise a lot of privacy concerns. Last but not least, electronic monitoring is directly related to employment ethics because its outcomes might affect the procedural justice of consultation processes as well as the distributive justice of reward. There are still unanswered problems regarding how future generations' work will be shaped by the usage of electronic surveillance [15].

3. Methodology

The research used a qualitative research paradigm because it allowed for friendly contact and enabled human interaction and interface [8]. Making sure that the informants were guaranteed secrecy and that the researcher maintained confidentiality helped the study with ethical difficulties. The problems and prospects of workplace electronic monitoring systems in the public sector are investigated best using a naturalistic approach to qualitative research, which is based on natural phenomena. Although not of a numerical and statistical nature, qualitative research does seek some form of generalization [5]. The opportunity to infer social meaning from qualitative research gave the researchers the chance to employ physical trace measurements through the use of a case study of a selected public sector organisation. A case study is a type of qualitative analysis in which a social group is evaluated by the observer [13]. Dahlqvist & Matsson [7] defined a case study as one that is intensively designed to capture a complete picture of the topic and the setting in which it was being researched. The researchers collected data through interviews and focus group discussions as well as through a questionnaire that was administered online. Each interview lasted for more than 40 minutes. Document analysis which is the in-depth analysis of documents created across a wide range of social practices in a number of formats, such as written text and visual images was also conducted on all documents that were availed to the researchers by the participants and information available online

and library [14]. The target audience for this study included Chief Executive Officers, Commissioners, Directors of ICT, Directors of Human Resources grades.

This article followed all ethical standards of research. The exact name of the organisations remained anonymous as requested by the organisation.

4. Finding and Discussion

The study centered more on understanding the opportunities available for the parastatal in harnessing employee surveillance, as well as establishing the major challenges associated with the said move. Partly the study applied the Technology Acceptance Model to guide the study simply because of the contrasting views from literature on the merits and demerits of employee surveillance [18]. Through the interview and focus group discussions done the following section presents the major findings.

To have a clear picture the researchers first established the surveillance mechanisms in use. All participants identified the use of closed-circuit television (CCTV), biometric logging, vehicle tracking, telephone tapping as well as email and internet monitoring. Participants pointed out that these measures were communicated to all employees and apply to all employees irrespective of position or grade. Out of interest the researcher asked if employees were consulted in the decision or whether there were policies that governed the application and operationalization of such. Of interest was the submission by a senior responded who pointed out that the nature of business the commission was involved in centered on highly classified government information, where highly trusted employees are vetted into the commission for security reasons. As such surveillance was given. The rest of the participants submitted that while members were disgruntled no one had raised an official complaint as this impliedly insinuated resignation. However, of interest was that for executives or their tablets and laptops had two accounts, one for the individual which they claimed was not monitored and 1 for the organisation which was monitored. The privilege was given to executives and not all employees. Asked on how ethical was the application of surveillance participants highlighted that it was completely ethical since to the employer this assisted in several ways and internal polices pointed to such. The study established that there are a number of policies in the ITS departments and members could sign for gadgets, as well as vehicle trakers that check routes and speed, especially for company vehicles and personal issue vehicle.

4.1. Opportunities for Electronic Surveillance System

The 21 participants who took part in the study identified several opportunities owing to the use of different electronic surveillance mechanisms Enhanced security (88%), increased compliance (56%), curbing abuse of resources (75%) and wading bad practices like sexual harassment (51%) and bullying (50%) were identified as some of the opportunities of electronic surveillance.

The researcher asked respondent to expand on enhanced security. It was established that the use of biometric system and CCTV was mooted considering the Commission's past experiences where the offices were stormed and attacked. The attackers were not captured because there was no implicating evidence, and it was easy for them to access the offices. Particpnats also pointed out that with the use of all the surveillance mechanism employee compliance was at its level best, no one afforded to be late as the hours would be affected on the payroll for deductions. The same denied all visitors access unless they pass through security check point. Equally saved vehivles from abuse so is the internet as the system shows what people are searching for on the internet.

The study also established that cases of sexual harassment and bullying were recorded previously, and the use of CCTVs has been effective to mitigate against such cases. While harassment normally happens when people are alone cases of sending through the company network sexually suggestive messages and videos was eliminated. Other forms of harassment that happens in the corridors and public areas under surveillance have been managed as was pointed out by the participants.

The research established that the majority of employees constituting 54% believed that electronic surveillance increase productivity. The finding was that electronic surveillance enhance compliance to statutes and policies, increase employee attendance and reduce truancy leading to increased production. Moonlighting, and social loafing is reduced. There were however discerning voices constituting 5% who strongly disagreed and 5% who disagreed. The discerning voices argued that surveillance cause stress, demotivate and cause employees to make lot of mistakes thus causing low productivity.

The above findings were confirmed by Holland [12] who opines that employees deploy electronic surveillance system to curb wasting time through social networking sites, attending to their personal

emails, shopping or even playing online games, thereby negatively affecting their productivity at work place. The same idea was confirmed by West [3] who posits that through monitoring issues such as time wasting due to socializing at the workplace can be cut by up to 80% with CCTV cameras in place. This therefore confirms the authenticity research findings which can be generalized.

In terms of opportunities that comes with installation of worker surveillance findings revealed improved productivity and efficiency, as well as the protection of company property from malicious damage etc. Ball [1] suggest that monitoring employees through any form of surveillance assist the organisation in improving profitability and productivity as employees are keen to work knowing they are being monitored. Through monitoring issues such as time wasting due to socializing at the workplace can be cut by up to 80% with CCTV cameras in place [3]. Contrary to the popular belief, workplace surveillance is not just about security and workers' safety. Corporations in the modern economy consider workplace surveillance an effective control technique that can facilitate control over the workforce and an increase in productivity [10]. Intellectual property theft (IPT) has always been a concern for companies – and internet-connected computers and mobile devices provide new opportunities for people to access and steal data [13]. This collaborates well with issues raised by participants. Indeed, owing to the previous break in there was need to introduce all forms of surveillance to eliminate theft of both physical and intellectual property as supported by the scholars identified.

4.2. Challenges of Employee Surveillance Systems

Participants lamented over poor lack of privacy, emotional labour, resources, resistance and at times abuse by managers as some of the major challenges compromising the surveillance of workers. Excessive surveillance at workplaces have negative effects on employees such as increased stress, loss of identity and the emergence of privacy issues [11]. The findings concur with the views by Newell [11] who points out that in many surveys, it has been observed that the employees who are under surveillance are more likely to suffer from health, stress and moral problems [11]. On the other hand, just like participants workplace surveillance is used by employers to gain access to intellectual property illegally [6]. Participants pointed out that many workers consider workplace surveillance a control tool. Employees consider "privacy a guaranteed human right" [20] sequently, they believe that no one including their employers have the right to deny them this right since it is provided for by the constitution. Employees' main concern is the fact that employers verify everything without distinguishing between private communication and official communication. Employees' opposition to acts such as verification of the content of their emails is based on the fact that the emails are their properties and not the employers [9]. Participants also pointed out that they were not happy since it demotivated them. This is in line with the argument that the intense of surveillance at the workplace leads to low motivation among the workers [8]. Management also pointed out to resistance by some employees which is in line with the view that exacting surveillance also sends a strong message to employees about the kind of behaviours the employer expects or values [1]. Of concern from participant and literature is the fact that, excessive monitoring can sometimes produce the behaviours it was designed to prevent. If employees perceive surveillance practices as an intensification and extension of control, it is

From the findings, the researcher found out that most employees in the Public Sector constituting 76% do not want to work under any form of electronic surveillance. The cost of installation, invasion of privacy, employee resistance and emotional labour were found out to be the main challenges of the system. The researcher also found out that there is no policy governing implementation of electronic surveillance. Formal policies are virtually a prerequisite if a company wants to maintain effective control over the usage of surveillance systems. Just as importantly, a defined surveillance policy goes a long way to satisfy employees as they would be aware of what is expected from them. This poses danger to employees as there are no mechanism to deal with excessive surveillance and there are no pathways for remedies if one's rights are violated.

The findings were also confirmed by Morrison [14] who pointed out that electronic workplace surveillance perpetuate power dynamics at the workplace. West [3] concluded that investing in "SCIENTIFIC SUPERVISON" is beneficial to the employer not employees. Because capitalists prioritize deskilling labour since it is less expensive and easier to manage than a highly skilled workforce. The same idea is confirmed by the labour Process Theory findings that, rather than ensuring their security, the main objective of workplace surveillance is to regulate employees' behavior [1]. The labour process hypothesis states that modern management techniques utilize

scientific management components and are enhanced through workplace observation [1]. The findings confirm the authenticity of the model and relevance to the current study.

The outcome shocked the researcher as what could be problem. The researcher is of the view that the big denial can be a management problem. Earlier results indicate that the majority of the staff do not understand how the system operate. We cannot rule that induction training was either not properly done or was never done. Employee involvement is an ideal approach as it helps to eliminate denial chances. Majority of employees lamented lack of consultation and engagement when the installation was made. It is very normal that if you do not understand something, it also affects the willingness. The findings are confirmed by Technology Acceptance Model which opines that lack of user acceptance is a major obstacle to the adoption of new information systems especially if users are not properly inducted. Newell [11] confirm the same idea by pointing out that users reject information systems that are recommended to improve organizational performance if they are not fully consulted. Alharbi and Drew [15] confirmed the findings by pointing out that new technologies may face acceptance challenges if user perception issues like usability and intentions are addressed. The findings confirm the authenticity of the model and relevance to the current study.

The researcher found out that covid-19 intensified electronic surveillance in the Public Sector in Zimbabwe. 54% of employees strongly agreed that covid-19 saw heightened surveillance implementation particularly email tapping and vehicle tracking. The results therefore reveal a nexus between increased surveillance and monitoring and covid-19 pandemic. This is not surprising considering that remote working become the new normal hence the only surveillance systems at the disposal of the employer for employees who were not physically at the workplace was email tapping and vehicle tracking. The above findings are confirmed by Ball [1] conclusions after research in Germany, Belgium and England that Global employee surveillance intensified as a result of the COVID 19 epidemic. The European TUC has also received direct information concerning the rise in employee monitoring since the outbreak from delegates across the EU-27. The same findings are also confirmed by BBC (2021) which opined that when millions of people across the world had to work remotely during the pandemic, demand for employee monitoring applications soared. In 2020, global demand for employee monitoring software had increased by 108% in April and 70% in May 2020 compared to 2019. The findings confirm the authenticity of the study and shows that results can be generalized.

The researcher also found out that there is consensus that the use of electronic surveillance at workplace is a controversial practice. 100% of respondents either agreed of strongly agreed that the practice was very controversial. It is possible that the reason why the practice remain controversial to this day is due to insufficient information on the real challenges and opportunities of this practice. There is no adequate information on the successes stories of the implementation of the system hence the fear and controversy.

5. Conclusion

The research found out that the main issue surrounding surveillance is on how it is implemented not the system itself. The research therefore contributes into the body of knowledge on how electronic surveillance systems are important. However effective policies should be put in place to make the system effective. It is important to note that in as much as surveillance provide safe and secure workplace, surveillance usage appears to have a number of unintended consequences such as increased employee stress

The findings highlighted that the employment relationship is not a balanced affair as the two parties have different often conflicting interests. The employers owning the means of production and the employee owning labour, both parties aiming to advance personal interests at the expense of the other, conflict of interest becomes inevitable. The findings of the case study of the Public Sector showed that surveillance has killed the zeal and motivation of many employees, as they perceived invasion of privacy and unfairness of the practice. This led many employees to propose an abolishment of the practice as surveillance tend to demoralize them.

Employees believe that employers oppress their social life taking advantage of the ownership of the means of production. Due to the political (power from resource ownership) and economic environment which is characterized by high unemployment, employers also tend to deliberately overlook employees in the decision making on the use of surveillance as the situation reduces employees' power. On top, the organization does not have clear surveillance and communication

policies. Hence, a situation has emerged where employees are particularly dissatisfied and demotivated with their jobs.

Therefore, the research suggested recommendations such as clear and reasonable surveillance and communication policies, involvement and participation of employees in surveillance decisions and legislation that limits the unrestrained monitoring in the present environment

An unexpected negative response from respondents because they were unwilling to give out sensitive organizational information. When conducting surveys or requesting information from respondents, it's important to consider that some individuals may be unwilling to provide sensitive organizational information. There could be various reasons for this reluctance, such as concerns about privacy, confidentiality, or potential misuse of the information. To handle such situations, it's crucial to approach respondents with transparency and respect for their concerns. Here are a few steps you can take clearly communicate the purpose. Explain the purpose of the survey or the information you are requesting and how it will be used. Assure respondents that their information will be handled with utmost confidentiality and will only be used for the intended purpose. Assure anonymity: Emphasize that the survey responses will be kept anonymous, and any information provided will be aggregated and reported in a way that no individual or organization can be identified. This can help alleviate concerns about personal or organizational exposure. The subject matter is very sensitive. This was addressed through counter-checking Human Resources records and minutes of meetings conducted and a perusal of exit interview minutes for employees terminating. The Language barrier was another challenge in carrying out the study considering the diversity in the workplace. The researcher made use of an interpreter. Time and financial resources visiting all key informants could not permit but the methods deployed for the study are sufficient to elucidate the challenges and opportunities of the workplace surveillance system

This study may lead to more effective ways of a monitoring employee performance which will lead to enhanced employee performance

References

[1]   K. Ball, *Electronic Monitoring and Surveillance in the Workplace*. England: European Union Commission Publication Centre, 2021.

[2]   S. Ariss, "Computer monitoring: benefits and pitfalls facing management," *Information and Management*, vol. 39, no. 7, pp. 553-558, 2002.

[3]   R. West, *Marx's labor theory of value.* New York: University Press, 2005.

[4]   V. Fernandez, and E. Gallardo, "Tackling the HR digitalization challenge: key factors and barriers to HR analytics." Adoption Competitiveness Review, 2020.

[5]   G. W. Bohlander, and S. Snell, *Managing Human Resources*, Pennsylvania, Cengage Learning Press, 2010.

[6]   L. Bryart, *What are the pros and cons of monitoring employees using video surveillance?*, 2006.

[7]   A. Dahlqvist, and A. Matsson, *The Impact of Extrinsic and Intrinsic Rewards on Employees' Motivation; A Case study of an Insurance company*, Sweden: Lund University Direktory, 2015.

[8]   J. Mishra, and S. Orampton, "Employee monitoring: privacy in the workplace*?,"* *SAM Advanced Management Journal*, vol. 36, no. 1, pp. 2-10, 2020.

[9]   P. Edwards, and P. Ramirez, "When Should Workers Embrace or Resist New Technology*?,"* *New Technology, Work and Employment*, vol. 31, no. 2, pp. 99–113, 2016.

[10]   J. Stanton, and E. Weiss, "Electronic monitoring in their own words: an exploration study of employees' experience with new types of surveillance," *Computer in Human behavior*, vol. 46, no. 4, pp. 423-440, 2002.

[11]   B. C. Newell, *Police on Camera: Surveillance, Privacy, and Accountability*, London: Routledge, 2020.

[12]   P. J. Holland, B. Cooper and R. Hecker, "Electronic monitoring and surveillance in the workplace: the effects on trust in management, and the moderating role of occupational type," *Personnel Review*, vol. 44, pp. 161-175, 2015.

[13]   C. R. Kothari, *Research Methodology, Methods and Techniques, second revised edition*, New Delhi: New age international publishers, 2004.

[14]   T. Morden, *Principles of management*. New York: Ashgate Publishing, 2004.

[15] S. Alharbi, and S. Drew, "Using the Technology Acceptance Model in Understanding Academics' Behavioural Intention to Use Learning Management Systems," *International Journal of Advanced Computer Science and Applications*, vol. 5, 2014.

[16] D. Lyon, *Theorising Surveillance: The Panopticon and Beyond.* London: Routledge, 2006.

[17] D. T. Newman, N. J. Fast, and D. J. Harmon, "When eliminating bias isn't fair: Algorithmic reductionism and procedural justice," *Human Resource decisions Organizational Behaviour and Human Decision Processes*, vol. 160 pp. 149 – 147, 2020.

[18] S. Schafheitle, A. Weibel, I. Ebert, G. Kasper, C. Schank, and U. Leicht-Deobald, "No Stone Left Unturned? Toward a Framework for the Impact of Datafication Technologies," *Organizational Control Academy of Management Discoveries*, vol. 6, no. 3, pp. 455–487, 2020.