УДК 349.2

I. V. Lagutina,
candidate of law, associate professor of the
department of labour law and social security law National University "Odessa Academy of Law"

THE RIGHT TO PROTECTION OF EMPLOYEE'S PERSONAL DATA

Protection of employee's personal information should enjoy great importance in the exercise of rights and obligations the employer has as a stronger party in employment relationships.

The protection of personal data as fundamental right studied such ukrainian scientists as V. M. Brizhko, V. A. Luzhetsky, A. V. Pazyuk, A. M. Chernobay, G. I. Chanysheva, R. I. Chanyshev and russian scientists: S.S. Bogatirenko, A. S. Dolgov, A.M. Lushnikov, N. L. Liutov A. S. Markevich, A. B. Prosvetov, V. I. Sedov, E. A. Stepanov, L. V. Tikhomirov, and also foreign scientists such as W.Berka, C. Grabenwarter, S. Gutwirth, Harris D., P. De Hert, Y. Poullet, M.Tinnefeld.

The purpose of this article is to analyze approaches to the definition of personal data, the legal regulation of personal data protection. Personal data is defined as any information related to an identified or identifiable employee. An employee is identifiable if by putting together different data contained in one or more files or documents the employee's identity can be determined.

Data protection refers to limits on the processing and use of personal data. This includes data about employees, such as personal health records, and data created or used by employees in emails or internet use.

The purpose of data protection is to protect individuals from the consequences of any form of processing of personal data, but particularly computer processing, and thereby to safeguard the right of self-determination over personal data.

In labour law, the employer may lawfully store personal data about employees provided that it is necessary in order to achieve the purpose of the

employment relationship. This is generally the case as regards data on the employee's age, training and performance.

International and European institutions are also paying increasing attention to the relationship between information and communication technologies (ICT) and privacy at work, with a number of recommendations and codes drawn up by bodies such as the Council of Europe and the International Labour Organisation - for example, in 1996, the ILO issued a code of practice on the protection of employees' personal data, covering general principles of protection of such data and specific provisions regarding their collection, security, storage, use and communication. There have also been relevant recent cases in the European Court of Human Rights.

On 26 April 2006, the Committee of Ministers of the Council of Europe decided to launch a Data Protection Day, to be celebrated each year on 28 January. This date corresponds to the anniversary of the opening for signature of the Council of Europe's Convention 108 for the Protection of individuals with regard to automatic processing of personal data which has been for over 30 years a cornerstone of data protection, in Europe and beyond.

Data Protection Day is now celebrated globally and is called the "Privacy Day" outside Europe.

Information and communication technologies (ICT) now play a significant role in enterprises, with growing use of computers in all aspects of operations and increasing communication and dissemination of information through the internet, internal intranets and the use of e-mail. For both employers and employees, there are new dangers linked to the development of ICT. Notably, as far as employees and their representatives are concerned, the main danger lies in the new capacity that exists for monitoring and surveillance. New technology may allow employees' work and productivity to be monitored, and also aspects of their personal lives, while their use of the internet and e-mail can be subject to monitoring (not least because of the traces any such use leaves). This raises questions of both privacy and the relationship of control at the workplace. These dangers can be even greater,

and the surveillance technology even more advanced, in situations where there is a physical distance between the employee and the employer [1].

The ILO Code of Practice does not prohibit monitoring of employees, but it does restrict it in two ways. First, the employees must be informed in advance. Second, employers must take account of the consequences on employees' privacy, etc. in choosing their methods of monitoring. Furthermore, the Code very much limits the use of secret monitoring to cases where it is necessary for health and safety reasons or for the protection of property.

The Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms states in Article 8 ('Right to respect for private and family life').

In 1970, the Council of Europe's committee of experts in human rights stated that the right to respect for private life is mainly based on a recognition of the interest that individuals have in being protected from all intrusions into their private lives and any parts of their lives that they legitimately want to keep to themselves. This interest, the committee went on, concerns personal communications and relationships, in addition to all matters touching the individual’s privacy and person, and in particular refers to his or her image, voice and home, and to all goods that relate to his or her personal life.

Case law in the European Court of Human Rights has established that the right to respect for private life extends to 'professional or business activities' and that as well as correspondence it applies to telephone conversations (whether business or private) - a principle which suggest that e-mails and internet use may also be covered [2, p. 12].

Trade unions in many countries are concerned that the current relationship between employees' privacy rights and employer monitoring rights is unbalanced, with the latter unfairly privileged. Trade unions are calling for clearer rules in this area and restrictions on employer monitoring.

A common data protection problem in today’s typical working environment is the legitimate extent of monitoring employees’ electronic communications

within the workplace. It is often claimed that this problem can easily be solved by prohibiting private use of communication facilities at work. Such a general prohibition could, however, be disproportionate and unrealistic.

For example, in Copland v. the United Kingdom, the telephone, email and internet usage of a college employee was secretly monitored in order to ascertain whether she was making excessive use of college facilities for personal purposes. The European Court of Human Rights held that telephone calls from business premises were covered by the notions of private life and correspondence. Therefore, such calls and emails sent from work, as well as information derived from the monitoring of personal internet usage were protected by Article 8 of the ECHR. In the applicant's case, no provisions existed which regulated the circumstances under which employers could monitor employees' use of telephone, email and the internet. Therefore, the interference was not in accordance with the law. The Court concluded that there had been a violation of Article 8 of the ECHR [3].

Collection of employees' personal data takes place even before the beginning of the employment relationship, during recruitment. It continues throughout employment and may extend even after its termination. Specific justifications may include compliance with the law; health, safety and security; assisting selection, training and promotion.

A specific aspect of data protection law in the employer–employee relationship is the role of employees' representatives. Such representatives may receive the personal data of employees only in so far as this is necessary to allow them to represent the interests of the employees [4, p.181].

Sensitive personal data collected for employment purposes may only be processed in particular cases and according to the safeguards laid down by domestic law. Employers may ask employees or job applicants about their state of health or may examine them medically only if necessary to: determine their suitability for the employment; fulfil the requirements of preventative medicine; or allow social benefits to be granted. Health data may not be collected from sources

other than the employee concerned except when express and informed consent was obtained or when national law provides for it.

Employers should regularly assess their data processing practices: (a) to reduce as far as possible the kind and amount of personal data collected; and (b) to improve ways of protecting the privacy of employees.

Important to note that employee must have the following rights:

1. Employees should have the right to be regularly notified of the personal data held about them and the processing of that personal data.

2. Employees should have access to all their personal data, irrespective of whether the personal data are processed by automated systems or are kept in a particular manual file regarding the individual employee or in any other file which includes employees' personal data.

3. The employees' right to know about the processing of their personal data should include the right to examine and obtain a copy of any records to the extent that the data contained in the record includes that employee's personal data.

4. Employees should have the right of access to their personal data during normal working hours. If access cannot be arranged during normal working hours, other arrangements should be made that take into account the interests of the employee and the employer.

5. Employees should be entitled to designate a employees' representative or a coworker of their choice to assist them in the exercise of their right of access.

6. Employees should have the right to have access to medical data concerning them through a medical professional of their choice.

7. Employers should not charge employees for granting access to or copying their own records.

8. Employers should, in the event of a security investigation, have the right to deny the employee access to that employee's personal data until the close of the investigation and to the extent that the purposes of the investigation would be threatened. No decision concerning the employment relationship should be taken, however, before the employee has had access to all the employee's personal data.

9. Employees should have the right to demand that incorrect or incomplete personal data, and personal data processed inconsistently with the provisions of this code, be deleted or rectified.

10. In case of a deletion or rectification of personal data, employers should inform all parties who have been previously provided with the inaccurate or incomplete personal data of the corrections made, unless the employee agrees that this is not necessary.

11. If the employer refuses to correct the personal data, the employee should be entitled to place a statement on or with the record setting out the reasons for that employee's disagreement. Any subsequent use of the personal data should include the information that the personal data are disputed, and the employee's statement.

12. In the case of judgmental personal data, if deletion or rectification is not possible, employees should have the right to supplement the stored personal data by a statement expressing their own view. The statement should be included in all communications of the personal data, unless the employee agrees that this is not necessary.

13. In any legislation, regulation, collective agreement, work rules or policy developed consistent with the provisions of this code, there should be specified an avenue of redress for employees to challenge the employer's compliance with the instrument. Procedures should be established to receive and respond to any complaint lodged by employees. The complaint process should be easily accessible to employees and be simple to use [5, p. 6, 7].

Thus, employers collect personal data on job applicants and employees for a number of purposes: to comply with law; to assist in selection for employment, training and promotion; to ensure personal safety, personal security, quality control, customer service and the protection of property. New ways of collecting and processing data entail some new risks for employees. While various national laws and international standards have established binding procedures for the processing of personal data, there is a need to develop data protection provisions which specifically address the use of employees' personal data.

The purpose for processing of personal data must be formulated in laws, other normative-legal acts), provisions, statutory and conform to the legislation in the field of personal data protection.

On 30 September 2010 Ukraine ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981. The Convention is aimed at the extension of the safeguards for human rights and fundamental freedoms, and in particular the right to the respect for privacy. It became a major step in realization of the Art. 8 of the Convention for the protection of human rights and fundamental freedoms of 1950.

The legislation on the protection of personal data is relatively new for all European countries. The Commissioner for Human Rights is convinced that it is extremely important for Ukraine to study and take into account the world's experience in order to create an effective mechanism that would ensure the observance of the constitutional right to the respect for privacy in the country.

The right to the respect for privacy is guaranteed by the art. 32 of the Constitution of Ukraine; the Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights" [6]; the Law of Ukraine "On the protection of personal data" [7], that came into force on 01 January 2011. This Law creates the State Service of Ukraine for the protection of personal data. The activity of the State service is aimed at protecting the person's right to the respect for privacy, analyzing the situation with the processing of personal data and providing necessary consultations on databases registration. According to the art. 22 of the Law of Ukraine "On the protection of personal data" the Ukrainian Parliament Commissioner for Human Rights exercises parliamentary control over the observance of person's right to the respect for personal data [7].

According to the art.14 of the Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights" the Commissioner is governed in his or her activities by the Constitution of Ukraine, the laws of Ukraine and other legal acts, observes the human and citizen's rights and interests protected by law, preserves confidential information and has no right to disclose any information concerning

the privacy of the applicant and others affected by this application without their consent. This obligation shall remain effective after the end of tenure in the Office of the Commissioner.

According to Article 2 of the Law of Ukraine "On Protection of Personal Data" (Date of entry into force: January 1, 2011), personal data is defined as data or a collection of data on a natural person that is or can be clearly identified. Processing of personal data is defined as any action or a series of actions performed partially or completely inside an information (automated) system and/or catalogue of personal data and related to collection, registration, accumulation, storage, adaptation, amendment, updating, use and dissemination (distribution, sale, transfer), depersonalization and deletion of data on a natural person.

Processing of personal data on a natural person is not allowed without their consent, except for cases determined by the law.

According to the Article 24 of the present Law, the state guarantees protection of personal data. Subjects of relations related to personal data are obliged to ensure protection of such data against unlawful processing and unauthorized access.

The processing of health data is in principle prohibited in view of the risk for the privacy of the individuals concerned. Nevertheless, taking into account the fact that the processing of health data is a necessary practice in the employment context, which may often be justified by various legitimate reasons for the benefit of both employers and employees, there are a number of general exceptions to this principle.

Also, employees should be informed about the purpose of the processing of their personal data, the type of personal data stored, the entities to which the data are regularly communicated and the purpose and legal basis of such communications.

Employers should also inform their employees in advance about the introduction or adaptation of automated systems for the processing of personal data of employees or for monitoring the movements or the productivity of employees.

Personal data on employees are processed for purposes directly relevant and necessary to the employment of the employee.

Personal data on employees collected are used in principle only for the purpose for which they were originally collected. Personal data must be processed fairly and lawfully.

The protection of employees' personal data is an increasingly debated issue. In its various aspects, it is currently the subject of active discussions, negotiations, regulations and research at international, European and national levels. This is notably due to the specific nature of the employment relationship as well as to recent socio-economic, organisational and technological changes.

In this context, it is important to strike a balance between the employees' fundamental rights, in particular that to privacy, and the employers' legitimate interests. Whilst this appreciation is carried out on a case by case basis, the question is raised whether it is advisable to have a framework of guidelines and rules regulating in a specific way processing of personal data in the employment field.

Key words: human rights, personal data of employees, processing of personal data of employees, use of personal data of employees.

У статті аналізуються основні підходи до визначення персональних даних працівників, роль захисту яких в сучасних соціально-економічних умовах значно зростає. Визначаються загальні вимоги до обробки і захисту персональних даних працівників.

Підкреслюється необхідність закріплення в національному законодавстві права працівників на захист персональних даних і гарантій його реалізації.

В статье анализируются основные подходы к определению персональных данных работников, роль защиты которых в современных

социально-экономических условиях значительно возрастает. Определяются общие требования к обработке и защите персональных данных работников.

Подчеркивается необходимость закрепления в национальном законодательстве права работников на защиту персональных данных и гарантий его реализации.

The article examines the main approaches to the definition of personal data of employees, the role of protection which in modern socio-economic environment significantly increases. Defines the general requirements for the processing and protection of personal data.

Emphasized the need for consolidation in the national legislation the right of employees to protection of personal data and guarantee its implementation.

Literature:

1. Delbar C., Mormont M., Schots M. New technology and respect for privacy at the workplace// [Electrical resource]/ Website the European Industrial Relations Observatory. – Mode of access: http://www.eurofound.europa.eu/eiro/2003/07/study/tn0307101s.htm

2. Kilkelly U. The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights/ Ursula Kilkelly.- Council of Europe, Human rights handbooks No. 1. – 2003. - 72 p.

3. ECtHR, Copland v. the United Kingdom, No. 62617/00, 3 April 2007// [Electrical resource]/ Website the European Court of Human Rights. – Mode of access:http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=00179996#{"itemid":["001-79996"]}

4. Handbook on European Data Protection Law Luxembourg: Publications Office of the European Union. – 2014. -214 p.

5. Protection of workers' personal data. An ILO code of practice Geneva, International Labour Office. - 1997. - 24 p.

6. Про Уповноваженого Верховної Ради України з прав людини: Закон України від 23.12.1997 № 776/97-ВР// Відомості Верховної Ради України. – 1998. – № 20. – Ст. 99.

7. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI// Офіційний вісник України. – 2010. – № 49. – Ст. 1604.

8. Protection of personal data//[Electrical resource] / Website the Ukrainian Parliament Commissioner for Human Rights. – Mode of access: http://www.ombudsman.gov.ua/en/index.php?option=com_content&view=article&id=1105