

*Juhani Korja**

SURVEILLANCE IN THE WORKPLACE AND WORKER PRIVACY

1. Introduction

As long as there has been employment, employees have been monitored. Recent years, however, in part due to technological advancements, have witnessed an explosion of monitoring and surveillance in the workplace¹.

With the present technological advancements, increased informatisation of our daily lives, and the potential for social management, surveillance has become a key to understanding the workings of power within the global information economy, and the exercise of power has always been an integral component of any employment relationship². Therefore, it can be argued that once modern techno-

* Researcher, Labour Law and Social Law Faculty of Law, University of Lapland, 96300, Rovaniemi, Yliopistonkatu 8, Finland.

¹ Long before the first electronic information systems, Jeremy Bentham and Robert Owen hatched schemes for improving human character through rigorous surveillance. What they had in common was that both had the idea that watching people more closely and correcting their behaviour more systematically would lead to more rational social arrangements. Both Owen and Bentham saw the workplace as the quintessential setting where enhanced surveillance and social control would help produce more efficient conduct, and ultimately better people.

² Although surveillance is seen as privacy invasive and intrusive, surveillance has also been linked to empowerment. As Ariene Ellerbrok puts it: "Can surveillance technologies be viewed as having the potential to empower those who are 'watched'? Or put another way, as an individual is made increasingly visible through their exposure to surveillance, is this visibility fundamentally exploitative, or might a person turn it to their own ends? The internet, web blogs, online social networks, and mobile phones all come to mind here, where increased visibility may allow for the "building of self as brand" and other forms of identity empowerment". A. Ellerbrok, *Empowerment: Analysing Technologies of Multiple Variable Visibility*, p. 201, <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3486/3440> [13.07.2014].

logy has given employers new tools to monitor employees and exercise power in the workplace, surveillance in the workplace must also be understood as the employer's means of exercising power.

Surveillance, due to its privacy invasive nature, is usually perceived as intrusive. For this reason, surveillance has become a central topic of legal discourse in the society. The problem with workplace surveillance lies in the competing interests of the employer and the employee.

Employees expect to have some privacy in the workplace in relation to the employer, even if they are on the employer's premises and using the employer's equipment. At the same time, it is normal that working for someone means giving up some privacy, suitably to the employee's position and tasks. Employers need basic information about their employees for things like pay and benefits, and they have to be able to ensure that work is being done efficiently and safely³.

By protecting privacy, including privacy in the workplace, the society protects the moral and other values in the society. Privacy is a counterpart of surveillance because one important aspect of privacy is the right to be beyond the reach of surveillance. Privacy therefore protects individuals from unauthorised intrusion into their private sphere.

2. Surveillance as a right of the employer

2.1. What is surveillance?

Surveillance technologies are increasingly embedded in the minutiae of our daily lives, tracking our more significant activities⁴.

Earlier the word surveillance was reserved for highly specific scrutiny of suspects. Since then the situation has changed. Surveillance nowadays occurs rou-

³ In the Finnish Employment Contracts Act is stated that the employer must ensure occupational safety and health in order to protect employees from accidents and health hazards, as provided in the Occupational Safety and Health Act (Chapter 2, Section 3). The act also states that the employees shall perform their work carefully, observing the instructions concerning performance issued by the employer within its competence. In their activities, employees shall avoid everything that conflicts with the actions reasonably required of employees in their position (Chapter 3, Section 1), and that employees shall observe the care and caution required by their work duties and working conditions and apply all available means to ensure their own safety and the safety of other employees at the workplace (Chapter 3, Section 2).

⁴ The increasing surveillance has led to the discussion about whether or not we are living in a surveillance society. It can be argued that we are currently living in a surveillance society where massive surveillance systems underpin our everyday activities. The same argument has been provided by L. Amore et al., *A Report on the Surveillance Society: For the Information Commissioner by the Surveillance Studies Network*, edited by: David Murakami Wood and Kirstie Ball, <http://libertyparkusafd.org/lp/Hale/Special%20Reports%5CSurveillance%20State%5CA%20Report%20on%20the%20Surveillance%20Society%20--%20Public%20Discussion%20Document.pdf> [13.07.2014].

tinely, locally and globally. One might even say that surveillance has become an unavoidable feature of everyday life in the modern society.

The Concise Oxford Dictionary equates surveillance with “supervision, close observation and invigilation of individuals who are not trusted to work or go about unwatched”⁵. While this definition has a traditional sounding ring to it, it captures a dimension of surveillance which is increasingly discussed in current debates – trust. Trust is the traditional element of and a motive for surveillance: surveillance is practiced because those in positions of authority do not trust those below them. Alternatively, however, surveillance can also be defined as collecting and processing personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered, and does not usually involve embodied persons watching each other⁶. Surveillance can therefore be considered as a practice of gathering and sorting data with one explicit purpose: to influence and manage the data subject. Therefore it can be argued that surveillance, especially workplace surveillance, should be viewed as a means of exercising power⁷.

2.2. Does the employer have the right to surveillance?

Power, in its most basic form, is the ability of a person (i.e. the employer or the employer’s representative) to exert his or her will over another. How the employer/representative chooses to use power in a workplace context depends greatly on his or her personality and position within the company⁸. The work situation

⁵ H. W. Fowler, F. G. Fowler, *The Concise Oxford Dictionary, 8th Revised edition*, Clarendon Press, 1990, p. 1302.

⁶ D. Lyon, *Surveillance Society: Monitoring Everyday Life*, Open University Press, Buckingham 2001, p. 2. This kind of definition of surveillance describes well how the surveillance has changed from the traditional into the “modern” surveillance.

⁷ Power can be defined as the possession of control, authority, or influence over others. In the Finnish labour legislation one characteristic of an employment relationship is to perform work for an employer under the employer’s direction and supervision (Employment Contracts Act, Section 1).

⁸ Lipkin discusses the different types of power in her book, “What Keeps Leaders up at Night”. Her analysis uses the five types of power introduced by psychologists John French and Bertram Raven in 1959, along with two types that were introduced later.

According to Lipkin, workplace power can be categorised accordingly:

1) **Legitimate power:** a person in a higher position has control over people in a lower position in an organisation;

2) **Coercive Power:** a person leads with threats and force;

3) **Expert Power:** the perception that one possesses superior skills or knowledge;

4) **Informational Power:** a person possesses needed or wanted information;

5) **Reward Power:** a person motivates others by offering rises, promotions, and awards;

also dictates the proper way to exercise power. For example, an employer attempting to exercise a type of power inappropriate for the given situation may find employees less receptive to obey.

The exercise of power is an integral element of any employment relationship. This is based on the fact that work is performed under the employer's direction and supervision. Each employer exerts a form of power in the workplace. How an employer chooses to use power in a workplace context depends greatly on the employer. The work situation also dictates the proper way to exercise power. One part of this power is surveillance. Surveillance can be justified at least for the following reasons:

- to guarantee legal compliance,
- to ascertain legal liability,
- to protect business information, security and safety,
- financial reasons (i.e. productivity and quality control).

Because the employer is responsible for all of the activities that happen during the working hours⁹, the employer has the right and obligation to monitor the workplace. This is also a strong indication that surveillance is an integral part of the workplace and of the rights of the employer¹⁰.

2.3. Possible Effects Of Workplace Surveillance

The growth of surveillance practices in the workplace has brought about discussion on the possible effects surveillance activities may have on the workplace.

6) **Connection Power:** a person attains influence by gaining favor or simply acquaintance with a powerful person;

7) **Referent Power:** the ability to convey a sense of personal acceptance or approval.

N. Lipkin, *What keeps Leaders Up at Night: Recognizing and Resolving Your Most Troubling Management Issues*, American Management Association, 2013.

⁹ It should be noted, however, that the employer's responsibility over the activities of the employees is not absolute. This is because the employee is also responsible for his/her actions. For example, in the Finnish Employment Contracts Act is stated that employees shall perform their work carefully, observing the instructions concerning performance issued by the employer within its competence. In their activities, employees shall avoid everything that conflicts with the actions reasonably required of employees in their position. The act also states that employees shall observe the care and caution required by their work duties and working conditions and apply all available means to ensure their own safety and the safety of other employees at the workplace (Chapter 3, Sections 1 and 2).

¹⁰ It should be noted, however, that the means and limits of surveillance differ in every situation. For example, in the Finnish legislation some more privacy intrusive surveillance activities have strict limits set in legislation. This is the case with i.e. video surveillance which has been stipulated by the Act on Privacy Protection in the Working Life (Chapter 5, Sections 16 and 17). This is to show that the surveillance activities of the employer are limited by legislation. In the lack of legislation, the surveillance activities of the employer are limited by the responsibility to respect the rights of others, in this case the employee's right to privacy.

Productivity and quality control are vital matters in running a business. Managers, therefore, believe that monitoring improves employee productivity and assures quality of service. This is understandable, because surveillance is a useful way of shaping conduct as individuals know they will be assessed and may start to behave accordingly¹¹.

On the other hand, however, it could be argued that monitoring has negative effects on employees. This is so because monitoring can lead to stress, anxiety, and loyalty decline. Workplace monitoring sends a direct message to employees that they are likely to do something wrong and, therefore, need to be watched¹². This causes distrust, which can be very harmful in an employment relationship, because it demoralises the employees. In any human relationship trust is a crucial element; without trust human interaction would be very limited.

Therefore opponents of surveillance also say that surveillance has adverse impacts on employees' attitudes, which results in lower productivity. It is argued that surveillance shows employers' distrust toward their employees, and when employees feel that their employers do not trust them, it might lead to a loss of motivation to work hard.

It has to be pointed out that surveillance may also harm the relationship between employers and employees. Surveillance might, therefore, generate undesirable tension between employers and employees.

3. Counterpart of surveillance – employee right to privacy

3.1. What does “privacy in the working life” mean and why is it protected?

Privacy can be seen as a contingent concept. Although privacy has been identified as one of the major ethical issues in the era of ICT, no one has been able to give an explicit definition of the concept¹³.

¹¹ The main reason not to engage in surveillance is because it affects employee conduct. B. Meier, *Panopticon Dreams: The Nightmarish Effects of Workplace Surveillance*, p. 105, http://ethicapublishing.com/ATEOI_ch7.pdf [13.07.2014].

¹² This view is shared by B. Meier, according to whom, employers who use panoptical surveillance are constantly knowingly or unknowingly increasing paranoia in the workplace. She argues that some companies even want their employees to feel as though their every move could be under surveillance. B. Meier, *op. cit.*, p. 100–101.

¹³ According to Solove, privacy is one of the most important concepts of our time, yet it is also one of the most elusive. As rapidly changing technology makes information increasingly available, scholars, activists, and policymakers have struggled to define privacy, with many conceding that the task is virtually impossible. Solove, *Understanding Privacy*. See also Saarenpää who describes

A sound communitarian treatment of privacy views it as a place or state in which an actor can legitimately act without disclosure and accountability to others. Privacy thus is a societal licence that exempts a category of acts from communal, public and governmental scrutiny¹⁴. In addition, privacy encompasses behaviours that members of a particular social entity are positively expected, by prevailing social mores or laws, to carry out so as not to be readily scrutinised. This kind of privacy definition is very normative because it includes an exemption from scrutiny and the requirement to close to view or hearing those elements considered normatively appropriate or inappropriate by the relevant society. Both the scope of privacy and the nature of the specific acts that are encompassed by definitions of privacy reflect particular values in the society¹⁵.

Because of the moral and societal nature, privacy is a multifaceted and dynamic concept that changes with the society and over time¹⁶. An exhaustive definition of privacy can therefore be seen unnecessary and even misleading¹⁷. But in order to evaluate the various privacy concerns, it takes to understand the areas¹⁸

the difficulty of defining privacy accordingly: “As a word, legal concept and institution, privacy is exceptionally challenging. It is easy enough to understand but difficult to define and identify. It is not particularly easy to legislate either. For the legislator, privacy very much resembles Tantalus’s fruit: just when it seems to be in reach, it withdraws yet remains temptingly visible”. A. Saarenpää, *Preface*, [in:] A. Saarenpää (ed.), *Legal Privacy*, Prensas Universitarias de Zaragoza, 2008, p. 9–16.

¹⁴ A. Etzioni, *The Limits of privacy*, Basic Books, New York 1999, p. 196.

¹⁵ *Ibid.*, p. 197. See also: F. H. Cate, *Privacy in the Information Age*, Washington D.C., 1997, p. 31 and A. Westin, *Privacy and Freedom*, New York 1967, p. 42.

¹⁶ A. Etzioni has stated that although we realise that individual rights were formulated under certain historical conditions, we tend to conceive of these formulations as truths rather than mores fashioned for a given time that are open to amendment as conditions change. A. Etzioni, *op. cit.*, p. 188.

¹⁷ According to A. Saarenpää a transitory comprehensive definition of privacy is unnecessary and would even be misguided. It must be recognised that privacy is not only a legal concept and principle but also, and above all, we are dealing with a broader description of the right to self-determination that is associated with the rights of the individual. If privacy was defined as a legal concept with utmost precision, that definition and any regulation that relied on it would have to be amended constantly to keep up with the development of society and technology. A. Saarenpää, *Perspectives on Privacy...*, p. 25.

¹⁸ A. Saarenpää has divided privacy into eleven main core areas: 1) physical privacy, 2) spatial privacy, 3) social privacy, 4) media privacy, 5) anonymity, 6) privacy in the processing of personal data, 7) ownership of information, 8) right to be assessed in the proper light, 9) patient privacy, 10) privacy in working life, and 11) communicative privacy. See also Stefanova, who separates four subcategories in privacy:

- 1) Physical inviolability – protection of the person in his or her physical aspect against procedures of interference such as tests for medications, experiments and so on;
- 2) Confidentiality of correspondence – security and confidentiality of the post services, telephone lines, including electronic mail and other means of communication;
- 3) Privacy of private property – posing restrictions against trespassing into the home and other kinds of environment.

which privacy protects. One of these areas is privacy in the working life. Privacy in the working life could be defined as follows: The employee's state or condition of being free from unauthorised and illegitimate observation or disturbance by other people in the workplace.

But why is privacy protected? On the individual level privacy is necessary for healthy personal development. An individual requires privacy to become autonomous and independent person who is able to interact with others, and also able to create rewarding and useful relationships. Respecting privacy can therefore be seen as an expression of respect for the autonomy of others. Since a society of incomplete individuals cannot function, privacy can also be justified by social considerations. Privacy not only allows us to develop healthy interpersonal relationships, it also seems to be required for democratic states to function. The answer to the aforementioned question is quite simple. Privacy is necessary for democratic states to function properly. This is also the reason why privacy needs protecting. We, as a society, should value and protect privacy, not because of its individual meaning, but because of its societal value.

3.2. Does the right to privacy apply to the workplace and to what extent?

The issue of privacy is central to the concerns raised by surveillance, wherever surveillance is applied. The multifaceted nature of privacy creates inevitable regulatory complexity. This is especially pronounced in relation to surveillance, particularly to the extent that it involves activities in the workplace. Surveillance is regulated to varying extent by constitutional or *quasi*-constitutional protections of privacy: statutory data protection regimes, civil law actions and laws restrict surveillance activities.

While the need for privacy protection against surveillance is not a new issue, it has become a more important one in recent decades because of the developments in technology. Technological development has increased the prevalence of surveillance and the forms it takes¹⁹.

Despite the ever-changing nature of privacy it has become an inerasable part of working life. Given that in nature privacy is a fundamental human right, employees enjoy at least a limited privacy protection in the workplace. In various

Inviolability of personal information – definition of rules managing the gathering of personal data such as credit information, medical expertise and so on. A. Stefanova, *Privacy on the Web*, [in:] A. Saarenpää (ed.), *Legal Privacy*, Prensas Universitarias de Zaragoza, 2008, p. 149–150.

¹⁹ The negative implications of surveillance first received detailed consideration in the context of convergence of computer and telecommunications technologies and its impact on information privacy. See, for example, M. Paterson, *Privacy Protection in Australia: The Need for an Effective Private Sector Regime*, "Federal Law Review" 1998, Vol. 26, p. 371.

institutions much of the traditional institutional power has yielded, the exclusive control of the employer over matters involving employee privacy is diminishing. The reasons for this are the general changes that have taken place in the working life, culture and, in part, legislation.

Human beings basically have, and should have, a right to be alone in society in relation to other individuals and organisations²⁰. This is the core of the right to self-determination. Private and public are profoundly different spheres. However, the right to privacy is clearly neither absolute nor inviolate. If this was the case, society and democracy would be impossible. This is also the case with workplace privacy. This is so because privacy not only allows employees to develop healthy interpersonal relationships, it is also required for the workplace to function properly. Privacy can therefore be seen as a moral value, even in the workplace context. It should be noted, however, that privacy, especially in the workplace context, is a relative right which sometimes has to give way to other important societal values²¹.

Although employee is under the direction and supervision of the employer and, therefore, subordinate to the employer, the right to privacy is a fundamental employee right which also applies in the workplace. The employer does not waive his/her right to privacy or any other fundamental rights and freedoms for entering into an employment contract. But because of the subordinate nature of the employment relationship, the employee's right to privacy has limited applicability. The reason for this is quite simple: the employer is responsible for all the activities that take place during the working hours. This does not mean that the employer has an absolute right to violate employee privacy. The employee should be able to function normally in the workplace without the employer's intrusion into the employee's private sphere.

This poses the question: How much surveillance is too much? One cannot set any definite and explicit demarcation line between surveillance and privacy. It can be said, however, that one knows that there is too much surveillance when employees begin to fear the surveillance activities and no longer feel free to exercise

²⁰ According to B. C. Stahl, we require privacy to become autonomous and independent humans, able to interact with others and create rewarding and useful relationships. B. C. Stahl, *Privacy and Security as Ideology*, [in:] S. Mercado Kierkegaard (ed.), *Legal, Privacy, and Security Issues in Information Technology. Volume 2. The First International Conference on Legal, Privacy and Security Issues in IT*, Institutt for rettsinformatik, Oslo 2006, p. 286–287.

²¹ One example of this kind of balancing of societal values is privacy vs. security. This balancing is a current question in the workplace context as well as in the society in general. The reason for this is that privacy and security overlap and reinforce each other. According to B. C. Stahl, security can be seen as a precondition of privacy because a lack of security may allow unauthorised access to data, which will jeopardise privacy. Both of these concepts also have to do with control. They also cater to the individual's psychological need to feel protected from outside interference. B. C. Stahl, *op. cit.*, p. 289.

their lawful rights²². The limits of privacy and surveillance can also be found in the Golden Rule: One should treat others as one would like others to treat oneself. In the workplace context this means that the employer should be very considerate when engaging in surveillance activities in the workplace.

3.3. Privacy in the workplace – finding the equilibrium

Privacy can be seen as an absolute or a relative right. Where it is perceived absolute, it requires no further justification. Privacy as an absolute right will have the status of a human right. But there is the other side of understanding privacy: privacy as a relative right. If perceived as such, privacy needs to be justified with regard to other values and rights²³.

The employer's right to monitor and the employee's right to privacy can be seen as counterparts, and both enjoy strong moral and legal protections. It should be noted, however, that it should not be about choosing one over the other. Surveillance in the workplace can be applied in a privacy-friendly way. The issue is about finding equilibrium between the rights of the employer and the rights of the employee. As Etzioni has said: "Good societies carefully balance individual rights and social responsibilities, autonomy and the common good, privacy and concerns for public safety and public health, rather than allow one value or principle to dominate"²⁴.

As mentioned in the previous chapters, the employer has a justified right and, in some cases, even a legal obligation to keep the workplace under surveillance²⁵. But this legitimate surveillance should be balanced with the employee's right to privacy. Essentially, this is an ethical issue²⁶.

²² B. Goold, *How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy and the Political Value of Privacy*, [in:] D. W. Schartum (ed.), *Overvåkning i en rettsstat*, Oslo 2010, p. 46.

²³ This distinction mirrors the one between privacy as an intrinsic or instrumental value. What both sides have in common is that both agree that privacy is a moral good. B. C. Stahl, *op. cit.*, p. 286. It should be noted, however, that both the European Convention for the Protection of Human Rights and the Charter of Fundamental Rights of the European Union state that everyone has the right to respect for his or her private and family life. This indicates that privacy can be understood as a human right and as a fundamental right. The Charter of Fundamental Rights of the European Union differs from the European Convention for the Protection of Human Rights in that the Charter also stipulates data protection as an individual fundamental right.

²⁴ A. Etzioni, *op. cit.*, p. 184.

²⁵ For example, in Section 3 of the Finnish Employment Contracts Act is stated that the employer must ensure occupational safety and health in order to protect employees from accidents and health hazards. This is one of the legitimate reasons of workplace surveillance.

²⁶ If a company truly wants to change behavior using virtue ethics is a simple way of doing so. B. Meier, *op. cit.*, p. 108.

The discussion of the ethics of surveillance should begin by noting the principles of fair information practice. These principles received widespread public notice in 1973 when drafted by the U.S. Health, Education and Welfare Department. Colin Bennett has expanded these to include²⁷: 1) accountability 2) identifying purposes 3) openness 4) limiting collection 5) limiting use, disclosure and retention 6) accuracy 7) safeguards 8) individual access 9) challenging compliance²⁸.

On the basis of these principles of fair information processing, the following surveillance principles have taken shape:

1) Respect of privacy

Surveillance always impinges upon the employee right to privacy, wherever it is applied. Therefore respect of the employee right to privacy must be the starting point. This stems from the societal value and fundamental nature of privacy. In a society an individual has a right to be apart from others. Therefore, the employer should respect the employee right to privacy when engaging in surveillance activities. In order to guarantee respect of the employee right to privacy, the employer should go through with a privacy impact assessment before engaging in surveillance.

2) Proportionality

Surveillance should be adequate, relevant and not excessive in relation to the purposes for which it is employed. The proportionality principle has three components: suitability, necessity and non-excessiveness. Suitability encompasses the notion of relevance, which means that the surveillance is relevant to the purposes for which it is employed²⁹. This implies that an employer should not engage in surveillance just because it is easy, cheap and effective. There must be a genuine need, a necessity, to engage in surveillance activities for the purposes of the legitimate interests of the employer³⁰. The employer should also remember that one aspect of harm and crossing possibly perilous personal borders involves going farther than is required or than has been publicly an-

²⁷ C. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca, New York 1992. G. Marx has stated that these principles are not adequate and that a more encompassing framework is needed. G. Marx, *Ethics for The New Surveillance*, <http://web.mit.edu/gtmarx/www/ncolin5.html> [13th July 2014].

²⁸ This data protection model forms the basis of the OECD Guidelines and most national legislation, i.e. the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

²⁹ This also implies that it is logically capable of achieving those purposes.

³⁰ In the Finnish Act on the Privacy Protection in the Working Life the necessity is phrased the following way: The employer is only allowed to process personal data directly necessary for the employee's employment relationship which is connected with managing the rights and obligations of the parties to the relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned (Chapter 2, Section 3 of the Act on the Privacy Protection in the Working Life).

nounced. Therefore the employer should remember that one should go no farther than is necessary for the task at hand. Non-excessiveness, therefore, implies that the means of surveillance is to be the one that is most privacy-friendly to fulfil the legitimate purpose³¹.

3) Openness

The openness principle can be divided into two different parts: awareness and consent.

A vital issue in surveillance is employee consent. Should the employer seek the employees' consent to surveillance? The answer is yes. The employer should seek employee consent. By consenting to it, employees are able to make informed decisions related to surveillance. Consent, as part of the openness principle, is necessary to respect employee privacy. Coercive surveillance does not belong in a constitutional state.

In keeping with the openness principle employers should inform employees whether they are subject to random or continuous surveillance³². Employees must also be informed about what surveillance tools are currently being used in their workplace and be provided with intelligible information as to what the management does with the data so acquired. Employees should be able to establish the existence of a surveillance system, its main purposes, as well as the identity of the person responsible for surveillance.

By doing so, the employer maintains openness and the employees are aware of the surveillance activities of the employer. Openness of surveillance is an essential part of the rights of the employee because covert surveillance does not belong in a constitutional state. According to Gary Marx, one component of justice is fair warning, which means providing people with information about the rules, procedures, rewards and punishments they are subject to. Marx argues that beyond showing respect for the person, full disclosure can be a means of shaping conduct as individuals know they will be assessed and may behave accordingly³³. This establishes an important point about surveillance: the ability of surveillance to make employees behave the way the employer wants them to behave. This is also the reason why surveillance can be seen as a means of exercising power.

4) Co-operation

Privacy is an essential part of individual self-determination. Individuals should have the right to choose to be beyond the reach of surveillance. This also applies to the workplace. Therefore, and in view of its privacy invasive nature,

³¹ See more on proportionality, Bygrave – Schartum: Consent, proportionality and collective power.

³² According to the Finnish Act on Privacy Protection in the Working Life it is stated in the case of using video surveillance in the work place there must be prominent notification of the video surveillance and its method of implementation is displayed in the areas in which the cameras are located (Act on Privacy Protection in the Working Life, Section 17).

³³ G. Marx, *op. cit.*

workplace surveillance should be implemented in co-operation with employees. This means that employees should be invited to participate fully in the decisions how and when electronic monitoring takes place. By doing so, the employer will know how the employees feel about the planned surveillance activities³⁴.

5) Safeguards

In order to effectively protect personal rights of individuals it is requisite to integrate sufficient safeguards into the surveillance system. In the context of workplace surveillance, these safeguards include the right to inspect, seek redress and sanctions, and challenge and express grievance.

Even if they're not required to do so by law, employers should give employees access to their personal information stored. This should be done so that employees can verify, and if necessary challenge, its accuracy and completeness. Employees must be permitted to inspect, challenge, and, when appropriate, request correction of their personal details and performance data.

Given the technological development dynamics and the fundamental nature of privacy, in order to guarantee that employee right to privacy is respected, certain legal safeguards must be put in place. This is so because the right to privacy, as a fundamental and societal value, cannot be hinged on morale alone. The stakes are too high for the workplace environment and for the society. People need privacy to develop themselves into properly-functioning individuals. Therefore surveillance activities in the workplace and the employee right to privacy need legal regulation in order to be balanced. The aforementioned workplace-surveillance principles can be used as a starting point for this legal regulation of workplace surveillance. Employers do not need an in depth understanding of privacy as a concept. But this does not mean that only awareness of the fact that the right to privacy also applies to the working life is enough in order to respect this right. Employers should also be aware of the value of privacy for the workplace environment.

³⁴ In the Finnish legislation the co-operation principle has been taken into account According to Section 21 of the Act on privacy protection in working life, the purpose and introduction of and methods used in camera surveillance, access control and other technical monitoring of employees, and the use of electronic mail and other data networks, are governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings and the Act on Cooperation in Government Departments and Agencies. In undertakings and in organisations subject to public law that are not governed by the legislation on cooperation, the employer must, before making decisions on these matters, reserve the employees or their representatives an opportunity to be consulted. After the cooperative or consultative procedures, the employer shall determine the purpose of the technical monitoring of employees and the methods used, and inform employees about the purpose and introduction of and methods used in the monitoring system, and about the use of electronic mail and the data network.

4. Conclusion

As mentioned above, workplace surveillance is not, in itself, a new practice. Nonetheless, this does not mean that the nature of supervising and controlling workers should be considered a stable, unchanging aspect of workplace relations.

This idea stems from the fact that the advancement of technology has significantly changed the workplace environment. The Internet and e-mail, in particular, allow employees to communicate effectively and efficiently with others. These technological developments have also provided employers with tools to monitor employees in the workplace. Monitoring could help reduce employee misconduct, increase productivity and prevent leakage of confidential information. On the other hand, it may also cause employee morale to decline in effect of the invasion of their privacy.

Surveillance has become a normal component of everyday working life. Paradoxically, surveillance, and in particular workplace surveillance, is much used but little understood. This is indicative of the need to understand how to manage an automated environment. We should remember that although technology is often involved in various privacy problems, these problems are not caused by technology alone. Privacy problems are primarily caused by people, businesses and governments, whose activities disrupt other valuable activities and thus create a problem³⁵.

Despite its controversial nature, surveillance is also an integral part of the rights of the employer. On the other hand, privacy, as the counterpart of surveillance, is a fundamental right of the employee. Therefore it can be argued that there are three major questions regarding surveillance in the workplace. First, the question of employer responsibility for employees. Employer has the right to monitor employees in the workplace during working hours because employer is responsible for all of the activities that take place during the working hours. Second major question is that of workers' privacy. Privacy is a fundamental part of the employee right to dignity and self-determination. This means that the employer is obliged to comply with the privacy rights of the employees. Putting these two questions together creates the third and probably the most difficult question: How to balance these to rights?

Employers have legitimate requirements for personal information about their employees. They need to know who they are hiring. They need to address performance issues and ensure physical security of their workplace. And they may see electronic monitoring and other surveillance as necessary to ensure productivity, stop confidential information leaks, and prevent workplace harassment.

³⁵ D. Solove, *Understanding Privacy*, Harvard University Press, Cambridge, Massachusetts 2009, p. 188.

In order to comply with the legal responsibilities in the workplace, employers sometimes have to delve into private matters. But they can keep those instances to a minimum, and limit the impact on personal privacy.

The possibility that an individual employee might do something harmful does not justify treating all employees as suspects. The questionable benefit of knowing what every employee is doing during working hours must always be weighed against the cost of surveillance – including the cost to staff morale and trust. Preventing workplace harassment, for example, is an important goal, but it must be noted that it is best achieved through workforce training and sensitisation, explicit anti-harassment policies, and appropriate remedial measures, rather than by depriving everyone of their privacy rights.

As a society, we should treat employees in a virtuous way. The virtue ethics perspective attempts to help people understand themselves and develop moral capacities to live and work well in all situations. We should therefore assume that workers are honest, trustworthy, loyal and focused employees³⁶.

How these two competing interests are balanced together is, in the end, a question of choice. Whatever the choice will be, it should be kept in mind that these two rights should be carefully balanced with each other, keeping in mind that good privacy practice is not just about avoiding complaints, grievances, or lawsuits. Fostering a workplace culture where privacy is valued and respected contributes to morale and mutual trust, and makes good business sense.

³⁶ B. Meier, *op. cit.*, p. 108.