# Personal Data Trails in Job Devices

## Risks with Mixing Professional and Private Life in Work Tools

2022

UNIONEN

# Table of Contents


Preface ..... 2

Introduction ..... 3

Digital data trails ..... 4

- Digital data trails ..... 4
- We are enticed to leave digital tracks ..... 4

Digital data trails in the workplace ..... 6

- Tracking and data trails in the workplace isn't really a new issue ..... 6
- One's private life and working life are intertwined ..... 7
- Some digital data trails can be read by employers ..... 8

Risks with employer collection and use of digital data trails ..... 10

- Risks related to the use of work devices for personal purposes ..... 10
- Unauthorised collection and impermissible use of digital data trails ..... 11
- Security risks with digital data trails in work devices ..... 11

The Privacy Paradox ..... 13

Studying the privacy paradox ..... 14

- Method ..... 14
- Observations in a day in a respondent's life ..... 15
- Intentions, digital footprints, and paradoxes of the respondents ..... 16

Unionen's proposal for improved personal digital integrity in work ..... 21

- 1. Comprehensive legislation regarding personal integrity in work ..... 21
- 2. Joint work on digital integrity ..... 21
- 3. Recommendation to the members of Unionen ..... 22

Sources ..... 23

# Preface

The right of privacy and protection of personal integrity in one's working life is an area that encompasses a number of complex issues. What they all have in common is that they include what an employer knows and what an employer should know about their employees. The fundamental principle must always be that the employer should know as little as possible and only collect the information about their employees that is necessary for the management and allocation of the work.

At the same time, we are in an age where the boundary between what we keep private and what we publicly share is becoming increasingly fluid. Technical possibilities for one to share their private life with the world-at-large and in their role as a consumer are driving factors.

This development is taking place in parallel with the blurring of the lines between work life and private life. The private sphere often takes place partly in laptops and smartphones that have been issued to people from their employer. We find ourselves at an intersection between work, personal privacy issues, and digital development. There are risks here, some obvious and others more subtle.

Personal digital privacy in one's working life is certainly not a new issue. However, the trend towards increased teleworking and innovations in data-driven working methods means that the conversation about personal digital personal in one's working life deserves even more attention. Even if the debate is not new, there are still not enough answers.

Unionen believes and hopes that the conversation about digital privacy in one's working life will become more important for more and more people in the coming years. We look forward to listening attentively to what others have to say, and to ourselves actively participating.

This is the first of two reports that Unionen is publishing concerning personal digital integrity in one's working life. This report focuses on digital data trails in work devices. The second report will delve into the issue of the collection and use of data generated by employees. The report has been translated from Swedish.

Katarina Lundahl
Chief Economist

# Introduction

The use of an Internet and/or network connected device (e.g., a smartphone or a laptop) leaves a trail in the form of data. These data trails, this information about our use of the device, can be collected, structured, and analysed. It raises questions about, among other things, personal privacy, the value of data, possibilities and risks of being constantly connected, and about democracy.

In recent years, we have had a debate about the relatively new, but still extremely large parties whose business concept is to collect and use our digital footprints. The very size of the parties is considered by many to impede and stifle competition, contributing to a deterioration of the democratic discourse by having unhealthily deep knowledge and insights about their users. Digital data trails have become a societal issue.

Similar problems that are discussed at a societal level are found in the working life of employees. It is not uncommon that laptops and smartphones that an employee has access to via their job will be used for personal purposes. It may even be the case that personal accounts with providers of e-mail, online music or movie services and search engines are enabled on work devices. Having your work mobile as your personal mobile is not uncommon.

One risk with digital data trails is that they can be used to commit a data breach resulting in an intrusive invasion of privacy. Filtering parts of one's private life via devices owned by one's employer results in certain problems arising. At the same time, a large proportion of us have behaviours that do not take such risks into account. Sometimes, on the contrary, our use of digital devices provided by one's employer can be in direct opposition to how we should use the devices.

This report analyses risks with digital data trails in work devices from a trade union perspective and what can be done to prevent such risks. Unionen hopes that this report will raise interest in a discussion about personal digital privacy in one's working life.

# Digital data trails

## Digital data trails

Every interaction an individual has with a digital device leaves some form of a data trail. These data trails can be collected, categorised, and analysed by anyone who have access to the data trails. Via such an analysis, a "digital version" of the individual can be created, a digital footprint.

The more clues there are from a particular individual, the greater the likelihood that this digital version of an individual is consistent with the real individual, at least in some respects. An individual who leaves, for example, large amounts of digital trails related to new-borns can be assumed to be in the process of forming a family or having just become a parent.

With a digital version of an individual, several assumptions can be made about, for example, the person's behaviour and life situation, which in turn may lead to probable changes in, among other things, the individual's consumption pattern.

Digital footprints can thus be said to have a value, at least for those who can, for example, use the information to sell a product. During the 2000s, several successful business models have emerged, where the analysis of digital footprints forms a core.

One illustrative example is social media platforms. Few owners of social media platforms charge their users a fee for use. This is due to that the data generated by the user in various ways, is more valuable to the platform owner, than the fee the same user would be willing to pay for the possibility to be present on the platform.

## We are enticed to leave digital tracks

Using smartphone apps to navigate is easy and provides user value in their daily life. But that value is also created for those who own and develop the apps, in form of data on how the user moves geographically, is rarely something the user consciously thinks about.

Every step and heartbeat can be registered by fitness trackers, smart health watches with or without smartphone apps. This can be perceived as something positive, as the user can then receive information that perhaps leads to them seek medical care, explore heart disease issues, or being inspired to exercise. That the information can be collected in a database with other users' information and analysed, seems to be overlooked.

Recently concerns have arisen about increased digital surveillance of office workers working remotely because of the COVID-19 pandemic-related restrictions. This is a debate that is likely to become more intense in the coming years.

# Digital data trails in the workplace

Discussions about digital data trails often take place within the framework of what information we as citizens and consumers share with private parties. One important aspect of this are the trails left to an employer, and what can happen later with such information.

## Tracking and data trails in the workplace isn't really a new issue

Already back in 2005, the Swedish Authority for Privacy Protection (then named the Swedish Data Protection Authority) investigated employers' surveillance of employees' activity on the Internet. The Swedish Data Protection Authority then found that the majority of employers had policies for how employees are permitted to use work devices for personal surfing the Internet and that about one-half of the employers surveyed exercised some form of surveillance.

The Swedish Work Environment Authority has written the following concerning its Regulation on Working With Computer Monitors (AFS 1998:5):

"The use of computer monitors and computers in one's working life can enable increased qualitative or quantitative control and surveillance of employees. This can be perceived as an intrusive invasion of privacy and risks increases the psychological strain at work if it takes place without the employees' knowledge.

Nor is it incompatible with the requirements of a good working environment from a psychological and social point of view to use computer technology in such a manner that information about individual employees is used in a way that becomes an invasion of privacy and violates their personal integrity."

In a case in 1999 (AD 1999 no. 49), the Swedish Labour Court found that a factual basis for dismissal (in the individual case) was that an employee had "installed Internet" on a computer without employer consent. By studying a file on the computer, the employer in this case was able to establish that of 2,700 website visits, the majority were of a personal nature.

In 2007, the American Management Association (AMA) published a survey of workplace surveillance in the United States. According to AMA, more than one in four of the employers surveyed had, at

one time or another, fired an employee due to misuse of an e-mail client.

Today we see that digital data trails, often in the form of e-mail messages, are used as evidence in labour disputes in Sweden. It is the rule rather than the exception that written evidence originating from digital environments is invoked in such disputes.

The most common reasons for dismissal from employment were breaches of company policies, use of inappropriate language, excessive personal use, and breaches of confidentiality clauses. In addition, it was identified that it occurs that employers track keystrokes and time at the keyboard, storage, and viewing of stored files, and time spent by employees talking on the phone.

In 2020, the issue gained new relevance as globally many people who worked in offices relocated their work from their office to their home, in line with the restrictions established to prevent the spread of COVID-19.

## One's private life and working life are intertwined

During the 2000s, the boundaries between private and working life have become less clear to people working in offices. It has become easier to take their work home. This is because portable employer-issued work tools (such as laptops and smartphones) have improved performance, while fast Internet connections and Wi-Fi networks in the home have become more common. Possibilities to respond to e-mails and to work with and share documents from home have increased.

For some people this has enabled a more flexible working life, but it has also meant that some feel that they are constantly on-call, which has a negative effect on recovery and private life.

The involuntary (but welcomed by many) teleworking by office workers because of the COVID-19 pandemic, has greatly increased the number of people who in their everyday lives have to deal with such more unclear and undefined boundaries. A report from the Swedish Post and Telecom Authority describes how some state that they also prefer to use their own personal computers and other tools in their teleworking, as the tools provided by the employer do not measure up.

A work environment that has no fixed physical boundaries means that the work devices also risk being used in a more limitless way. There is a high probability that they, in whole or in part, will combine private life and professional life together. Work devices can

be used for, for example, personal banking, shopping, media consumption for personal purposes or gaming, depending on the settings and restrictions on the device that have been installed by the employer.

In addition, certain activities that are possible to use the device for may be prohibited under the company's applicable policy. Irrespective of whether it is permitted, it is clear that certain personal activities take place with professional devices. As a result, in doing so part of one's private life takes place in a device belonging to their employer.

## Some digital data trails can be read by employers

A central aspect of digital footprints and work devices concerns employers' access to such digital data trails. However, which digital data trails an employer can have access to is a question with several answers. One fundamental factor is the purpose for which the digital data trails and other information in a work device are examined.

If an employer wants to investigate which websites have been visited on a work device, it may be justified if it concerns security. However, if the purpose is to monitor browser use in real-time, it is not permissible (unless it is for protecting the employees' safety and their exposure to risks).

According to similar principles, that an employer reads an employee's' e-mails may be permissible in certain contexts. If there are strong suspicions of disloyalty or criminality, it is likely that the reading of personal e-mails may be regarded as being justified. The same may apply to correspondence about work tasks where the employer has informed the employee in advance that their e-mails may be read; under the precondition that there is a legal basis for doing so. Ultimately, in the individual case, a balancing of interests must be struck between the employee's interests in personal privacy in relation to the employer's surveillance and 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 establish consent based on equal positions. Note: A

violation of the GDPR[1] can occur even if the employee has given their consent.

It is difficult, if not impossible, to list in detail what an employer may and may not do with digital data trails in work devices. Whether or not a certain collection and use of digital data trails (in real-time or afterwards) is permissible depends upon the circumstances in each individual situation. But at the same time, one's digital data trails are not automatically kept secret from the employer. An assessment must always be made in each individual case.

If employers want to study certain digital data trails, such collection and processing is always limited to a clear purpose. Digital data trails that are collected and processed for one purpose cannot then be used for something else. Regardless of this, the employer is required to inform the employee in advance e.g., that the reading of e-mails will take place or that a software system will be used to measure and/or evaluate performance. Otherwise, it may be a breach of the GDPR.

Finally, it should be noted that if an impermissible collection and use of digital data trails takes place, the damage has (at least in part) already taken place. Even if the collection and use is subsequently after-the-fact deemed unauthorised and impermissible. There are also risks that a digital footprint is made available via leaks or hacker attacks. That is reason enough as an employee to be extremely restrictive in their use of Internet connected work devices.

Entirely irrespective of whether the data that the employer has access to has been generated in a permitted or impermissible manner, a Swedish employer can use it in the event a dispute arises.

[1] The General Data Protection Regulation is a law that applies throughout the European Union.

# Risks with employer collection and use of digital data trails

In a questionnaire survey that has been done for this report (and which is presented later in the report), about 25 percent responded that they have good knowledge of how the employer collects and uses digital data trails left in work devices.[2] In other words, a large group does not have sufficient knowledge of how digital data trails are collected and used, even though they regularly leave such data trails. This gives rise to several problems, which are described in more detail in this chapter.

## Risks related to the use of work devices for personal purposes

Using one's work mobile and work computer for personal use seem to be, to some extent, relatively common. This is particularly the case for work mobiles, where the survey conducted for this report shows that a high proportion of the digital data trails left in work mobiles are of a personal nature.

This should not be interpreted as people are not working but are instead sitting and looking at apps in their phone for personal purposes. Rather, it shows that the work mobile is used relatively little for work and even more so after the end of the working day. This in turn suggests that many people also use their work mobile as their personal mobile.

Distinguishing between working life and working hours on the one hand, and private life and leisure on the other, becomes more difficult if both take place in the same devices. Not least at a time when more and more of work and private life involves the use of devices in ways that leave digital data trails.

Leaving a digital representation of oneself in a work device increases the risk that one will be exposed to an invasion of their personal privacy. This is a risk that may seem small to those who "have nothing to hide."

[2] The respondents who have responded with a 4 or 5 (on a five-point scale), where 5 corresponds to a high level of knowledge, to the question "Your use of work computer and work mobile leaves digital data trails in the form of, for example, web surfing history, geographical information, cookies and similar data. Do you know how your employer collects and uses such data trails?"

But personal privacy and digital footprints are not a matter of hiding secrets. Rather, it is a shift in values, where we do not think it is strange that employees in practice register which TV programmes they watch, or where they have been in their spare time, by using software programs and apps in the employer's devices.

In the long run, these are movements of boundaries between private life and working life that are probably not in the employee's best interest. Even if most employers do not study the information.

## Unauthorised collection and impermissible use of digital data trails

The risks of using work devices for private purposes are to some extent abstract. That does not make them any less important. But there are also more concrete risks concerning how one's employer collects and uses the digital data trails, irrespective of whether they are private or left as part of the use of the devices for work.

One major risk is that if the knowledge about collection and usage of digital data trails is limited, an employer can process digital data trails in a way that is not permissible, without a suspicion that this is taking place. This applies to not only to intentional collection and use, which can be said to be in direct opposition to the employee's interests, but also to unintentional or unreflected collection and use.

Personal data trails can become, in the worst case, a means of power in a conflict between employers and employees. Even if it is unusual, the mere risk of such an invasion of personal privacy is something that requires solid preventive work.

Some computer systems have functions that register data in various ways without informing employees. An analysis of such data may appear to potentially increase productivity for the person reading it. At the same time, there is a risk that the reader of the information lacks knowledge, for example of the GDPR provisions, or assumes that everything is in order. This further illustrates the need for efforts to prevent digital data trails from being used inappropriately, irrespective of the purpose.

## Security risks with digital data trails in work devices

Over the past decade, Sweden has seen a series of breach incidents in private and public systems where secret data was leaked in one way or another. Not infrequently was sensitive personal data leaked. The question is no longer *if* a breach of personal data will

happen again but rather *when* it will happen. Computer systems are regularly attacked, while many systems in use lack what could be regarded as adequate protection.

Here are further arguments for refraining from using work devices for private purposes. The data trails left can simply end up in the wrong hands. It is conceivable that hackers get access to individuals' digital data trails that the individuals do not want the employer to have access to.

It is not uncommon for individuals to have what can be regarded as a substandard level of security in the use of digital devices. It could even be said that for a large proportion of us, it seems almost impossible to achieve a sufficiently high level of security.

Whether it is due to a lack of understanding that a high level of security usually requires tools such as password managers, or something else, can be discussed. Irrespective of the reason, the effect is that the level of risk increases. Thus, when work devices are also used for private purposes, they are also exposed to additional risk.

In conversations about digital security, the importance of difficult-to-crack and unique passwords is often mentioned, as is the recommendation not to open files in e-mails from insecure sources, et cetera. That is without doubt good advice. But at the same time, the security responsibility in the use of work devices cannot rest solely on the individual. The ambition that everyone should maintain a consistent and high level of awareness of the security situation will probably not be fully achievable, in almost any organisation.

It is better that recommendations on conscious security behaviour come with robust security systems. One important way of dealing with this is that no individual user should be able to jeopardise the security of the system via the use of a work device. The responsibility for security must always be the employer's.

# The Privacy Paradox

This report has so far discussed how the use of work devices for private purposes poses risks. This chapter discusses why such use often takes place against one's better judgment. It turns out that people seem to have strong thoughts about invasions of personal privacy related to digital data trails. At the same time, such views do not lead to a pattern of behaviour in line with such views.

In this report, this is categorised as the "privacy paradox." A paradox arises when something in a theory or explanatory model cannot fully explain what is occurring in human behaviour. For example, it can be about human behaviours that take place even though an understanding of the behaviour should lead to it not taking place. In this case, it concerns a behaviour that increases the risk of an invasion of personal privacy personal via the use of workplace issued devices, despite a generally high level of sensitivity for invasions of personal privacy.

The privacy paradox is centred around the following: Although the majority state that they are concerned about how their personal privacy may be violated in connection with the use of digital devices provided by one's employer, they do very little (or nothing at all) to protect or prevent the collection of personal data and behavioural data when using digital devices provided by their employer.

At the heart of this theory is knowledge of people's general attitudes vis-à-vis personal privacy and digital devices. The knowledge testifies to a dichotomy between personal privacy attitudes and actual behaviour. It is even the case that many people voluntarily share information about themselves in exchange for an increased degree of custom-made offers, based on the digital representation of one's person.

In social media there is a similar pattern. Even if it is possible to limit how one's communications are made available to others, concerns that third parties may be in the background and collecting data often do not seem to lead to such restriction in practice. Personal information is posted relatively openly, sometimes even with a conscious indication of the time and physical location where the post was made. It is reasonable to assume that many people treat their employer-issued devices in a similar way.

# Studying the privacy paradox

To explore the issue of personal digital privacy in the working life, this report uses a methodology based on observations of a group of respondents' digital behaviours, in a study commissioned by Unionen.

The respondents' digital behaviours have been investigated via an app that has been, with the individual's consent, installed on a digital device. The observations have been combined with a questionnaire looking into the respondents' views on digital privacy and related issues.

The method is described here in more detail before the survey itself is presented.

## Method

For a period of four weeks, the respondents' web surfing history and search terms, app usage and time spent on the device were registered, after which the data was analysed. The respondents were also asked to answer a questionnaire with questions related to digital behaviour. The combination enables an exploration of the respondents' attitudes and opinions and how it relates to their actual digital behaviour.

The respondents were recruited in a web panel, representative of Sweden's population aged 25–79. They filled in a recruitment and profiling questionnaire form that collected demographic, socio-demographic and attitudinal (especially in relation to technology and views on personal privacy) information. They were also asked if they could consider installing an application that collects data about their digital behaviour on any device (smartphone, computer or tablet).

About 10 percent of the respondents who filled out the profiling form approved the use of the app. It should be noted that the survey was conducted before the COVID-19 pandemic. The collection of data took place during the period June-September 2019. To ensure the representativeness of this group, the collected data has been weighted on gender, age, and region, as well as based on their approach and attitude to technology and personal privacy. After

completing the registration of the digital behaviour, the respondents received a follow-up questionnaire with more in-depth questions about personal digital privacy and digital working life.

Analysing the extensive amount of data collected that this type of methodology generates means that one needs to have a data-driven approach. Furthermore, data may inform the analyst about what is important to focus on, rather than validating preconceived theses or questions. In some cases, insights rest on the behaviours or responses of many individuals, and in other cases, it is an individual's behaviour that forms the basis for the conclusions drawn. The analysis in the report thus rests on both quantitative and qualitative approaches to the issue.

The total number of respondents upon whom the report's insights and understandings are based on is 190 persons, who are either gainfully employed for a company or sole traders. All 190 have had an app installed on a digital device of theirs and have responded to the follow-up questionnaire. Among these, 17 respondents have installed the app on what they state is a smartphone provided by their employer. On average, approximately 5,000 trackable activities were registered among respondents with a laptop over a 30-day period. The same figure for smartphones was approximately 3,700. Respondents who were registered on a work-issued smartphone registered approximately 6,100 trackable activities.

## Observations in a day in a respondent's life

To illustrate the level of information made available by digital footprints, here is an excerpt from a respondent's actual behaviour, from Unionen's survey. It is possible to follow each digital step the respondent takes, what time is devoted to various things and what they engage in. The information reproduced here is only a small fraction of the total of the respondents' data and an extremely small part of the total amount of information generated from the questionnaires.

**07.07** They start their computer. Logs into Facebook. And then Google and Microsoft Outlook. The hour between 7am and 8am is devoted to Microsoft Word, a PDF reader and visiting etsy.com in an Internet browser.

**08–09** They seem to be more focused on their work. Alternates between Microsoft Outlook and Edge.

**09–10** Continues the work and goes over to VISMA Administra-

tion. Social media also interrupts the working day at regular intervals, primarily in the form of Facebook.

**10–11** They work concentrated in VISMA Administration.

**11-12** The activity becomes more disparate. They visit loppi.se, visits familjeliv.se and read some threads about various family-related problems and challenges.

By studying in detail (the hours reported above in the respondent's digital life is a simplified overview) the digital data trails, a picture of a person is drawn. It is not a very complicated task to put together the puzzle that consists of a user's collective digital data trails into a digital footprint, to create an idea of who the person is, what they like, what they worry about, where they go, how they interact with their surroundings and so on. The likelihood of successfully identifying who the person is increases with access to more digital data trails.

## Intentions, digital footprints, and paradoxes of the respondents

In addition to the registration of digital data trails, the respondents in the survey were asked to answer a questionnaire. The answers have then been analysed based on how they use their devices, to give an idea of when paradoxes arise and what it looks like.

We start by looking at how much of the use of work devices was work and how much was other.

**Table 1: Average distribution of use of work mobile/work computer**

| Device | Non-work-related use | Work-related use | (total) |
|---|---|---|---|
| Work mobile | 89% | 11% | 100% |
| Work computer | 58% | 42% | 100% |
| N=190 | | | |

It turns out that on the respondents' work computers, almost 60 percent of the activity is not work-related. On work mobiles, just over 10 percent is used for work-related activity. In other words, both desktop computers/laptops and smartphones are used for a lot that have nothing to do with one's work.

Here it should be pointed out that the table should not be interpreted as meaning that those who have a designated computer at work are working only 43 percent of a working day and doing

other things the rest of the time. All activity, even outside normal working hours, is reported above.

The point is to illustrate what we do with the devices in addition to work-related tasks. When it comes to mobile phones, it becomes especially clear. One possible interpretation is that those who receive a work mobile from their employer do not feel the need to also have a private mobile in addition to that. In addition, the figures can be read as meaning that the modern smartphone, despite its great potential, is underused as a work tool, which is why such a large proportion of its use is not work-related.

The figures are interesting since relatively few state that they have a very good knowledge of how the employer, who owns the devices, collects, and uses the digital data trails registered on them.

**Table 2: Your use of work computers and work mobiles leave digital data trails in the form of, for example, web surfing history, geographical information, cookies, and similar data. Do you know how your employer collects and uses such digital data trails?**

| | |
|---|---|
| 1. I have no knowledge of how my employer collects and uses such data trails | 38% |
| 2. | 12% |
| 3. | 25% |
| 4. | 12% |
| 5. I have very good knowledge of how my employer collects and uses such data trails | 13% |
| (total) | 100% |
| N=190 | |

It is noteworthy that half of the respondents responded with a 1 or 2 on the five-point scale. At the same time, an overwhelming majority state that they have been informed and are fully aware of the employer's policy regarding non-work-related use of work devices.

**Table 3: Have you been informed of and are aware of the contents of the policy regarding non-work-related use of your work mobile/work computer?**

| | Work mobile | Work computer |
|---|---|---|
| 1. I have no idea what is in the policy | 1% | 1% |
| 2. | 0% | 1% |
| 3. | 6% | 6% |
| 4. | 38% | 38% |
| 5. I have been informed of and am fully aware of the contents of the policy | 55% | 54% |
| (total) | 100% | 100% |
| N = 65/62 | | |

One interpretation is that there is an understanding of what the devices can be used for, but less understanding into how digital data trails are collected and used. It may then seem paradoxical that such a large proportion of the use of the devices is not work-related, when those who use the devices at the same time do not know how their data trails are collected and used.

One way of explaining this is that the value of being able to use the device for other than work is greater than any risks, or that one does not consider that there are any risks.

A high level of knowledge about digital data trails and footprints and their collection and use does not seem to significantly affect the use of work devices for private purposes.

**Table 4: Percentage who state that they also use their work mobile/work desktop computer for personal things**

| | Work mobile | Work computer |
|---|---|---|
| Has a work device (N = 105) | 76% | 82% |
| Has a policy concerning use of work devices (N = 62) | 81% | 76% |
| Fully aware of the contents of the policy (N = 57) | 80% | 74% |
| Knowledgeable about digital data trails AND fully aware of their collection and use (N = 43) | 78% | 71% |
| N = 190 | | |

Another explanation is that the respondents trust that their digital data trails are not used in an objectionable way.

When the respondents are faced with a number of situations concerning the issue of digital tracking and are asked to categorise them based on whether or not they constitute an invasion of privacy or otherwise are intrusive, some interesting answers can be seen.

**Table 5: To what extent do you think these situations constitute an invasion of invasion of personal privacy?**

| | 4. 5. Invasion of privacy/ intrusive invasion of privacy | 3. | 1.2. Not/not at all an invasion of privacy |
|---|---|---|---|
| Your employer sells parts of your digital data trails, such as location services, to another company. | 85% | 8% | 7% |
| By looking at your digital data trails, your employer has become aware of an event in your private life and questions you about it. | 78% | 16% | 6% |
| A prospective employer requests access to your social media accounts before giving you an employment contract to sign. | 73% | 14% | 13% |
| Your employer uses the digital data trails you have left behind as a factor in setting your salary and/or deciding upon your career advancement opportunities. | 70% | 23% | 7% |
| A social media company uses data trails from your activities on the Internet and in apps for financial gain. | 68% | 21% | 11% |
| Your employer requests to go through all your e-mail, chats, and Internet surfing history on your work computer. | 54% | 20% | 26% |
| By looking at your digital data trails, your employer has become aware that you have visited a website with sensitive material and is taking it up for discussion. | 46% | 30% | 24% |
| Your employer requests to go through all your use of your work mobile. | 40% | 25% | 35% |
| N = 190 | | | |

Some of the hypothetical situations that the respondents have had to decide on are perceived by a clear majority as an invasion of privacy. At the same time, it is not a concern that leads to risk-minimising behaviour. It is not possible to deduce from the answers whether this is due to, for example, a high level of trust that digital data trails are collected and used properly by their employer.

However, it is regarded paradoxical that many people seem to be very concerned, while at the same time there is extensive use of devices for private purposes and there is a lack of deeper understanding among the majority regarding how digital data trails are collected and used.

# Unionen's proposal for improved personal digital integrity in work

## 1. Comprehensive legislation regarding personal integrity in work

Legislation on personal integrity issues in the working life is currently found in the four fundamental laws forming the Swedish constitution, in the Swedish Penal Code and other criminal law legislation, in labour and employment law legislation including work environment legislation, and in the transposition of the EU General Data Protection Regulation. In other words, the legislation is not coherent, which opens for context-dependent subjectivity and inconsistencies in assessments. This is a problem, as the relationship between employer and employee cannot be regarded as one of equal power.

Unionen wants to see comprehensive legislation on personal integrity in work. Such legislation should not only encompass digital integrity, but also issues surrounding extracts of criminal records from registries, camera surveillance and drug tests, for instance.

The issue of improved legislation regarding personal integrity in work has been debated and studied in Sweden in the 2000s. However, no proposal for comprehensive legislation has been submitted, despite a clearly established need. The challenges and risks in maintaining digital integrity as have been discussed in this report add to the urgency of enacting such legislation.

## 2. Joint work on digital integrity

Unionen sees great advantages in the social partners jointly tackling the challenges that a higher proportion of connected work devices entails for the development of the labour market. There is reason to work together on the issue of how digital integrity should be dealt with, in addition to the legislation that Unionen wants to see.

Unionen encourages a broader dialogue between the social partners on the issue of digital data trails in one's working life. As with many other issues, there are large variations regarding the challenges and possibilities that exist with digital integrity, depending on the sector in the labour market. The Swedish social partner model constitutes a well-established framework for such a dialogue. Promoting digital integrity jointly also has the potential to further evolve the social partner model.

Unionen recommends that local union representatives and employers jointly establish, for example, policies for the use of work devices. Such a policy will need to exist in line with robust security systems. In this context, it is important to ensure that such a policy is embedded in all employees in the company, and that the policy or security system does not result in an infringement of, for example, the GDPR.

## 3. Recommendation to the members of Unionen

This report illustrates the problems and risks associated with the use for personal purposes of digital devices provided by one's employer, usually laptops and smartphones, referred to in this report as "work devices' or "work mobiles." Unionen recommends its members to generally avoid using work devices for private purposes, if possible.

The use of work devices for personal purposes may appear to be harmless. A social media account on one's smartphone, a funny video clip on the desktop during lunch, and so on. Certainly, not every single use of a digital work device for personal purposes is a big deal. But one use often becomes more. A shift in boundaries is slowly taking place that is not healthy and exposes both the individual and their employer to risks.

There is not much to lose by avoiding the use of work devices for private purposes, except possibly a good laugh. But that effect should be achievable during a break with one's personal mobile.

# Sources

AD 1999 No. 49

AMA & ePolicy Institute Research (2007): 2007 Electronic Monitoring & Surveillance Survey

The Swedish Post and Telecom Authority (2021): “Digital omställning till följd av covid-19” [Digital Transformation Post COVID-19].”

**We live in a time where the boundaries between what we keep private and what we are public with are becoming more and more blurred. These developments are taking place in parallel with the blurring of boundaries between work and private life. This leads to the private sphere partly taking place in laptops and smartphones people have received from their employer to do their work. We reach an intersection between work, privacy issues and digital development. There are risks here, some obvious and others more subtle.**

**This report discusses the risks of private data trails in network connected work devices from a trade union perspective. The report is the first of two on issues of digital integrity published by Unionen.**

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.

Reg. no.: 3213-1 Production: Unionen