

SECTION 4.

PRACTICAL INNOVATIONS IN THE FIELD OF INTERNET OF THINGS AND ARTIFICIAL INTELLIGENCE

YAVORSKA O. S.

Ivan Franko National University of Lviv,
Head of the Department of Intellectual Property,
Informative and Corporate Law, Doctor of Law, Professor

LEGAL PROTECTION OF A PERSON IN CONNECTION WITH HIS PERSONAL DATA PROCESSING: EU EXPERIENCE

Key words: *personal data, Constitution, EU Directive, principles.*

The right to personal data legal protection should be considered in connection with the constitutional right to non-interference in one's private life and family matters (article 32 of the Constitution [1]), personal non-property rights fixed in the Civil Code as a constitution of private law, such as the right to information, the right to personal privacy and its secrecy, the right to personal papers, the right to the privacy of the correspondence [2]. In general, the national legislative approaches conform with the international ones, fixed in the General Declaration of Human Rights, Convention on Human Rights, International Pact on Civil and Political Rights.

Taking into consideration the informative technologies development, the problem of data protection is being actualized. Not often a usual passer-by has a clear idea about how, by whom and with what aim his personal data can be used. A person presents his own personal data while enjoying his right to labour, medical aid, education in accordance with the legislative requirements. Is this data properly protected from its further disclosure and application by the other subjects distinctive from those to whom it was granted according to the established requirements?

In the autumn of 2017 a leading firm which provides audit and consulting services «Deloitte» reported about the hackers attack which caused the data outflow both of the company employees and its clients. The data outflow was also possible due to the technical reasons in the system of corporate computer net protection. Large scandals concerning the usage of the personal data of the Facebook users by British company «Cambridge Analytica» showed that personal data protection is far from the desirable one. The private British company used the data analyzing technologies in order to elaborate the election campaign strategy and other social processes.

A scandal in Ukraine concerning the sale of the «Nova Poshta » clients personal data – an information about half a million people with personal data involving name, surname, city, passport data, email address and 18 million notations with less detalization involving only name, surname and phone number comes to mind.

The law «On personal data protection» [3] which was adopted in the context of Ukraine`s performance of the duty concerning the Treaty of the EU Association signature, partially solved a number of issues concerning personal data protection. It seems that the approach according to which data or totality of data about a person, who is identified or can be specifically identified, without an exact enumeration of it is personal data is absolutely correct. The rights of a subject of the personal data are established by the article 8 of the law. Among them is the right to know about the source of collection, location of one`s personal data, aim of its processing, location or place of residence either of the holder or manager of the personal data; to receive the information about the personal data granting permission conditions, in particular, the information about the third people to whom the personal data is being transmitted; to access to one`s personal data; to receive a response whether one`s data is being processed no later than 30 days since the request income, except for cases foreseen by the laws as well as to receive the content of such personal data; to present the motivated requirement concerning either shift or destruction of one`s personal data by any holder or manager of it in case this data is being processed illegally or is not authentic; to address a complaint on one`s personal data processing to the Authorized or court.

It is of great importance that every subjective right of a person should be corresponded by an appropriate duty either of a holder or manager of the personal data. For such duties not performance not only a civil responsibility in a form of inflicted losses reimbursement, an amount of which should be also proved, but public responsibility should be applied as well.

Decisive measures concerning this issue were taken in the EU. On the 27th of April, 2016 a Regulation of the European Parliament and Council (General Data Protection Regulation) was adopted and EU 95/46 directive was abolished [4]. Until the adoption of Regulation, EU Directive, which, on the one hand was obligatory to every member-state, but on the other was reserving a choice of the form and the way of the result achievement to internal instances was in force. The Regulation has full legal power and is to be enforced directly by every member-state. The adjustment of the personal data relation in the Regulation supports the importance of the issue. According to the article 99: the Regulation is to be enforced since the 25th of May, 2018.

Both the Directives and the EU Regulations are not boundary for Ukraine. However, their instructions are used as experience in formation the national legal base.

The validity of the personal data protection is attested by more than one hundred pages of the Regulation instructions, especially the instructions of the article 3 – territorial scope.

Its content attests the extraterritorial performance of the Regulation. Its instructions are applied to controllers or processors not established in the Union, where the processing activities are related to: the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union. A controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The main principles which are the basis of the personal data processing are the following: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.

Personal data processing is lawful if it is based on the person's consent. Child personal data processing is lawful if the child is at least 16 years old. Besides, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: the categories of personal data concerned; the recipients to whom the personal data have been or will be disclosed; the envisaged period for which the personal data will be stored; where the personal data are not collected from the data subject, any available information as to their source. The Regulation states «the right to be forgotten»: the data subject shall have the right to the erasure of personal data, which should be carried out not only by the controller without undue delay, but another people to whom the data was transmitted.

The duties both of the controller and processor are strictly fixed. In particular, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Taking into consideration the modern development level, costs on the realization, specifics, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, which are caused by the processing, the controller and the processor shall implement appropriate technical and organisational measures to ensure the safety level according to the risk.

Data protection certification mechanisms and of data protection seals and marks are being established, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The certification shall be voluntary and available via a process that is transparent. However, it does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities. Particular

attention is drawn to the formation, competence and interaction between the independent bodies of the member-states concerning the personal data protection. An origination of the European Council of data protection is foreseen as well.

According to the article 82 of the Regulation any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Stiff sanctions (fines according to the 83 article) for not applying the Regulation instructions are established. Depending on the nature of the offence administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher can be enforced. For separate kinds of offences the fine is up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Such an approach attests both the seriousness of the problems concerning personal data and the seriousness of the intentions to cope with them.

Applying any legislative instructions, in particular those directed at person`s rights and freedoms protection, should be ensured by the state coercion measures in case of their non-performance. If such instructions coincide with the subject inner will to act fairly, this is considered to be the ideal behavior model. However, the risks of the mismatch always exist. Therefore, the only way to reach the desirable model of the social behavior is a public responsibility for non-applying the legislative instructions.

References:

1. The Constitution of Ukraine. Verkhovna Rada of Ukraine. URL : zakon.rada.gov.ua/laws/show/254к/96-вп
2. The Civil Code of Ukraine. Verkhovna Rada of Ukraine. URL : zakon.rada.gov.ua/go/435-15
3. On the personal data protection. Law dated to 01.06.2010. Verkhovna Rada of Ukraine. URL : zakon4.rada.gov.ua/laws/show/2297-17
4. General data protection regulation. URL: https://zakon.rada.gov.ua/laws/show/984_008-16