Total Data Control at Work?

Surveillance and Data-driven Decisions in the Workplace

2022

UNIONEN

Table of Contents

Preface

An increasing number of entities are increasing what they know about us. This includes information about what, when and where we shop, what movies we prefer to watch, and whose pictures we like. Information processed by computer systems around the clock.

Often it concerns a relatively harmless collection of data. But even if there is no malicious intent, the amount of information we leave when we use smartphones and laptops is staggering. In so many ways, we submit to voluntary surveillance and monitoring of our lives.

And within one's job and working life is no exception. Using Internet connected employer-issued work tools creates data about our behaviour. It is data that can be collected, structured and analysed. One important difference, however, is that we cannot voluntarily choose to use the work tools or not. The question then becomes what regulation and policy applies at the workplace?

This report discusses monitoring and data management in the world of work. The report takes note that interest in data-driven, or algorithmic, workforce management has increased sharply in the past decade. It seeks to clarify what is permissible, what is not permissible, and what aspects are important to keep an eye on. Note that the report is written from a Swedish labour market perspective and is a translation of a report first published in Sweden.

All parties in the Swedish labour market need to engage with how we govern surveillance, monitoring and data-driven methods in the workplace. What can employers do on their own, and what is permissible? What in fact is not okay, and how and when should trade unions be involved as a partner? With this report, Unionen wants to put the spotlight on these issues and seek to stimulate discussion.

Katarina Lundahl
Chief Economist

Introduction

More and more have people have a job in which all or part of the work can be carried out irrespective of time and location. Where there is an Internet connected work tool, such as a laptop or a smartphone, people who previously needed to work in their employer's office, can now perform their work tasks in a location of their choice.

In the early years of the 2020s, a large percentage of the work of white-collar workers was moved to their homes, to prevent spreading of COVID-19. A significant portion of the people who previously worked in offices hope to continue telecommuting going forward, at least to some degree.

A working life for white-collar workers with a wider framework than traditional office environments is enticing to many. But as ever-larger parts of office workers working lives are filtered through digital environments and extensive computer systems, new challenges are emerging. Which carries with it some risks.

There have been reports in the United States and the UK of employers installing software in work devices whose sole purpose is to monitor employees. In Sweden, we fortunately have a work culture that can be characterised by greater respect and trust between employer and employee than that. But good intentions offer no automatic protection against invasions of digital privacy or data breaches via hacking.

It is likely that an increasing number of office workers in the 2020s and onward will work at companies that make use of different variants of data-driven practices in the management of the workforce and within personnel matters. Already today, such features in work computer systems are hotly debated.

The above are questions that relate in various ways to employers' collection and use of the data recorded when employees use employer-issued digital work tools. Or more simply put, where do our digital data trails, the ones we leave behind at work, go? These are questions that arise with the use of new technology. However, it is also a discussion that needs to be placed in a centuries-old context of supervision and monitoring at work.

Surveillance at work

Are you under surveillance at work? Whether the answer is ‘yes’ or ‘no’ at the individual level, surveillance at work definitely occurs. Sometimes it’s obvious, other times it happens in a more subtle or concealed manner. With the emergence of new technologies, the possibility and potential of surveillance has progressively increased.

Cameras allow a person to overview large areas and inaccessible locations from a desk. Sensors can monitor production flows at speeds far exceeding human capabilities. GPS and other geolocation technologies are used to optimise logistical flows. Often these are processes that go on in the background, without it consciously arousing thoughts.

The person in charge of and carrying out surveillance may not even think of it as surveillance. It might rather be seen as an attempt to optimise production and control quality.

Perhaps it’s not so strange that there is sometimes a lack of awareness of the monitoring taking place. Quite often it’s abstract. Being under surveillance, being aware of being under surveillance and the immediate feeling of being under surveillance at the moment, are different things.

Surveillance or even monitoring is often associated as something malicious, negative, or hidden. That’s not so odd or unexpected. Surveillance and monitoring of behaviour has been used throughout history to acquire power, to exert control, and to punish.

Surveillance and supervision at work

Surveillance has also been a recurring feature of life in the workplace. In a workshop where the masters sat with their craft, with their apprentices to assist, the surveillance was personal and immediate. The masters owned their workshops and was at the same time experts in the craftsmanship that needed to be done. They both taught and supervised the work being done.

As our world began to be industrialised, work was often organised around the machines that employees were assigned to operate. In long rows, machines were driven by belts straps attached to a shaft in the ceiling. The shaft itself was often powered by a gigantic machine elsewhere in the factory.

The work was broken down into small simple steps, where each part could be carried out following simple instructions. To be performed, each element became a sequential operation dependent on the previous element, in what was called a production line.

In a production line, processes can become so complex that it is difficult to obtain a decent overview of the big picture. Consequently, in order to ensure that the outcome is desired and that the rate of production is maintained, the quality and flow must be monitored and controlled.

In Foucault's 1975 work *Discipline and Punish: The Birth of the Prison*, he describes how the need for surveillance is being driven by an increasingly competitive market. Competition increases the demands for greater efficiency. Thus, to ensure that time and resources are devoted to creating value, the work must be put under surveillance:

"Surveillance thus becomes a decisive economic operator both as an internal part of the production machinery and as a specific mechanism in the disciplinary power."

Foucault argues that the increased need for surveillance leads to an increased need for specialisation, leading to monitoring becoming a task in itself. I.e., surveillance becomes an intimate part of production efficiency.

For the workers at the machinery of industry, the work supervisor, or foreman, watched whose role it was to monitor and control the work the employees were doing. To direct it so that the work was carried out according to the wishes and instructions of the management. Often from an elevated position, to get better overview.

In other words, surveillance in the world of work is no new phenomenon. The ambition to ensure that the work is done properly, prescribed and effectively, has long been used as an argument for surveillance. How this might manifest itself in the present day is discussed in this report.

Data breaches, interception of data, and personal integrity

One of the primary uses of surveillance in general is the acquisition of information. This also applies to the unlawful acquisition of information. The information can then be used to identify shortcomings and deficiencies, as well as the need for improvement.

The issue is complex. The methods that can be used to improve productivity, protect against injury, or facilitate work, can also be used maliciously.

During the 1930s, in the United States the La Folette Committee found that wiretapping and undercover infiltration were widely used methods of surveillance, when employers hired private detective agencies to disrupt trade union organising. The employers defended themselves by saying that the methods were necessary to stop theft and sabotage.

The first laws against surveillance primarily protected property from theft and damage. They emerged during the 19th century with the spread of new technologies such as the newspaper, photography and the telegraph. With these, a new understanding of what constitutes "property" also grew. In 1890, Samuel Warren and Louis Brandeis described it in their essay *The Right to Privacy*:

"From corporeal property arose the incorporeal rights issuing out of it; and then there opened the wide realm of intangible property, in the products and processes of the mind, as works of literature and art, goodwill, trade secrets, and trademark."

Warren and Brandeis go on to describe how the right to a private life emerges in a similar way to the understanding for intellectual property. Every human being has the right to be left alone, from feeling threatened or being disturbed in their home. According to Warren and Brandeis, a person's thoughts, emotions and even likeness are part of their inviolate personality, their right to privacy. The person has rights related to their privacy and protection of their personal integrity and a right to privacy.

Privacy, data and user as raw material

Today, information that was previously been seen as part of personal privacy is being shared in new ways. Often this involves sharing things that previously were kept private, in exchange for a service or feature in (for instance) an app in a smartphone. User benefits are exchanged for surveillance opportunities.

When the Internet was popularised during the late 1990s, there were still no broad possibilities to commercialise its use. Creating user accounts sometimes required physical signatures, a contract on paper. The most common business model primarily involved the selling of advertisements, which also meant that content mostly was without charge for the end user.

The search engines were so basic that the easiest way to find information was through portal sites. It was from this version of the Internet that companies like Google emerged. By implementing a search algorithm that ranked hits, not by content but rather how many people linked to that content, Google was at the same time collecting data on its users.

Soon Google began selling advertisements that were customised to what users were searching for, based on the data it had collected about them. In the 2000s, Google launched new products in the form of e-mail, map services and the Android mobile operating system.

The products generated increasing amounts of data for Google about the users. With the data, Google was able to study who a particular person communicated with, where they were at different parts of the day, and what shops and restaurants they patronised.

At the same time, in the social media sphere companies such as Facebook and in trade companies like Amazon were established. Both built business models around the realisation of the potential value of user data. As understanding and insights grew, users increasingly became creators of data for the companies whose services they used, often free of charge.

With new data on users, companies were able to customise ads in such a way that previously would not have been possible. In addition, by analysing via machine learning patterns of behaviour, companies could make predictions about people's future behaviour.

Shoshana Zuboff states her opinion in her essay book "The Age of Surveillance Capitalism" that user data can be regarded as a kind of digital raw material, not unlike mineral ore or crude oil.

"We are no longer subjects of value realization. Nor are we as some have insisted, the 'product' of Google's sales. Instead we are the *objects* from which raw materials are expropriated for Google's prediction factories." (Zuboff, 2019)

In data-driven production, data on production becomes the digital raw material. Accordingly, when people's behaviours are a major part of production, data on their work behaviours is needed. With employees already accustomed to sharing information about themselves in their private use of digital services, it is not a long stretch to casually do the same unreflectively at work.

User data in one's working life

Attempts have been made, with the use of user data, to predict consumer behaviours. The same data and machine learning technology being used to predict behaviours can also be used to "nudge" consumers in the direction towards a desired behaviour.

Nudging is a method of influencing and changing behaviour based on how ostensibly free choices are presented, with the term being popularised by authors Richard H. Thaler and Cass R. Sunstein in their book *Nudge: Improving Decisions About Health, Wealth, and Happiness*. It involves influencing people's behaviour in a non-coercive way, by reinforcing and rewarding them when they act in a desired manner, for example via gamification.

Using similar methods in one's working life is not far off. The software used does not care about the purpose for which it is used. For the software, everyone are users.

Instead, the difference lies in which analyses are used and the purposes for which employers may want to analyse user data generated by employees. For example, delivery companies have used sensors to measure acceleration, GPS to track driving route choices, and cameras to film the driver's attentiveness. Everything and anything to improve driving safety, it is asserted.

Software for office work often don't solely include the functions to editing documents and sending e-mails. The software can also collect information about the number of keyboard downstrokes and who is working with whom, to give a few examples.

In an article for the Harvard Business Review, Mareike Möhlmann (2021) discusses examples where companies have used "nudging" to get employees working longer hours and faster, eat healthier, or use less resources. Möhlmann argues that algorithmic nudging is not necessarily unethical, as long as there is transparency regarding which factors influence classification and assessment/rating levels.

More blurred and indistinct boundaries between work and personal life actualise issues of personal integrity, ethics, surveillance and employment law. There are anecdotal examples of both nudging and more outright surveillance from other countries. These are examples that would likely be challenged as being inappropriate in Sweden but can be said to be more normalised in other countries.

One example is an employer in Japan handing out points to employees who slept a certain recommended number of hours per night. The points could then be exchanged for discounts in the workplace lunch restaurant. Sleep was measured by a special mattress. In doing so, a peculiar social control was exercised, irrelevant to the work, in which private data on sleep was collected and retained by the employer.

Another is an article in a British computer journal, where various software programs to monitor employees was tested. The software was tested for its effectiveness in employee surveillance and in analysing the speed of the employees' work at a detailed level.

In the United States there are companies selling computer systems aimed at measuring employee emotions using artificial intelligence. Some believe that such a system is not even technically possible, others believe that the technology is solid. Regardless, it illustrates a labour market where products, whose sole purpose is the surveillance of employees, have buyers.

Digital Versions of Employees

Desktop computers, smartphones and other Internet connected tools provided by one's employer to do work, leave digital data trails when used. Sometimes this is due to that the employer-issued work tools regularly registers data, for example, on geographical location. Not infrequently, such registration is built into the tool and the default setting is set to on. Sometimes it results in the tool actively collecting information and data that is related to the job. Data on e-mail activity, what meetings people have had, telephone call traffic are a couple of examples.

In the 21st century, possibilities for employers to collect data from employees have increased, as Internet connected employer-issued work tools have become more common. Furthermore, the presence of Internet connected employer-issued work tools has spread to more and more sectors of the labour market.

Anyone who has access to detailed digital footprints from an individual and who at the same time has the capacity to analyse it, can draw a digital version of the person. With the increasing number of tools we use at work being digital and/or connected to a network, employers can theoretically draw an increasingly detailed digital version of their employees.

It should also be pointed out that such digital version does not necessarily correspond well to reality. Nor can it be said to be likely

that it provides an accurate overall picture of a person. But nevertheless, the creating of such digital versions of employees can appear tantalising, for anyone who wants to work with data-driven methods.

Digital Data trails on Work Devices and the General Data Protection Regulation

The fusing of privacy and work life described above raises the question of what possibilities employers have to use the digital data trails generated on a work device. Here it is wise to look at the General Data Protection Regulation. The General Data Protection Regulation (GDPR) is a law that applies throughout the European Union.

If data generated at work causes a natural person to be personally identified, the General Data Protection Regulation becomes applicable. Conversely, if a natural person cannot be identified on the basis of data, then the GDPR is not applicable. In the normal case, it is fraught with considerable difficulty in completely de-identifying personal data from large datasets, which is why the starting point here is that the GDPR becomes applicable.

What an employer can do with digital data trails is a multiple-answer question. However, one aspect that is always present in such an assessment is the *purpose* for which digital data trails and other information in a work device has been collected in the first place, and the purpose for which it is then examined.

The GDPR regulates how personal data may be collected and processed. Examples of personal data include telephone numbers, office/residential address, IP addresses,[1] and audio and image recordings of people who can be identified. Even encrypted/encoded personal data is encompassed here, if there is a key that can link encrypted data to a particular individual.

Generally, a legal entity or other body that collects and processes personal data is the personal data controller. It is not a particular manager in a workplace or an employee who is the personal data controller. A natural person may however be the personal data controller, for example in the case of a sole proprietorship/sole

[1] An IP address (Internet Protocol address) is a set of numbers used as an address on the Internet. The IP address normally identifies a particular computer, and at the same time the address indicates the network which the computer is connected to.

trader. The Swedish Authority for Privacy Protection have, based on Article 5 of the GDPR, compiled a list of the fundamental principles for personal data controllers:

- may collect your personal data only for specific, specifically specified and legitimate purposes
- may not process more personal data than necessary for the purposes
- must ensure the accuracy and correctness of your personal data
- must delete your personal data when it is no longer needed
- must protect your personal data, for example against unauthorised access, loss or destruction.

The personal data controller must also ensure that individuals are informed about why the personal data is being collected and how their personal data is processed and otherwise dealt with.

Employers, according to the GDPR, have the possibility to process a wide range of personal data relating to their employees. However, the employer must have legal basis for processing the personal data. The legal basis may be, for example, that the personal data is needed to perform a contract, such as the contract of employment, or to fulfil a legal obligation arising from statute or collective bargaining agreements. Another legal basis may be the trade-off of interests, where the employer's interests should be weighed against that of the employee.

As a general rule, the employer has an obligation to minimise the collection and retention of data, meaning to ensure that the personal data processed is appropriate, relevant and not excessive in relation to the purposes for which it is being processed. Data may not be processed for purposes other than those for which is was collected. In other words, the question of *purpose* is central.

That means employers cannot use digital data trails generated by work devices in any way they do desire. In employment, the starting point should be that the personal data is originally collected and processed in order to perform a contract provision or to fulfil a legal obligation, and after a trade-off between the employer's interests in collecting and using personal data, and the employee's interests in avoiding personal data about them being collected and used. For example, if the personal data is resold to third parties on

this basis, it is likely to be an infringement of the GDPR, considering that the personal data is then being processed for purposes other than those for which it was originally collected.

The GDPR can provide protection in situations that infringe on personal integrity and is especially relevant if an employer wants to implement fully or partially automated decision-making within the framework of workforce management law. The corresponding protection does not exist via the Swedish Co-Determination in the Workplace Act (*Medbestämmandelagen*, MBL) where the employer can make purely substantive decisions at its own discretion.

The employer has the same obligation to negotiate under the Co-Determination in the Workplace Act when introducing systems or changes to systems that involve GDPR issues. Examples of matters that may require negotiation include when case management systems are updated with GPS tracking features, if this is compatible with the GDPR and what right to protection exists for employees' personal data.

Data Driven/Algorithmic Production and Management

An increasing number of parties are in a situation where, thanks to the development of digital tools, they have access to large amounts of data about their activities. One concept that has simultaneously become increasingly prevalent in the conversation about productivity and how companies should work is to work with "data-driven" or "data informed" methods.

Essentially, it involves an increasing willingness among companies to incorporate big data analytics as part in the production of goods and services and for the purpose of making operational and business-critical decisions. This also includes a more data-driven approach to the work, based on data on employees and/or data generated by employees while performing their work tasks.

Succeeding with a data-driven mode of work is however, not simple or easy. Data may be incomplete, poorly catalogued, or be sitting in different systems in different parts of the company. Part of the work with a more data-driven production is therefore not about collecting information, but rather about structuring information that has already been collected, and analysing it.

Today, there are possibilities to build computer systems (hardware and software) that make such processes possible. Such computer systems often have elements of some form of artificial intelligence (AI). But there are at the same time limitations, which mean that implementing such systems does not automatically always produce good results or is always desirable.

Most relevant to the discussion in this report are data-driven practices in the efforts with workforce management the work engaged in by human resources departments. The term "Workforce Analytics" is often used. In this report, we chose the term "algorithmic management" as an umbrella term to generally refer to the various aspects and iterations. Unionen has previously discussed the issue in its report "Maskinen som chef" [The Machine as the Boss] (2019).

Algorithmic management includes analysis of data that employees produce or leave behind in the use of Internet connected employer-issued work devices. The analysis then forms the basis (alongside other bases) to make decisions on the management of the workforce and/or personnel matters (Lee et.al., 2015).

Implementing systems for a more data-driven work can have both positive and negative effects. In simple terms, a positive effect could be a better quality with the efforts with workforce management and personnel issues. At the same time, such methods place major demands on the computer systems designed to extract information and knowledge from employee-generated data, as well as on those who use the systems.

Issues of security, personal integrity, ethics and transparency towards those who generate data become central. If such issues are ignored, the risk is huge that the precision in decisions will be worse than before. That far-reaching intrusion takes place in the personal privacy of individuals and that parties who have no right to access certain information can nonetheless access and obtain it. Moreover, such negative consequences may prove difficult to correct, due to that the data is very difficult to retrieve back once it has been copied.

Technology Hype, Technology Scepticism and Benefits with New Technologies

New technologies have always been surrounded by both great expectations and great concern. In the 2010s, a commonly used discourse in the debate over technology and work was that "the robots will take our jobs."

This is however not a new debate. The same prediction can literally be found at regular intervals in history, at least since the mid-20th century.

In a broader perspective, for centuries people have been worried that they would be replaced, their job taken over by machines whereupon they would be thrown into unemployment and destitution.

Generally speaking, such concerns have mostly been allayed. Throughout history, we have always shifted tasks from humans to machines. But that in and of itself has not meant that people have been deprived of work, as new jobs have been created. Robots have not yet made humans redundant.

However, the absence of disaster should not be taken to mean that the introduction of new technologies into the labour market is positive in every way.

It is important not to let an interest in the potential of new technologies override an analysis of the benefits and drawbacks of investing in them. The purpose of new technologies in one's working

life must always be that the technology can contribute to improvements, for all parties concerned. If the benefits of an implementation of technology come at a cost in terms of increased surveillance or invasions of privacy, it cannot be seen as an unqualified success.

The employer's use of data on their employees

What follows here is a set of hypothetical situations regarding the collection and use of digital data trails by employers and if this is to be regarded as being compatible with the GDPR, labour/employment law and the Swedish labour market model.

As a rule, in the individual case, a trade-off of interests must be made between the employee's privacy interests in relation to the employer's supervision interests.

As a starting point, an employee cannot consent to any and all processing of personal data no matter what, for example by initialling acceptance of a policy. This is because employees are in an unequal position of power vis-à-vis their employer, which makes it impossible to provide a consent on the basis of equal positions. Note: A violation of the GDPR may occur even if an employee has given their consent to certain policies or similar.

It should also be noted that GDPR is legislation governing the storage of individual personal data. This means that what is permissible or not in any given situation is ultimately determined by deciding an individual's case.

Looking into one's website browsing history

Is the employer permitted to check what websites an employee has visited on their work computer or work mobile?

There may be a justification to investigate website visits an employee has made, if there is a security aspect. The least intrusive method should always be chosen, such as monitoring of logins over checking actual visits, and setting up features that block access to certain websites over a review of data after visits.

Collecting data in real-time about which websites employees visit, for the purpose of checking which websites an individual is visiting, is not to be regarded as being permissible. However, exceptions to this main rule apply in the case of serious suspicion that the employee has committed crimes that may be affected by the employer or on serious suspicion of disloyalty.

Monitoring of work activity

Is the employer permitted to compel their employees to have a webcam turned on throughout the business day, or otherwise monitor employees on a regular basis?

Compulsion to always have a webcam turned on to show that one is sitting at their workstation (or laptop in their workspace at home) or continual monitoring by computer software and/or of keyboard use is difficult to justify. The volume of data collected if the employer constantly monitors their employees in how they work, becomes considerable. Such monitoring is likely to be in breach of the GDPR. Such surveillance likely violates the GDPR.

The Swedish Authority for Privacy Protection as well as the European Data Protection Board have stated clearly that real-time monitoring is impermissible, with the exception in the case of more extreme situations that concern safety, such as when a journalist or the Armed Forces is about to enter a dangerous situation.

Reviewing of e-mail messages

Is the employer permitted to go through an employee's e-mails?

The reading of employees' e-mails, as an employer, may be permissible in certain contexts. If there are strong suspicions of disloyalty or criminality that may affect the employer, personal e-mails may be read, and certainly when the personal e-mail is sent from/to the employer's e-mail address/account.

The same may apply to correspondence about work tasks where the employer has informed the employee in advance that their e-mails may read; under the precondition that there is a legal basis for doing so. The employer risks committing a data breach if in some way it gets into the employee's personal e-mails, social media accounts, or similar sources containing personal data.

It should be pointed out that in situations where an employer cannot be regarded as being entitled to read employee e-mails, the employer likely has technical possibilities to do so. In other words, information should not be regarded as being secure simply because it is impermissible to obtain the information.

Data Driven/Algorithmic management systems

Is the employer permitted to make use of computer systems and data collected on employees, known as data driven/algorithmic workforce systems, in their management of the work and the setting of salaries?

In the Swedish labour market, employers have the right to manage and allocate the work. But that does not mean that an employer can exercise managerial authority in whatever way they choose disregarding limitations imposed on them. Such is regulated in is legislation such as the Swedish Co-Determination in the Workplace Act (*Medbestämmandelagen*, MBL) and the Swedish Work Environment Act (*Arbetsmiljölagen*, AML).

The MBL and AML govern related matters, for instance how more important changes in operations should be implemented. The introduction and use of artificial intelligence systems in the workplace must be dealt with in the same manner as any other issue related to more important changes in the workplace, via the MBL and AML.

Data driven/algorithmic management systems raise integrity issues in some respects. The data on employees necessary for the functioning of such a system needs to be collected, stored and analysed.

Here a series of questions and risks arise. How is it ensured that the data being collected is the proper kind of data? How is the personal integrity of employees guaranteed in the collection and retention of data? Who has access to the personal data? In what way is it ensured that the system is not used for purposes other than the stated one? How are risks prevented from impermissible and unwanted monitoring?

In this respect, too, it is important that the implementation of new computer systems should be preceded by negotiation between employers and trade unions. The practice in such contexts is that unions representing employees generally can be said to have an interest in having an influence on the issue.

To the extent that systems potentially affect protection of personal integrity and covert monitoring of employees, such interests should typically be regarded as being a starting point. Several of the computer systems used in algorithmic/data-driven management that are on the market today can be said to have such components.

It follows rulings from the Court of Justice of the European Union and by the GDPR that an employer must never spy on its employees in secret. The right to information in the GDPR as well as the right to privacy in Article 8 of the European Convention on Human Rights makes secret surveillance impossible, because the employer is obligated to thoroughly inform how the collection, processing, and retention of data takes place, along with related matters.

In data driven/algorithmic management, some form of digital versions of employees are created. While technically possible, it is far from obvious that such digital versions should be regarded as good tools or a good basis for decision-making.

Taken together, such issues mean that the introduction of data-driven/algorithmic management systems should likely be negotiated between employers and trade union representatives. (However, there may be occasional situations where this is not the case.)

Data driven/algorithmic management systems are not to be regarded as prohibited per se, but they also cannot be introduced irrespective of manner. In addition, the question can be posed whether it is effective or not to introduce such systems.

The sale of digital data trails to third parties

Do employers have the right to share and/or sell employee's data to third parties?

Assume that an employer states in a transparent way that data is being collected for the purpose of being resold and that the employer believes that there is a legal basis to do so. In such a situation, the outcome is unclear, as there is a balancing of interests involved being made, and in that the personal data is not being processed contrary to the stated purpose.

How an employee acts also has an impact on digital data trails. If the employee clearly informs the employer that they object to the reselling of personal data in the forms of digital data trails, the balancing of interests should not result in an outcome in the employer's favour.

This, in turn, would mean that an employer who continues, after the employee has objected to the processing of personal data for this purpose, to process the personal data for this purpose, is likely to be in breach of the GDPR.

There is a needed for coherent legislation concerning personal integrity in the workplace

Surveillance has been occurring in communities and in work for a long time. In the 2010s, interest in digital surveillance increased, as ever-larger parts of our lives became filtered through a digital sphere, within which we leave digital data trails behind.

The world of work is no exception. More and more people who work are carrying out an increasing part of their work using tools that can be used for various types of surveillance. Sometimes such surveillance is easy to justify, for example based on security aspects. In other situations, it may be suspected that the collection of digital data trails in the workplace takes place routinely or unemotionally, or in the worst case, for the purpose of surveillance simply for the sake of surveillance.

Either way, increased digital surveillance in the workplace is fraught with a number of risks and challenges. The parties in the Swedish labour market need to discuss more broadly what increased digital surveillance in work can have for effects, and how risks can be prevented and avoided.

Unionen takes the position that the framework that presently exists in the Swedish labour market, where i.a. the Co-Determination in the Workplace Act, the Work Environment Act, and the GDPR and collective bargaining agreements included in the Development Agreement, provides a good basis for dealing with the challenges involved in this report.

At the same time, there is a problem in that the elements that are currently governed in legislation are not being dealt with optimally. There is a lack of coherent legislation protecting personal integrity in the workplace; the issues are instead dispersed in the legal system. Unionen advocates for coherent legislation in personal integrity in the workplace being adopted.

Unionen believes that unions and employers must work more closely together on issues related to digital surveillance and personal integrity. This is necessary in order to safeguard the personal integrity of individuals while allowing businesses to harness the potential of new ways of working and new technologies. Unionen looks forward to doing its part in that effort.

Sources

Brynjolfsson, E. & McAfee, A., (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.*

Foucault, Michel (1975). *Discipline and Punish: The Birth of the Prison [Surveiller et punir: Naissance de la prison*].

Frey, C. B. & Osborne, M. A. (2017). "The Future of Employment: How Susceptible Are Jobs to Computerization?" *Technological Forecasting and Social Change, 114*, pp. 254–280.

Lee, M.K., Kusbit, D., Metsky, E. & Dabbish, L. (2015). "Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers." *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1603–1612.

Möhlmann, M., (2021). Algortithmic "Nudges Don't Have to Be Unethical" in *Harvard Business Review* (April 2021).

O'Neil, C. (2016). *Weapons of Math Destruction*

Thaler, R.H. & Sunstein, C.R., (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness*.

Warren, S. & Brandeis, L. (1890). "The Right to Privacy" in *Harvard Law Review, 4*(5), pp. 193–220.

White, A (2018). "A Brief History of Surveillance in America," in *Smithsonian Magazine, April 2018.*

Zuboff, S. (2019). *The Age of Surveillance Capitalism.*

An increasing number of people have a job in which all or part of the work can be carried out irrespective of time and location. With work tools such as the laptop or the smartphone people who used to work in an office can become free to perform their work tasks in a location of their choice.

At the same time, we live in an age where the methods of digital surveillance and the analysis of large data sets is becoming more sophisticated. There are great risks associated with this, such as when this technology is used in the workplace or otherwise in life of the employee. Will there be extensive surveillance of data in one's work and what does that mean?

UNIONEN

UNIONEN IS SWEDEN'S LARGEST TRADE UNION

We welcome all white-collar workers in the private sector, irrespective of their post, educational background or level of pay. Our members include everyone from senior executives to the self-employed and students. Our vision is to work together to create success, security and job satisfaction.

Ref. no.: 3212-1 Production: Unionen