UDC 347.77:(007:004.056.5:004.738.5)
DOI https://doi.org/10.32850/sulj.2022.4.2.36

# LEGAL APPROACHES TO SOLVING SECURITY ISSUES IN THE FIELD OF THE INTERNET OF THINGS IN THE LIGHT OF EUROPEAN INTEGRATION OF UKRAINE

***Nekit K. H.***

*The article examines the peculiarities of legislative approaches to the legal regulation of relations in the field of the Internet of Things, which have developed in the European Union and the United States. In particular, approaches to defining the concept of the Internet of Things and its components are analyzed. Based on the analysis, it was concluded that the Internet of Things is defined as a kind of ecosystem that includes physical things equipped with devices that can connect to the Internet for the purpose of interaction. However, this concept does not apply to objects designed specifically for human use through an Internet connection, such as computers, laptops, smartphones, etc. The article pays special attention to the problems of security and protection of personal data in the field of the Internet of Things. In order to determine recommendations for the Ukrainian legislator in the field of ensuring the security of the Internet of Things, the existing European and American legislative acts are analyzed. In particular, the approaches to ensuring security in the Internet of Things at the level of GDPR, European and American legislation on cyber security were analyzed. Based on the results of the analysis, a conclusion was made regarding the need for certification and standardization of devices that are elements of the Internet of Things. However, standardization in the field of the Internet of Things should be carried out carefully in order to prevent the development of technologies from being held back. 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. However, according to the European as well as American approaches, some common standards for the IoT devices should be implemented on the legislative level.*

***Key words:*** *Internet of Things, personal data, cyber security, standardization, certification, European integration.*

**Некіт К. Г. Законодавчі підходи до вирішення питань безпеки у сфері Інтернету речей у світлі євроінтеграції України**

*У статті досліджуються особливості законодавчих підходів до правового регулювання відносин у сфері Інтернету речей, що склалися в Європейському Союзі та США. Зокрема, аналізуються підходи до визначення поняття Інтернету речей та його складових частин. На підставі проведеного аналізу зроблено висновок, що Інтернет речей визначається як своєрідна екосистема, що охоплює фізичні речі, оснащені пристроями, які мають змогу під'єднуватися до інтернету з метою взаємодії. Однак це поняття не поширюється на об'єкти, створені спеціально для виконання людиною роботи через підключення до Інтернету, такі як комп'ютери, ноутбуки, смартфони тощо. Окрема увага у статті приділяється проблемам безпеки і захисту персональних даних у сфері Інтернету речей. З метою визначення рекомендацій для українського законодавця у сфері забезпечення безпеки Інтернету речей аналізуються наявні європейські та американські законодавчі акти. Зокрема, проаналізовано підходи до забезпечення безпеки у сфері Інтернету речей на рівні GDPR, європейських та американських законодавчих актів щодо кібербезпеки. За результатами проведеного аналізу зроблено висновок щодо необхідності сертифікації та стандартизації пристроїв, що є елементами Інтернету речей. Однак стандартизацію у сфері Інтернету речей слід проводити обережно, з метою запобігання стриманню розвитку технологій. Враховуючи це, для забезпечення інформаційної безпеки у сфері Інтернету речей необхідно, насамперед, застосовувати саморегулювання, яке повинно забезпечуватися шляхом тісної співпраці між технологічними компаніями та громадянським суспільством. Це мінімізує втручання держави в цю сферу, що сприятиме швидкому розвитку інноваційних технологій. Однак, згідно з європейськими та американськими підходами, деякі загальні стандарти для пристроїв IoT повинні бути імплементовані на законодавчому рівні.*

***Ключові слова:*** *Інтернет речей, персональні дані, кібербезпека, стандартизація, сертифікація, європейська інтеграція.*

**Introduction.** 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 2025 the rollout of over 41 billion IoT devices is expected [1]. On the one hand, it opens up tremendous prospects for the development of society. With processing moving closer to the edge, communication and storage costs as well as energy consumption can be reduced. Machine learning and AI can be applied for safe identification of data patterns that impact physical processes or businesses. However, on the other hand, any other new phenomenon 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. Some attempts to solve legal issues in this field, mainly regarding data protection and security were made in the EU and USA. In the light of granting Ukraine the status of a candidate for accession to the European Union and the necessity to align Ukrainian legislation to the European standards, these solutions should be taken in consideration by Ukrainian legislator.

**The state of research on the topic.** Legal issues in the field of the Internet of Things are practically unexplored, since this phenomenon is completely new. Among the modern Ukrainian researchers who paid attention to the issues in the field of the Internet of Things, we can mention O. Baranov, M. Ozhevan, A. Biloshchytskyi, I. Doronin, E. Kharitonov, O. Kharitonova. However, there are very few papers in this area, therefore the issues of the Internet of Things require further in-depth research.

**The purpose of this study** is to briefly reveal the concept of the Internet of Things, to determine the range of issues arising in this area and pay special attention to the international approaches to solving legal issues in the field of the Internet of Things, mainly those, connected to data protection.

**Presenting main material.** The term 'Internet of Things' appeared in 1999, when Procter & Gamble employee Kevin Ashton offered to improve the corporation's logistics with the help of radio-frequency identification (RFID) tags [2]. However, today this term is criticized on the grounds that the Internet is, in fact, a proper name used to denote a global network of networks built on certain standards. While there is still the World Wide Web (WWW) – the most popular Internet platform that provides access to documents and technically does not contain obstacles to connect to this network of things-devices, that is, to create networks consisting of things using Internet technology. As critics point out, the interchange of concepts arose and strengthened due to a lack of proper understanding of the differences between the Internet and the WWW. The World Wide Web is a distributed system that provides access to interconnected documents located on different computers connected to the Internet. When talking about IoT, usually not just communications are meant, but something similar to the WWW, something like the web of things. This circumstance was realized only recently, and after that the corresponding term Web of Things (WoT) appeared, which more closely fits the idea of IoT [3].

However, the term 'Internet of Things' was already established by that time; it became widely used in 2008–2009, when the switchover from the 'Internet of People' to the 'Internet of Things' took place, because the number of objects connected to the Internet exceeded the population of the Earth. And the fact this term was already established terminologically, causes the need to implement it into the legal field.

One of the first international acts, which provided the definition of the Internet of Things, was Recommendation ITU-T Y.2060 (06/2012), according to which Internet of Things was defined as global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [4].

'Things' with regard to the Internet of things are defined as an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks [4].

The Recommendation also explains difference between 'things' and 'devices'. Thus, it shows relationship between devices and physical things and states that the main task of a devise is support of communication capabilities. Devices are categorized into data-carrying devices, data-capturing devices, sensing and actuating devices and general devices. A data-carrying device is attached to a physical thing to indirectly connect the physical thing with the communication networks. A data-capturing device refers to a reader/writer device with

the capability to interact with physical things. The interaction can happen indirectly via data-carrying devices, or directly via data carriers attached to the physical things. In the first case, the data-capturing device reads information on a data-carrying device and can optionally also write information given by the communication networks on the data-carrying device. A sensing and actuating device may detect or measure information related to the surrounding environment and convert it into digital electronic signals. It may also convert digital electronic signals from the information networks into operations. A general device has embedded processing and communication capabilities and may communicate with the communication networks via wired or wireless technologies. General devices include equipment and appliances for different IoT application domains, such as industrial machines, home electrical appliances and smart phones [4].

Thus, when talking about the Internet of Things, it is worth distinguishing between things as physical objects and devices, as various devices that give physical objects the ability to connect and consequently to be elements of the Internet of Things. Such devices are usually built-in elements and, obviously, should be considered as components of a thing within the meaning of Art. 187 of the Civil Code of Ukraine, that is, such elements are transferred to ownership as part of a thing without additional notice, since the separation of such elements from a 'smart' thing will turn it into an ordinary thing, which will lead to its significant depreciation.

In the European Commission staff working document 'Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe' Internet of Things is understood as an ecosystem where areas that have been developed as vertical silos (manufacturing, transport, healthcare, devices, etc.) relate to each other, thanks to common platforms and cross-cutting innovation [5].

In the USA have been enabled a new legislative act recently, IoT Cybersecurity Improvement Act of 2020, which defines Internet of Things as extension of internet connectivity into physical devices and everyday objects. It covers devices - often labeled as 'smart devices' - that have a network interface, function independently, and interact directly with the physical world. While the Act's definition of IoT devices expressly excludes conventional information technology devices (for example, computers, laptops, tablets, and smartphones), it extends to a variety of sensors, actuators, and processors used by the federal government [6].

Thus, by now on the legislative level in the EU and USA is clearly established, that Internet of Things covers devices, which interact through the Internet with help of sensors, actuators and so on, apart from things, designed directly to complete work with the access to the Internet, such as laptops, computers, smartphones etc.

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). The GDPR establishes a framework within the European Union and the UK, the right to be forgotten, clear and affirmative consent and, in particular, severe penalties for failure to comply with these rules. 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.

Regarding Internet of Things Art. 19 of the GDPR can be applied, according to which the controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16 (right to rectification), Article 17(right to erasure or 'right to be forgotten') and Article 18 (right to restriction of processing) to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it [7]. Thus, the GDPR provides for principles of data protection among which is to ensure that personal data is processed in accordance with the right to privacy of the data subject [8].

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 [9].

Apart from GDPR, in the field of the Internet of Things, the EU Cybersecurity Act (2019) and the NIS Directive (2018) are used to enable cybersecurity measures.

An important point of the EU Cybersecurity Act is that it defines an EU-wide cybersecurity certification framework. The European Cybersecurity Certification Framework should enable the issuance of cybersecurity certificates and statements of conformity for IoT products, services, and processes. Initially, manufacturers and vendors will be able to have their products and services meet the EU cybersecurity pending standards voluntarily. However, the certification may eventually be compulsory.

It is stated, that similar to GDPR, the Cybersecurity Act provides a model that other non-EU countries and territories are following when crafting legislation, so getting prepared now will be a competitive advantage for the future [10].

The Directive on security of network and information systems (the NIS Directive) [11], in turn, provides legal measures to boost the overall level of cybersecurity in the EU by ensuring: Member States' preparedness, by requiring them to be appropriately equipped; cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States; a culture of security across sectors that are vital for the economy and society and that rely heavily on information and communication technologies, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure [10].

In the USA the main act regarding security in the field of the Internet of Things is the IoT Cybersecurity Improvement Act of 2020. The Act has a few primary components for strengthening IoT cybersecurity and the government's critical technology infrastructure. First, the National Institute of Standards and Technology (NIST) was tasked with developing security standards and guidelines for the appropriate use and management of all IoT devices owned or controlled by the federal government and connected to its information systems. This includes establishing minimum information security requirements for managing cybersecurity risks associated with these devices. In formulating these guidelines, NIST had to consider its current efforts regarding the security of IoT devices, as well as the 'relevant standards, guidelines, and best practices developed by the private sector, agencies, and public-private partnerships' [6].

Thus, both, European and American legislators pointed out the necessity to standardize items, which can be elements of the Internet of Things. The discussion on standardization in the field of the Internet of Things has lasted for several years. Specialists in the field of IoT have actively discussed the need to coordinate the coexistence of various devices by introducing open certification of IoT products [12]. According to researchers, the introduction of certain standards in the field of the Internet of Things would also help to solve the problem of coordinating the coexistence of various components of the Internet of Things. Thus, it was noted that the proprietary and closed systems of the Internet of Things must give way to a more open space. A situation where there are many different non-standardized devices is similar to a situation where, for example, each car manufacturer would use its own control system, one car would have a steering wheel, and another would have a joystick or control panel. Or if e-mail systems were incompatible, and the telephone could not be used to call numbers of other operators, and different brands of household appliances required different types of water or electricity connections. Likewise, in a closed or proprietary Internet of Things world where devices are not connected to each other, a homeowner will not be able to control lights, security, thermostat, locks, etc. from a central app or control panel. The need for standards for the Internet of Things was recognized several years ago. At that point, the Association for Standardization has developed a number of standards and protocols designed to help the development of connected systems [13]. Nowadays, these considerations were taken into account on the legislative level.

However, there's no national IoT cybersecurity regulatory framework nor a comprehensive set of standards in the US. At the same time, California was very progressive in this field. California legislature passed a new IoT security law in 2018 that became effective on 1 January 2020. This became the first IoT-specific security law in the USA. The law defines new security requirements for IoT devices connected directly or indirectly to the Internet with an IP or Bluetooth address. It requires that these devices sold in California be fitted with 'reasonable security features.' The security features should protect both the IoT device and the data it contains,

in particular, if the device integrates a password, it must either be uniquely linked to that device or require the user to set their own password during the initial setup [10].

Such a law in California was very likely conditioned by the case of D-Link. Thus, on January 9, 2017, the US Federal Trade Commission filed a lawsuit against the Taiwanese company D-Link for failing to ensure the security of its products, leaving them vulnerable to hacker attacks. According to the lawsuit, D-Link failed to implement the necessary security mechanisms in routers and video cameras that connect to the Internet, thereby putting the safety of thousands of consumers at risk. The reason for the lawsuit was the use of unprotected IoT devices by cybercriminals to create botnets that were used for powerful DDoS attacks. These include, in particular, the Mirai botnet, which consists of routers, webcams and video recorders with untrusted factory passwords, which was used to launch the most powerful DDoS attacks in history. At the same time, D-Link used advertising to mislead users about the security of its products, claiming that all security measures against known threats, including immutable passwords, were taken. Thus, as a result of the manufacturer not taking care of the security of its software, its products allowed hackers to monitor the location of users in order to commit theft or other crimes [14].

**Conclusions.** For the purpose of proper legal regulation of relations in the field of the Internet of Things, it is necessary, first of all, to define the concept and structure of the Internet of Things at the legislative level, since various components of the Internet of Things require their own legal regulation (separately for physical objects, software, access to Network, hosting services, etc.). When implementing the definition of the Internet of Things to Ukrainian legislation, the European and American approaches should be taken into account. The concept of the Internet of Things covers devices, which interact through the Internet with help of sensors, actuators and so on, apart from things, designed directly to complete work with the access to the Internet, such as laptops, computers, smartphones etc.

Among legal issues which arise in the field of the Internet of Things the most important is data protection and security. With this regards such legislative acts from the EU and USA might be guides for Ukrainian legislator: GDPR, the EU Cybersecurity Act and the NIS Directive (European level) as well as IoT Cybersecurity Improvement Act of 2020 (USA) and California IoT cybersecurity law. According to the last ones, the necessity of certification and standardization for the appropriate use and management of all IoT devices was recognized.

However, 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. However, according to the European as well as American approaches, some common standards for the IoT devices should be implemented on the legislative level.

**Acknowledgement:** the research was conducted at the Center of SME research and entrepreneurship of the University of Mannheim with support of the Volkswagen foundation.

**References**

1. European commission. Europe's Internet of Things Policy. URL: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy.

2. Интернет вещей. Безграничные возможности взаимодействия человека и машины. Медиасектор и индустрия развлечений. URL: https://docplayer.com/80646555-Internet-veshchey-bezgranichnye-vozmozhnosti-vzaimodeystviya-cheloveka-i-mashiny-mediasektor-i-industriya-razvlecheniy.html.

3. Что такое Интернет вещей. *TAdviser.* URL: https://cutt.ly/ZWmU4zl.

4. International Communication Union. Recommendation Y.2060 'Overview of the Internet of Things'. URL: http://handle.itu.int/11.1002/1000/11559.

5. European Commission staff working document 'Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe'. *European Commission*. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137.

6. Dunn G. New Federal Law for IoT Cybersecurity Requires the Development of Standards and Guidelines Throughout 2021. URL: https://www.gibsondunn.com/new-federal-law-for-iot-cybersecurity-requires-

the-development-of-standards-and-guidelines-throughout-2021/#_ftn1.

7. Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection on natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 45/46/EC (General Data Protection Regulation). *European Parliament and Council of Europe*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

8. Kariuki Mulika C. Privacy Regulation On The Internet Of Things (IoT). URL: https://tripleoklaw.com/privacy-regulation-on-the-internet-of-things-iot/.

9. Nekit K., Kolodin D., Fedorov V. Personal data protection and liability for damage in the field of the Internet of Things. *Juridical Tribune*. 2020. Vol. 10. Issue 1. P. 80–93.

10. IoT Cybersecurity: regulating the Internet of Things. URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations.

11. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *European Parliament and Council of Europe*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

12. Виндерских Н. Опасность интернета вещей: зачем IoT рынку сертификация. *ain.ua*. URL: https://ain.ua/2017/09/01/opasnost-interneta-veshhej.

13. Некіт К.Г. Деякі правові проблеми Інтернету речей і напрями їх вирішення. *Часопис цивілістики*. 2018. № 31. С. 54–58.

14. Некіт К.Г. Проблеми забезпечення інформаційної безпеки та відшкодування шкоди, заподіяної пристроями, підключеними до Інтернету речей. *Часопис цивілістики*. 2017. № 27. С. 107–112.

***Nekit K. H.,***
*Doctor of Law, Associate Professor,*
*Professor of Civil Law Department*
*National University "Odesa Law Academy",*
*Guest Researcher at the Center*
*of SME Research and Entrepreneurship*
*of the University of Mannheim (Germany)*
*ORCID: 0000-0002-3540-350X*