

financial
services
union

110 351 2567 1575
0101 0101 100111001 01110
STRONGER TOGETHER



Employee Experiences of
**TECHNOLOGICAL
SURVEILLANCE**
in Financial Services

A complex network diagram consisting of numerous blue and grey nodes connected by thin lines, forming a dense web-like structure that fills the right side of the page.

Employee Experiences
**TECHNOLOGICAL
SURVEILLANCE**
in Financial Services

**financial
services
union**

STRONGER TOGETHER



Table of Contents

List of Figures.....4
List of Tables.....4

FOREWORD5
The Research Team6

SECTION 1: INTRODUCTION7
 Research Background.....7
 Report Structure.....7
 Methodology8
 Survey Respondent Profile8

SECTION 2: SURVEY AND INTERVIEW RESULTS.....10
 Technological Surveillance10

SECTION 3: SURVEY FINDINGS.....17

SECTION 4: SYNOPSIS OF FINDINGS AND RECOMMENDATIONS19
 Findings19
 Recommendations.....19
 Reference notes.....21

List of Figures

Figure 2.1 Organisational Data Tracking of Employees’ Work.....10
Figure 2.2 Personal Impact of Surveillance11
Figure 2.3 Impact of Surveillance on Trust12
Figure 2.4 Fairness and Control13
Figure 2.5 Surveillance and Productivity13

List of Tables

Table 1. 1: Survey Participant Profile (Number and Percentage).....9
Table 1. 2: Survey Participant Area of Work9

FOREWORD

I would like to thank our research partners in the Department of Work & Employment Studies, Kemmy Business School, University of Limerick (UL) who collaborated with us on this research.

The FSU first commissioned this research in partnership with UL in 2019 and again in 2021 with a follow up survey carried out by the FSU in 2023.

The research project has sought to establish the experiences and attitudes of financial services employees to technological change in their job and this report focuses on employees' experiences and attitudes towards technological surveillance by their employer in particular.

The findings are based on interviews conducted with financial services employees by the University of Limerick pre-COVID19 in 2019 followed by a large-scale survey of employees during COVID19 restrictions in 2021 with a further survey of members conducted by the FSU in February 2023.

Survey respondents reported having some experience with technological surveillance of their devices, but significant proportions were unaware if their devices were monitored or not. Interviewees spoke of varying levels of employer technological surveillance pre-COVID from very little to very extensive depending on where they worked and their role. Overall, employees had negative attitudes towards technological surveillance, viewing it as demoralising, stressful, and indicating a lack of trust by employers.

The report is segregated into number of distinctive areas. It firstly reports on the responses to the interviews of members in 2019 and the survey results of 2021 and then outlines the results of the more current 2023 survey.

The report makes recommendations for employers and the government. For employers, the concerns of employees and the issues arising from technological surveillance should be negotiated with the union. Employers need to be transparent with how they collect data and what surveillance they are employing to track their employees.

For the government, it should undertake research on possible legislative changes that may be required to keep pace with technology advances whilst ensuring proper regulation of employers' collection and use of data from surveillance functions. The government should also seek the Data Protection Commissioner to be proactive in inspecting employments to ensure adherence to GDPR legislation.

John O'Connell,
General Secretary of FSU



The Research Team

Dr. Michelle O'Sullivan
Dr. Juliet McMahon
Dr. Caroline Murphy

Dr. Lorraine Ryan
Dr. Jonathan Lavelle
Prof. Tony Dundon

Department of Work & Employment Studies

Kemmy Business School
University of Limerick
www.ul.ie/business/



SECTION 1: INTRODUCTION

Research Background

Digitalisation has been identified as one of the major global challenges of our timeⁱ. This report was commissioned by the FSU to fully understand how digitalisation is impacting employees – its benefits and risks. The study which started in 2019 was originally focused on the impact of workplace technology involving the automation of tasks, on employers' use of technology to monitor employees, and employees use of mobile technology to work outside the workplace. In October 2019, the University of Limerick produced its first report for the FSU - Technology, Work & Skills - which highlighted the evidence in research of the emergence of long hours and always on culture in organisations. On foot of that report, the FSU called for increased regulation on the right to disconnect in Ireland and the government signed a new Code of Practice on the Right to Disconnect in April 2021. Remote working has contributed to the blurring of boundaries between work and non-workⁱⁱ, a development which accelerated dramatically with the emergence of COVID-19. Ireland had one of the highest levels of employees working remotely partially or fully during the pandemic in the EUⁱⁱⁱ. The “Making Remote Work: National Remote Work Strategy” was launched by the government in January of 2021 with the objective of ensuring that remote working becomes a permanent feature in the Irish context, maximising economic, social and environmental benefits.

This report for the FSU presents research findings on financial services employees' experiences of, and attitudes to, technological surveillance by employers. Technological surveillance refers to “management's ability to monitor, record and track employee performance, behaviours and personal characteristics in real time or as part of broader organisational processes”^{iv}. While employers have always engaged in some form of surveillance of employee activities, its scale and intensity has increased which is associated with becoming more technological and more pervasive^v. The first report for the FSU noted that technological surveillance may have benefits such as increased productivity, protection against fraud, and potentially providing a more accurate assessment of employee performance. There are also potential negative consequences from surveillance including in regard to employee privacy, control, and working relationships. This report will investigate these issues.

Report Structure

Section 2 of the report presents the findings of the interviews and a national survey of financial services employees and seeks to address the following research question:



What are employees' experiences and views on technological surveillance by employers?

Section 3 of the report presents the findings of a survey of FSU members taken in February 2023

Section 4 of the report summarises the key findings of the report and makes a set of recommendations to address issues arising from the survey results.

Methodology

This report is part of a larger research project on the impact of technology on financial services employees undertaken between 2019 and 2021. The research had a mixed methods design consisting of qualitative and quantitative data collection in a two-stage process. In the first stage, 23 interviews were undertaken by the research team in Ireland and Northern Ireland in 2019. The interviewees worked in a variety of roles in financial services including customer service and support roles, relationship managers, IT specialists, mortgage advisors, bank branch supervisors and managers, and business analysts. The objective of the interviews were to gain deep insight into how technology has impacted different employee roles. The second stage consisted of a large-scale survey distributed over in September and October 2021. The survey sought to capture employees' experiences of technology including in regard to technological surveillance. A further survey of staff was carried out in February 2023 to ascertain post covid restrictions if surveillance had surfaced as an issue taking into account the number of people working from home.

Survey Respondent Profile 2021

There were 1077 responses to the survey. The majority of respondents to the survey were female (62%), were aged between 35 and 54 (75%) and had salaries of between €25,000 and €79,000 (84%) (Table 1.1). Over 80% of respondents had a third level qualification, the vast majority were union members and approximately one third worked in supervisory positions. Most respondents worked in retail banking (75%) (Table 1.2). The remaining 25% worked in a variety of sectors including insurance, international banking, professional services, payments, funds/asset management and other areas.

Table 1. 1: Survey Participant Profile (Number and Percentage)

Gender	Male	Female	Non-binary/ not say			
	402 37%	666 62%	10 1%			
Age*	25-34	35-44	45-54	55-64		
	80 7%	364 34%	437 41%	187 17%		
Salary	≤24,000	25,000- 34,000	35,000- 44,000	45,000- 59,000	60,000- 79,000	≥ 80,000
	40 4%	124 12%	201 19%	284 27%	273 26%	133 13%
Union member	Yes	No				
	1035 97%	32 3%				
Supervisory position	Yes	No				
	345 32%	729 68%				

*4 respondents were aged 15-24 and 5 people were 65+

Table 1. 2: Survey Participant Area of Work

Work area*	Retail banking	Technology & professional services	Payments	International	Insurance banking	Other
	810 75%	83 8%	33 4%	19 2%	12 1%	101 9%

*17 respondents worked in either funds, buildings societies, credit unions or video gaming.

SECTION 2: SURVEY AND INTERVIEW RESULTS

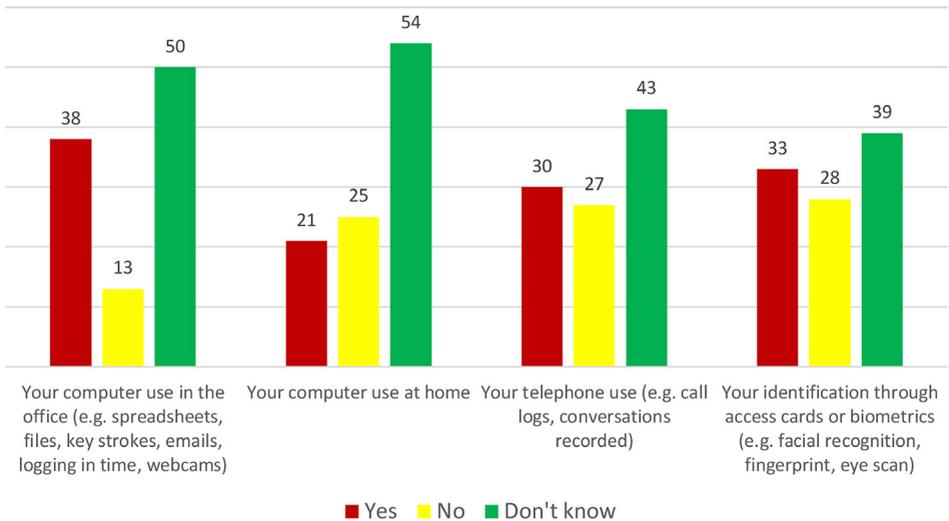
Technological Surveillance

In the survey, we asked respondents the extent to which their work devices were monitored. In 2021, a fifth of respondents indicated that their computer use at home was monitored, 38% had their office computer monitored, almost one third noted their telephone use was monitored and one third accessed work systems through personal identification mechanisms. A notable finding was the extent to which respondents were unaware of the level of employer tracking and monitoring, with over half indicating they did not know if their office or home computer was monitored (Fig. 2.1). Almost one quarter of respondents reported that their employer had increased data collection on their work since they started home working while 28% said data collection had stayed at the same level.

“Working from home is a major game changer. If increased monitoring is the price of working from home, I’m ok with that.”

“Level of surveillance has certainly increased even though we are using the same technology & systems that we have when in the office. We are being reminded regularly that our outputs are being monitored and compared with other team members”.

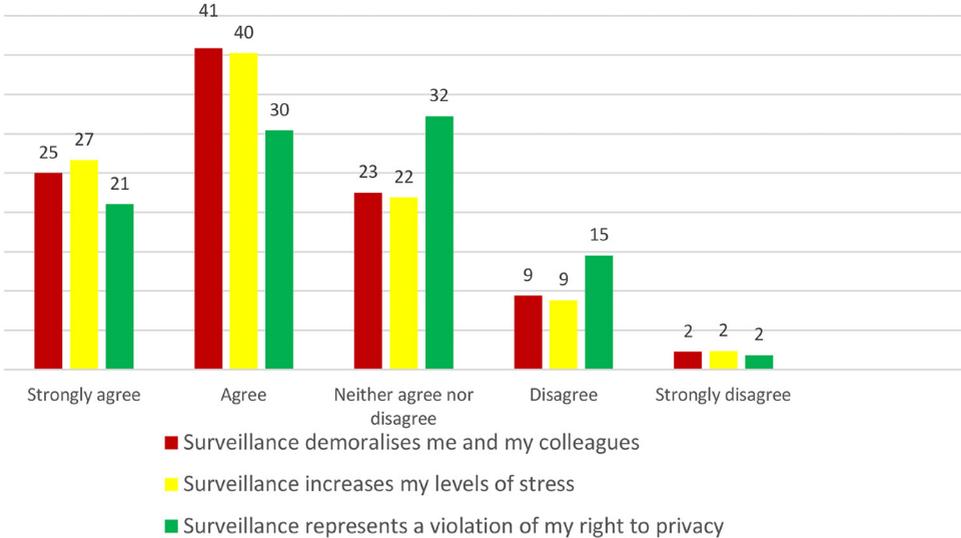
Figure 2.1 Organisational Data Tracking of Employees’ Work



The survey gathered respondents' views on the impact of surveillance on their personal lives and wellbeing. Two thirds of respondents felt surveillance was demoralising and indicated that surveillance increased their levels of stress while over half felt that surveillance at work was a violation of privacy (Fig. 2.2). A greater proportion of younger respondents reported surveillance-related stress than older respondents. For example, more than three quarters of those aged 25-44 stated surveillance increases their stress compared to 62% of 55-64 year olds.

“Employer surveillance would be a determinant factor in my continued tenure. I'd leave over these things”.

Figure 2.2 Personal Impact of Surveillance



Employee attitudes on trust in the employment relationship were stark. A majority felt that surveillance indicated a lack of trust on the part of their employer (60%) while an even larger percentage (63%) felt that the use of surveillance erodes trust (Fig. 2.3). Only a quarter of respondents agreed that they trusted how their organisation used their data. The qualitative comments by survey respondents highlight these trust issues.

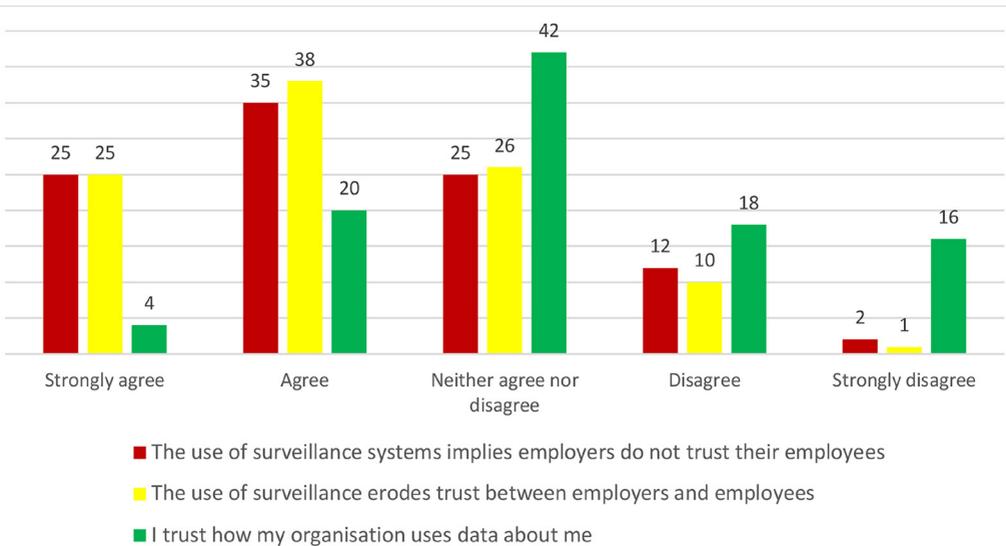
“Bank uses technology to track customer footfall v sales. Bank not interested on time spent building relationships, providing customer service, doing tasks etc. this puts pressure on staff to sell to detriment of everything else. Also pits staff against each other so teamwork is gone”.

“It’s not moral to monitor our clicks on a computer. If you have an issue with my job talk to me, don’t spy on me”.

“My concern is that I do not know if my employer is using surveillance systems to monitor me and I should know that”.

“No concern on data surveillance if it is discussed first by staff with why”.

Figure 2.3 Impact of Surveillance on Trust



We asked respondents their attitudes to surveillance systems in terms of employer control. Just under half disagreed that the fairness of employer decisions increased through surveillance, while a substantial proportion were neutral on the issue (Fig. 2.4). Respondents were far more likely to agree than disagree that surveillance weakens employees’ trust and that it is used by employers as a control mechanism. We asked respondents to indicate how they felt surveillance had impacted productivity. A majority (56%) disagreed that surveillance helped to improve productivity, and roughly one third disagreed that surveillance was legitimate and disagreed that surveillance allows for a more accurate measure of employee performance (Fig. 2.5).

Figure 2.4 Fairness and Control

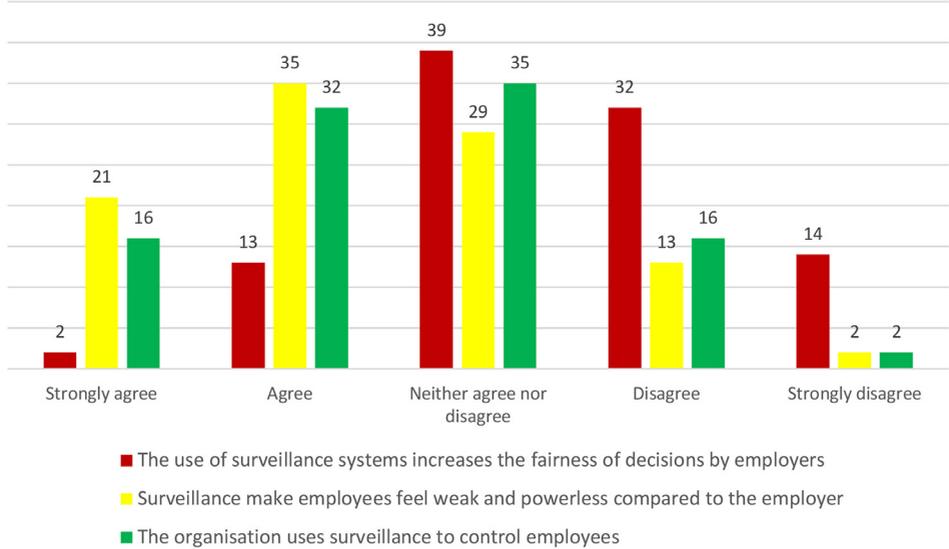
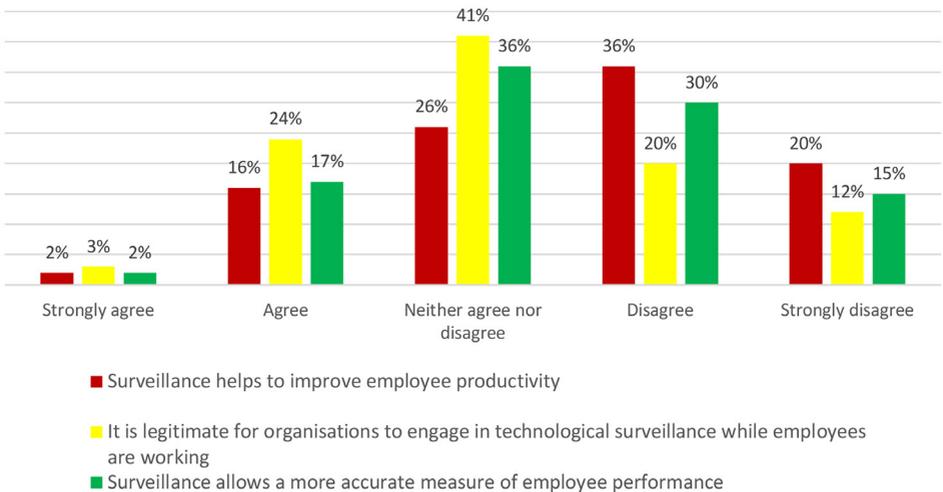


Figure 2.5 Surveillance and Productivity



In interviews in 2019, the feedback from employees suggested that the extent of employer surveillance of employees’ work depended on several factors. One was the level of organisations’ technological capability to monitor employees’ work. For some interviewees, “*monitoring work is down to how good the tech is but it’s not that good*”, while for others, “[management]...can see absolutely everything

everyone does, every single thing” and similarly, “everything is monitored – the whole lot! It’s constant, it’s unrelenting. They have a measurement for everything – how many customers did you deal with today?”

A second factor associated with the level of surveillance was the occupational role of the employee. Overall, interviewees indicated that there was a high level of surveillance of employees in bank branch roles in some retail banks and in call centre roles while interviewees in non-customer facing roles like underwriting, lending, and IT experienced monitoring to a lesser extent. Surveillance of employees was primarily directed towards increasing productivity and sales, and performance management. Interviewees pointed to examples of surveillance:

“Everything you type is being recorded in instant messaging”.

“[I’m] regularly challenged on how long a job takes me to do. A lot of what I do is on a spreadsheet which can be viewed by a manager who might say a job should take 3 hrs instead of 5”.

“Worse in the call centres – the mortgage debt section in particular have to watch tone etc for monitoring”.

“We’ve none of that [monitoring calls / emails]. There are call stats fed into score card, and phone answering is monitored but there are no scripts. The percentage of dropped calls / unanswered calls is tracked. The aim is not to miss any”.

“... a new phone system called genesisthey brought that into our area recently, you’re supposed to log in in the morning, all your calls go through it.....all your breaks, lunch, your comfort breaks go through it.....this is a whole monitoring phone system that give the stats on what time I arrived logged in, what time I was absent from my desk, what time I logged out, how many calls I took. How long, how many emails came in and how many I answered.”

Those who worked remotely pre-COVID19 were also monitored in terms of their active and inactive periods on computer systems though they were not aware how the information was used by management.

“Your little icon goes from active to away, and you feel someone is watching [if working from home] but if you’re in the office you don’t mind”.

An interviewee noted that in their organisation, computer systems tracked all employee activities and this data was used to score employees’ performance based on their targets around items like customer experience, mortgage sales and customer acquisition. If the management information system scored employee

performance as below par, they would be subjected to a heightened level of surveillance.

In terms of the extent to which employees knew they were being monitored, some noted that *“you do have fair warning that they are monitoring”*. While others were aware of the existence of certain monitoring practices, they would not necessarily know when they were being monitored. For example, one retail bank had a policy of using mystery shoppers who covertly recorded conversations with staff and the employee would later be warned about their *“transgressions”* in those conversations.

Participants noted that in addition to management systems which record what employees do, management also expected or required employees in some organisations to record their own actions or manually detail how their time was spent in a week (akin to a billable hours principle):

“It starts off as you get a credit for doing it [writing guides to your work] but very quickly its standard part of the job....definitely the amount of time you’re spent recording what you’re doing has increased relative to the time you spend actually doing it.

Interviewees noted that such exercises were time consuming but not considered in performance management conversations. Some commented that technological and manual recording of staff activities allowed management to maintain significant control and kept workers ‘on a tight leash’:

“Up the line they want oversight of everything, centralisation of tasks brings control. Automation brings control.”

In terms of employees’ acceptance of surveillance, views varied. Some with lower levels of surveillance did not identify major issues with monitoring of staff behaviour while others with more invasive levels of surveillance had accepted it as a part of the job. Even when employees initially found monitoring *“daunting”*, *“now we expect it and it becomes normal; it’s what you’re used to”*. Employees though were critical of surveillance used for the purpose of pressurising them to achieve unrealistic targets.

“Sales targets in the biggest things like mortgage products are crazy, are unattainable and that adds pressure to you when technology breaks down. That takes time out of your day”.

“They’re always stretching targets. Don’t know how they’re set. We’re told it’s an analytics thing in headquarters that works out what they reckon should be attainable in each branch. Yearly targets – for each product. It tends to go up every year. A reprieve would be staying the same”.

Some interviewees spoke of measures they undertook to resist or defend surveillance. One interviewee noted that he advised others to write down all tasks completed during the workday so that if targets were not met, they would have a record of why and how their time was spent e.g. covering for absent colleagues, dealing with breakdowns in technology.

SECTION 3: SURVEY FINDINGS

In February 2023 the Financial Services Union carried out further research seeking to document the attitudes of staff to employer surveillance of their activities, what their knowledge is of the surveillance carried out by their employer and whether they feel new protocols need to be introduced to ensure there is full transparency around how the surveillance is carried out and how the data is managed and used into the future.

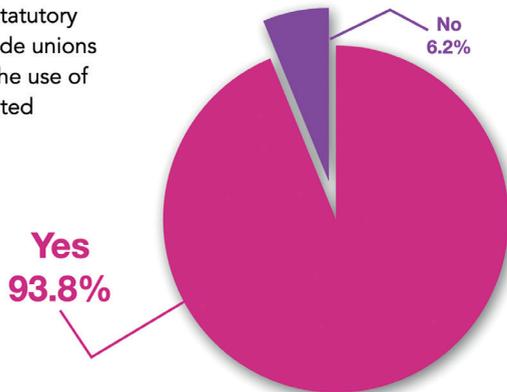
The results are set out in the three graphs below. These findings mirror the findings of the previous research and indicate that the high level of concern of employees on how employers are utilising surveillance and the data they collect.

Ninety-one percent of respondents report concern on this matter with 39.4% very concerned.

An overwhelming number of respondents (95.9%) feel that employers should have to consult with trade unions prior to introducing monitoring and surveillance at work.

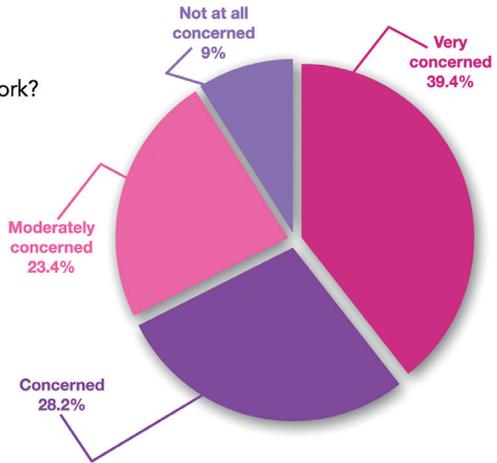
Do you think there should be a statutory duty on employers to consult trade unions before an employer introduces the use of artificial intelligence and automated decision-making systems?

1328 out of 1339 people answered this question



Are you concerned about excessive surveillance and data collection at work?

1330 out of 1339 people answered this question

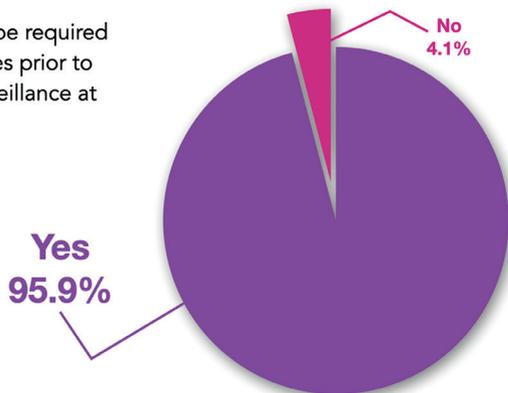


When asked the question : Do you think there should be a statutory duty on employers to consult trade unions before an employer introduces the use of artificial intelligence and automated decision making process 93.4% of respondents indicated in the affirmative.

These recent results further strengthen the results obtained in 2019 and 2021 and leave no room for doubt that action is required both by employers and Government on the face moving issue of surveillance at work.

Do you think employers should be required to negotiate with their employees prior to introducing monitoring and surveillance at work?

1333 out of 1339 people answered this question



SECTION 4: SYNOPSIS OF FINDINGS AND RECOMMENDATIONS

Findings

- i. The level of technological surveillance is varied across occupations and organisations. Some financial employers have invested heavily in technology to capture most aspects of employee performance while others have invested to a lesser extent. The consensus amongst interviewees was that some types of occupations are monitored to a greater extent than others. Customer-facing roles in particular were considered more likely to have stringent employer surveillance.
- ii. In terms of surveillance of devices, there is a large information gap amongst employees. The majority of survey respondents did not know if their computers were monitored, and a significant proportion were unaware of their phones were monitored. Surveillance can also happen in less direct ways, for example, through covert recording of in-person conversations.
- iii. Survey respondents overall held negative views about surveillance. They believed surveillance had negative implications for their morale, stress levels, level of privacy, their sense of control, and level of trust in their employer.
- iv. Survey respondents were much more likely to view surveillance as being negatively linked to employee productivity. A much higher proportion of respondents held negative rather than positive views in regard to technology's ability to accurately capture their performance.
- v. The majority of survey respondents either did not view surveillance as a legitimate employer activity or had no opinion on the matter.

Recommendations

The issues raised in this report can be addressed in two ways: through collective bargaining between employers and employee representatives and through statutory regulation.

Collective bargaining

The concerns of employees evident in the survey findings can be addressed through collective bargaining between employers and trade unions. Employers should prioritise the following issues:

- Providing evidence on the necessity and proportionality of technological surveillance in all its forms.
- That surveillance functions should only be introduced with the agreement of the union and affected employees.
- That the employers' collection of data from surveillance functions and the nature of its usage should be negotiated with the agreement of the union and affected employees.
- To address, with the union, the impact of surveillance on employees, such as their stress and trust levels.
- Providing evidence to the Union on the organisations' cybersecurity measures to protect employee data collected, in particular, biometric data.

Government Regulation

Given the increased prevalence of technological surveillance by employers, the Government should:

Request the Business Committee in Dail Eireann to commission a report into the use of surveillance in the workplace and legislative changes that may be required to best protect workers and provide for workers voice on this issue:

- Introduce stronger legislative mechanisms that (i) support trade unions access to, and representation of, workers for feedback on these issues and (ii) require employers to meaningfully negotiate with unions on technological surveillance.
- Introduce legislation regulating employers' collection and use of data from surveillance functions with the aim of ensuring procedural justice, distributive justice^{vi}, interpersonal justice and informational justice within organisations.
- Empowering the Data Protection Commission to proactively inspect employments to ensure compliance on current GDPR legislation.

Reference Notes

- ⁱ Schulze, S. (2021). 'Aligning the Challenges of our Time'. *The Progressive Post*, 6th November 2021. Available <<https://progressivepost.eu/aligning-the-challenges-of-our-time/>>, accessed 16th November 2021.
- ⁱⁱ Secretariat to the Expert Panel on Modern Labour Standards (2019). *Disconnecting from Work-Related E-Communications Outside of Work Hours Issue Paper*. Government of Canada. Available at <<https://www.canada.ca/en/employment-social-development/corporate/portfolio/labour/programs/labour-standards/reports/issue-paper-disconnecting-e-communications-outside-work-hours.html>>, accessed 20th April 2021.
- ⁱⁱⁱ Eurofound (2020). *New Forms Of Employment: 2020 Update*. Luxembourg: Publications Office of the EU.
- ^{iv} Dandeker, C. (1990) *Surveillance, power and modernity: bureaucracy and discipline from 1700 to the present day*. Cambridge: Polity.
- ^v Thompson, P. (2003) 'Fantasy Island: a Labour Process critique of the 'age of surveillance'', *Surveillance & Society*, 1(2), 138-151.
- ^{vi} Colquitt, JA. (2001) 'On the dimensionality of organizational justice: A construct validation of a measure', *Journal of Applied Psychology*, 86(3): 386-400.

NOTES

- 
- Stephen Street Upper, Dublin 8, D08 DR9P T: +353 (0)1 475 5908
 - Quaygate House, 5th Floor, 15 Scrabo Street, Belfast, BT5 4BD. T: +44 (0)28 90200130.

E: info@fsunion.org www.fsunion.org