Critically evaluate the law on privacy in the workplace. As part of your evaluation you need to consider the statutory and common law protection of workplace communication, and data about employees. Is the current law an unnecessary burden on employers?

In the modern technological society, it's all so easy for an employer to monitor the activities employees via electronic means. Nevertheless, this practice has the potential for abuse of the private life of the employee. As privacy is one of the principal civic and political rights declared by the Council of Europe in the 1950 European Convention on Human Rights (ECHR), the issue of confidentiality at the workplace has forced British government to pass number of legislative acts, such as the Data Protection Act 1998 (DPA), regulation of Investigatory Powers Act 2000 (RIP) and telecommunications (legitimate business practices), (Interception of Communications). Position in 2000 is putting greater responsibility on employers for privacy protection in the workplace. These laws accuse that it unnecessarily study due to the workplace and, thus, the employer must carry a greater burden. Indeed, the cost is expensive, but in fact creates a kind of balance between the interests of the employer and employee private life. The employer may have its causes for invading of privacy of employees, but the reasons have to be tested for effect to recognized human rights. Evidently, they must take into account the value of this test, and all the actions they should take if they are permitted by law to invade the privacy of the employee. Thus, a reasonable employer would not abuse the privacy of worker if it is necessary to do. This article attempts to assess the law of privacy in the workplace in the UK under the ECHR, DPA and the RIP, and the cases are filled with gaps in the statutory in this area, often mentioned in this article.

In a typical office, computerized data is recorded and processed with the moment the employee arrives. Arrival at work is recorded on CCT. The used of a swipe card to gain entry is recorded, and logging onto a PC is recorded, as well. He or she then starts their work, perhaps sending and receiving email… accessing the internet, using a telephone and leaving

voicemail messages, all of which are likely to involve recording of data. Data recording continues until the employee goes home.

This comment illustrates how employee's privacy has been interfered by employers. Employer can have many reasons why they need to monitor their employee during their work, such as to ensure they are doing their work and do not spend their time on their private life; to increase the chance that the business goes now without mistakes made by employee etc. Though Article 8 of the ECHR, it is declared that if there is an economic interest, such activities are not allowed. Ford, one of the known academic said: "The potential for abuse is clear. Information may be collected for purposes, which are irrelevant to performance at work; it may include private facts; it may be collected for one purpose but used for another; it may be inaccurate; and it may be disclosed to third parties without the knowledge or concept of the worker." [1]

Personal information collected by the employer is so important that they are parts of the definition of human existence. If employers can collect and use information about individuals, as an issue who took over greater significance or as a result of the computer revolution and greater power, now store and process personal information. Nevertheless, the storage and use of personal information in different forms took place during many years before the invention of the computer at work. Obvious examples include the personal files background and address of the contract staff, the disclosure of medical information to insurance companies and employers, and blacklisting of trade unionists held organizations sympathetic employers.

An important aspect of the protection of private life can be found in the Data Protection Act 1998. It was designed to give effect to Council Directive 95/46/EC. In 1984, it is replaced into the Law of the same title that applies only to computer information. Data subject to purposes of the 1998 Act is determined as "information" that is recorded or computer pro-

[1] Ford, Email and Internet Monitoring in the Workplace

cessed, as well as any other information that is recorded as part of the corresponding file system. The law also applies to certain medical and educational documents, local authority records or other information of the employer. These terms were narrowly presented to the Appeals Court [2]. Certain dates are described as being "sensitive personal data", a subset, or species from "personal data", and specified in mind personal information consisting of any of the following information about the data subject, race or ethnic origin, political opinions or religious beliefs, trading union status, sexual life, commission or the alleged commission of crimes and any criminal case brought against him or her (2).

The bases of the Law are eight principles for data protection, with which data controllers must comply s4 (4). They are presented in 1 of the following: 1) personal data has to be handled fairly and lawfully, 2) they should be received only for the specified legitimate purposes, and 3) they should be " adequate, appropriate and not exorbitant" in relation for the purposes, for which they are processed 4) they must be precise and kept up to data, and 5) they should not be kept longer than it necessary for the purposes, for which the data is processed, 6) they should be processed according to the right of a data subject, and 7) the relevant actions should be taken against unauthorized or illegal processing of personal data. 8) They cannot be passed outside the European Economic Area.

These principles may be further interpreted in the Act itself, and in the case of the first, it will provide, in addition, that in, at least, Sch 2 to be performed. This implies that the data will be handled only if the data subject has (the employee) consent to carry out any legal obligation, of which the data of the controller topic protect the interests of the data subject. It is not for "the purpose of legitimate interests of the data controller or hold by a third party or sides to see such information revealed. "If the data is "sensitive personal information", for at least one of the eleven conditions in the Sch 3 (as amended) must also be met.

[2] Durant V Financial Service Authority (2003) EWCA City 1746

The first of two key substantive aspects of the Act relate to the rights of the employee. Under the Act employee is entitled on request and in writing to be a) informed by the employer whether any personal data are being processed by the controller of data; b) given a description of the personal information and the purpose, for which they are being used, as well as the people to whom they can be opened and c) supplied with the information, which is being processed and informed of the logic, if any decision taken in relation to him or her is based solely on the "processing by automatic means of personal data" s7. The last is designed to protect people excluded credit because of their postal code or workers refused employment or promotion because of psychometric testing. There is a number of exceptions to the right of access, particularly, where it would necessarily involve disclosing confidential information about another person or company, and provision is made in the manner, in which the information should be disclosed. In normal circumstances, employee is entitled by giving notice in writing requiring the data controller to shop processing his or her personal data. An application may be made to court for an order to the data controller to correct or destroy an inaccurate personal data, being stored or processed by employer.

The second of the two main substantive provisions of the Data Protection Act 1998 relates to the responsibilities of the employer. Personal data are not to be processed unless the employer has first registered with the Information Commissioner s17. A post, which is created by the Act s6. Those applying for registration must describe the personal data to be processed, the purposes for which they are to be processed and the persons to whom employer intends to disclose the data s16. They must also provide a "general description of measures to be taken for the purpose of complying with the seventh data protection principle" s18 (2) (b). In addition, there is a duty to notify the Commissioner of any material changes to the practice of employer with regard to personal data s20. It is an offence to process data without being registered and to fail or notify any relevant changes s21. Though, it is rarely happen, the Secretary of State is empowered to make regulations to provide for the appointment of data protection su-

pervisors by employers; the role of the supervisor would be monitor “in an independent manner the data controller’s (employer) compliance with provisions of the Act” s23. An individual, who suffers damage, as a result of breach of the Act by the employer is entitled to recover latter compensation, and in some cases, it may be possible to recover also for distress suffered as a result of the breach s13. An example is the monitoring of the implementation of this Act. Monitoring, to a certain extent, is a part of daily employer - employee relationship. Most employers do some checking on the quality and quantity of the work done by their employees and employees are generally expected of.

Some employers supervise to protect their workers and to protect their own interests or the interests of their clients. For example, monitoring can help to ensure that the workers in dangerous jobs are not at risk from unsafe methods of work. Nevertheless, every person has the right to a degree of privacy at the workplace and the law does not establish certain restrictions on the monitoring activities. Some of the most controversial forms of control over the work include opening and reading emails of employees, control of Internet use, listening phone calls and installation of CCTV.

Usually, when employers are going to monitor the activities of employees, they must consult with the trade unions or employees and inform them about the control measures they are planning to introduce. They should also be clear that these measures are necessary and there is no less intrusive alternative. Monitoring should be done in a way that is not oppressive to employees.

Employers might want to control their workers for various legitimate reasons, such as discouraging thefts or violence. Workers tend to expect and accept a certain level of control as necessary - monitoring can help to control the workers in dangerous jobs, which are not in danger from the unsafe practices.Tthe monitoring may have an unfavorable impact on staff, if it is used inappropriately or in the wrong situations. This could invade

their privacy, disturb their work, or spoil a relationship of mutual trust between them and their employers.

The Data Protection Act does not stop the employers of monitoring the workers. Monitoring should not be routine or undue, while it includes collecting, storing and using information. In addition, if the employer holds the data he must do this in a safe way.

Before making a decision, whether to introduce mechanisms for monitoring, the employer must have a clear view of the reasons for monitoring of the personnel and benefits it will bring. Identifying any negative consequences of monitoring may have an impact on the staff, including their private lives at the workplace. It helps to consider are there the less obtrusive alternatives of monitoring to judge whether monitoring is justified, taking into account all aforesaid.

The employer should also consult with professional associations or staff representatives. The employer should inform the staff about any control mechanisms and the reasons why they are being or have been introduced except extremely limited circumstances.

If, for example, the employer is going to keep records of the websites visited by employees, the employee must be told the reasons for this. Employee should know which information will be recorded and stored, for how long, who has access to the information and how that information will be used.

In conclusion, it should be noted that the monitoring of personnel has its positive and negative sides to both parties. Successful monitoring is an ideal balance between the employers and workers' interests. It should aim at improving the performance of companies but also do not have to cross the line of ethical and moral standards. Penetrating too deeply into the private lives of employees in their workplaces will only hurt the overall result and success of the company.