References:

1. Бусел В.Т. Великий тлумачний словник сучасної української мови. – К.: ВТФ «Перун», 2003. С. 106, 306.
2. Бистрова Б. Основні поняття дослідження та концептуальні засади професійної підготовки фахівців із кібербезпеки // Педагогічні науки: теорія, історія, інноваційні технології. – 2017. – № 8. – С. 60.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. – 2014. – № 2. – С. 61.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163 -VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.
5. Європіна І.В. види протиправних діянь у сфері новітніх інформаційних технологій // Вісник академії адвокатури України. – 2010. – № 3. – С. 129.
6. Дімітрова Н. М., Н. М. Білик Основні види кіберзлочинів та причини, що їх породжують // Соціально-гуманітарний вісник. – 2018. – Вип. 22. – С. 50.
7. Кіпа О.О. Правопорушення в мережі Інтернет // Часопис Київського університету права. – 2010. – № 4. – С. 347.

NEKIT K. G.

National University «Odesa Law Academy»,
Associate Professor at the Department of Civil Law,
PhD in Law, Associate Professor

THE IMPLEMENTATION OF INFORMATION SECURITY AND PERSONAL DATA PROTECTION IN THE FIELD OF THE INTERNET OF THINGS

Key words: *personal data, European Union, GDPR, software.*

At the end of the twentieth century, the history of humankind was divided into two eras due to the emergence of the Internet. And the speed in the development of technology is gaining so fast, that today, at the beginning of the XXI century, we can talk confidently about a new era in our history – the era of the Internet of things. The number of devices connected to the Internet was 500 million in 2003, by 2010 their number had increased to 12.5 billion, and by 2020, according to various sources, Internet connections from 26 to 50 billion devices are predicted [1]. On the one hand, it opens up tremendous prospects for the development of society, but on the other hand, like any other new phenomenon, it gives rise to a number of issues. There are some issues in the legal sphere as well, because today we have no comprehensive solution regarding the legal regulation of relations in the field of the Internet of Things.

One of the most important issues in the field of the Internet of Things is the issue of personal data protection.

In order to ensure the personal data protection in the European Union, new rules for the processing of personal data were developed and the

General Data Protection Regulation (GDPR) was adopted (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC). According to that Act, companies that violate the rules for processing personal data risk being held accountable with fines of 20 million euros, or 4% of the company's annual income. The basic principles for processing personal data on GDPR are as follows:

1) personal data must be processed legally, fairly and transparently. Any information about the purposes, methods and amounts of personal data processing should be expressed as accessible and simple as possible;

2) target limitation: data should be collected and used exclusively for the purposes stated by the company (online service);

3) data minimization: it is impossible to collect personal data in a larger volume than is necessary for processing purposes;

4) accuracy: personal data that are inaccurate must be deleted or corrected (at the request of the user);

5) storage restriction: personal data should be stored in a form that allows the identification of data subjects for a period not longer than necessary for processing purposes;

6) integrity and confidentiality: when processing data of users, companies are obliged to ensure the protection of personal data from unauthorized or unlawful processing, destruction and damage [2].

The great importance for the development of innovations in the field of the Internet of Things are the so-called innovation-friendly rules enshrined in the GDPR. This rules are called Privacy by Design or Data Protection by Design. According to these rules, data protection guarantees in products and services that are being developed must be provided at the design stage. The basic principles of Privacy by Design are:

1) the necessity to take preventive measures, not just the elimination of consequences: the embedding of confidentiality in the design of the system should be active, and not limited to elimination of consequences. This approach should prevent the breach of confidentiality before it occurs. In other words, personal information must be protected before the system begins to work, and not after identifying breaches of confidentiality;

2) confidentiality as a standard setting: Privacy by Design seeks to achieve the maximum degree of protection of personal information, ensuring that personal data is protected automatically in a particular information system or business relationship. Even if an individual takes no action, his personal information remains secure. No action is required from the individual to protect personal information – the system initially contains the necessary settings;

3) confidentiality as a part of the structure: the protection of personal information should be an integral part of the architecture of any information system or business relationship. This should not be an additional component, introduced into the system post-factum;

4) protection of personal information throughout the entire cycle of its collection, storage, processing and destruction: confidentiality must be embedded into the system even before the data collection begins. Moreover, this protection must reliably extend over the entire data storage and processing cycle. In other words, the data preservation is important for confidentiality from the moment the system starts up to the end of its existence. This ensures reliable data storage, and after the end of its use – reliable and timely destruction;

5) accessibility and openness: all components and operations remain open and accessible, both for users and for those who provide this type of service;

6) respect for user privacy: the system should be user friendly. This is achieved by such measures as the protection of personal information by default, timely notification of the collection of personal information, giving the user the freedom to choose in a convenient and understandable way [3].

The above mentioned provisions on the personal data protection should be taken into consideration by the Ukrainian legislator. This is necessary both to ensure the protection of personal data of Ukrainian citizens through the adoption of a similar act, and taking into account the extraterritorial nature of Regulation (EU) 2016/679. The extraterritoriality of the GDPR means that this act applies to all companies that process personal data of citizens and EU residents, regardless of the location of such a company.

The problem of ensuring information security in the field of the Internet of Things requires close attention. One of the key tasks for ensuring information security in the field of the Internet of things is to take responsibility for this issue by the professional community. It is assumed that self-regulation and certification of devices belonging to the Internet of Things system will be able to help in ensuring information security.

The problem of reconciling the coexistence of the various components of the Internet of Things will help to solve the introduction of certain standards in the field of the Internet of Things. Proprietary and closed IoT systems must give way to open space. The situation when there are many different non-standardized devices is similar to the situation when each car manufacturer uses its own control system, a steering wheel would be installed in one car and a joystick or a control panel in the other. Or if it would have been impossible to call other operators by phone, and for household appliances of various brands, different types of water or electricity connections would be needed. Similarly, in the world of the Internet of closed or proprietary Things, in which devices are not connected to each other, the home owner will not be able to control the lighting, security system, thermostat, locks, etc. using a central application or control panel. Today the need for standards for the Internet of Things is increasingly recognized. For this purpose, the Association for Standardization has developed a number of standards and protocols designed to support the development of connected systems [4, p. 120-121].

It should be mentioned that excessive government intervention in the regulation of relations in the field of the Internet of Things may hinder the

development of technology. Considering that, to ensure information security in the field of the Internet of Things it is necessary, first of all, to apply self-regulation, which should be ensured through close cooperation between technology companies and civil society. This minimizes government intervention in this area, which will contribute to the rapid development of innovative technologies. There is only the need for legal regulation of relations between civil society, consumer protection organizations and technology companies. First of all, efforts should be directed at protecting human rights from violations related to the functioning of the Internet of Things. It is necessary to prevent such violations by monitoring the installation of proper protective software on all devices connected to the Internet.

References:

1. Храмцов П. Всеобъемлющий интернет: прогнозы и реальность // Открытые системы. – 2013. – № 4. – URL: http://www.osp.ru/os/2013/04/13035552/
2. GDPR – новые правила обработки персональных данных в Европе для международного IT-рынка. – URL: https://habrahabr.ru/company/digitalrightscenter/blog/344064/
3. Кавукиан Э. Privacy by Design: 7 основополагающих принципов. – URL: https://online.zakon.kz/Document/?doc_id=31633216#pos=0;0
4. Грингард С. Интернет вещей: будущее уже здесь. – М. : Альпина Паблишер, 2016. – 188 с.

MUZYKA V. V.

National University «Odesa Law Academy»,
Post-graduate student at the Department of European and International Law

USING ARTIFICIAL INTELLIGENCE IN JUSTICE SYSTEM AND THE MAIN CHALLENGES TO HUMAN RIGHTS REALIZATION

This article examines the issues of the operation and use of AI-powered systems and algorithms in justice system, and the main concerns they raise. It also analyses the most relevant examples of AI use, its ability to predict and the factors associated with predictive justice that may negatively affect human rights. Notwithstanding all the concerns, it is argued that AI-powered systems or algorithms may be used in harmony with human rights standards.

Key words*: artificial intelligence, AI, human rights, predictive algorithm, AI-judge.*

The reality of the world «as it is» is such that artificial intelligence (AI) might play a greater role than we think. Peoples all around the world use it in their everyday lives because AI brings obvious benefits, improve our lives and even makes us happier. However, relying enormously on AI may also