Personal data protection and liability for damage in the field of the internet of things

PhD. **Kateryna NEKIT**[1]
PhD. **Denis KOLODIN**[2]
PhD. **Valentyn FEDOROV**[3]

Abstract

This article analyzes the concept and legal issues of the Internet of Things to explore whether the existing legal framework is appropriate to deal with this new phenomenon. It examines the system of legal issues in the field of the Internet of Things and the ways of their solution. The attention is paid to the personal data protection issue. The conclusion is made about the necessity to ensure the realization of GDPR provisions concerning privacy outside the European Union, which is possible by the conclusion of international agreements with non-EU countries. The article also considers how it is possible to deal with damage caused by the Internet of Things. This takes into account conditions of compensation of damage caused by IoT devices. The necessity of self-regulation in the field of the Internet of Things for ensuring information security and preventing damage caused by the Internet of Things is emphasized. This would be possible in case of close cooperation between technology companies and civil society. Such an approach would minimize government intervention in this area, which would contribute to the rapid development of innovative technologies.

Keywords: *Internet of Things, GDPR, personal data protection, information security, privacy, compensation of damage*.

JEL Classification: K15, K22, K24

1. Introduction

The impact of technology on human life and the development of society is difficult to overestimate. 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[4]. On the one hand, it opens up tremendous

[1] Kateryna Nekit - National University "Odessa Law Academy", Ukraine, katerinanekit@gmail.com.
[2] Denis Kolodin - National University "Odesa Law Academy", Ukraine, kolodinodessa@gmail.com.
[3] Valentyn Fedorov - National University "Odesa Law Academy", Ukraine, pom.president@gmail.com.
[4] Храмцов П., *Всеобъемлющий интернет: прогнозы и реальность.* "Открытые системы", 4, 2013 [Hramtsov P., *Comprehensive Internet: forecasts and reality.* "Open Systems", 4, 2013]. [online], available at: http://www.osp.ru/os/2013/04/13035552/ [Accessed 28 Aug. 2019].

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.

Relations connected to the functioning of the Internet of Things are regulated by various branches of law, depending on the sphere where they arise and the grounds for their occurrence. Therefore, the Internet of Things can be called a complex phenomenon, completely new, and therefore causing a large number of questions. In particular, issues of confidentiality of information, protection of personal data, compensation for harm caused by the functioning of the Internet of Things, the use of evidence obtained through the Internet of things, and many others are becoming acute.

This article aims to explore the concept, elements of the Internet of Things and some issues that arise because of the development of the Internet of Things. Special attention is paid to the problem of compensation for damage caused by the Internet of Things.

The present article uses general and special scientific research methods. Legal nature of the Internet of Things was considered on the basis of scientific literature analysis. As material for study were used social relations arose in the sphere of the Internet of Things. Methodological basis for study was a dialectical method that allowed reviewing the issues in their development and interconnection.

2. The concept and elements of the internet of things

Despite the popularity of the Internet of Things (IoT), it still has no single definition. There are many technical definitions of the concept of the Internet of Things. In particular, the Internet of things is defined as the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment[5]. According to another definition, the Internet of Things is "things", such as devices and sensors other than computers, smartphones or tablets that combine, interact or transmit information from each other through the Internet[6].

Noteworthy is the definition according to which the Internet of Things is the concept of a communication network of physical or virtual objects ("things") that have technologies for interaction between themselves and the environment,

[5] Gartner IT Glossary, *Internet of Things*, 2019 [online], available at: https://www.gartner.com/it-glossary/internet-of-things/ [Accessed 28 Aug. 2019].

[6] Открытая концепция *"Интернет вещей: правовые аспекты (Российская Федерация)"*, [Open concept *"Internet of Things: legal aspects (Russian Federation)"*], 2016, [online] Available at: http://www.dentons.com/ru/whats-different-about-dentons/ connecting-you-to-talented-lawyers-around-the-globe/news/2016/june/dentons-develops-russias-first-ever-whitepaper-on-the-legal-aspects-of-the-internet-of-things [Accessed 28 Aug. 2019].

and can also perform certain actions without human intervention. The essence of this concept is that all household items, goods, process units, etc., should be equipped with embedded computers and sensors, can process information from the environment, exchange it and perform various actions depending on the received information[7].

According to Recommendation ITU-TY.2060 of the International Telecommunication Union "Overview of the Internet of Things", the Internet of Things is a 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. With regard to the Internet of Things, "thing" is 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[8].

Legal aspects of the Internet of things are reflected in the definition proposed by A. Baranov, according to which the Internet of Things includes complexes and systems consisting of sensors, microprocessors, actuators, local and/or distributed computing resources and software, artificial intelligence programs, cloud computing technologies, between which data transfer is carried out using the Internet, and which are intended to provide services for individuals and legal entities[9].

This definition seems to be quite acceptable for understanding the concept of the Internet of Things in its legal meaning, except with the clarification that the Internet of Things should be defined as the above mentioned set of components that are used to satisfy the interests of individuals, legal entities or the interests of the state and society (taking into account the fact that the Internet of Things is a multifaceted concept and can be used in various fields, with different purposes, therefore, various legal relations with different participants may arise here).

The main components of the Internet of Things include:

- physical objects equipped with sensors and mechanisms for receiving and processing signals;
- Internet access: communication standards and protocols for connecting sensors to a single network;
- Network (connection): Internet access (wireless/wired access, Wi-Fi, Bluetooth, ZigBee, VPN, 2G/3G/4G/5G);
- cloud servers: corporate and cloud computing systems/platforms

---

[7] Інтернет речей [Internet of Things], 2016, [online] Available at: http://glossary.starbasic.net /index.php?title=%D0%86%D0%BD% D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82 _%D1%80%D0%B5%D1%87%D0%B5%D0%B9 [Accessed 28 Aug. 2019].

[8] Recommendation ITU-T Y.2060: *Overview of the Internet of things*, 2012, [online], available at: https://www.itu.int/rec/T-REC-Y.2060-201206-I [Accessed 8 Sep. 2019].

[9] Баранов О.А., *Інтернет речей (IoT): огляд правових проблем*. "Інтернет речей: проблеми правового регулювання і впровадження". Київ: «Політехніка», 2017, с. 7. [Baranov O.A. *Internet of Things (IoT): legal review*. "Internet of Things: problems of legal regulation and implementation". Kyiv: "Politehnica", 2017, p. 7].

capable of processing data and performing other analytical operations in real time, storage and delivery of content, application hosting;
- Applications and user interaction: the interaction of people, applications and business processes.

Because of such complicated structure, the Internet of Things sometimes is called an ecosystem built on technological connections[10].

3. Scopes of the internet of things

The scope of the Internet of Things is quite diverse. In particular, the Internet of Things is used in the following areas:

1) Housing. The 'smart house' technology combines the technology of the Internet of Things and 'Network of things'. In other words, various technological devices are interconnected into a local system for the purpose of coordinated functioning (NoT technology – 'Net of Things', 'Network of things'), as well as the corresponding devices have access to the Internet (IoT technology).

For example, meters for water, electricity, gas in such a system independently transmit data to the suppliers of these resources, which significantly reduces the cost of home maintenance and improves the quality of relevant services.

Among other 'smart' things from a 'smart house' that may already have access to the Internet, there are various security systems, ranging from a door lock and ending with alarms, lighting and heating systems, sockets, taps and even mirrors.

Of course, for proper legal regulation of relations arising from such things, it is necessary to take into account their specificity. In this case, things cease to be just objects of the material world completely controlled by the owner. There is a risk of intrusion into the sphere of interests of the owner via the Internet. Accordingly, relations regarding such things require close attention of lawmakers.

2) Medicine. A variety of trackers allow you to monitor the patient's condition around the clock. In case of any deviations from the norm, there is a real opportunity to immediately help a person or adjust the treatment process.

In the field of medicine, there are already a wide variety of devices to facilitate operations, improve treatment processes, rehabilitation and so on. Such technologies, on the one hand, significantly help patients, on the other hand, there are many issues related to the differentiation of the responsibility of doctors from the responsibility of engineers and programmers who create such equipment.

3) Sport. In this area the Internet of Things is used, in particular, to analyze the physical condition of athletes. Sensors are installed on the participants of the competition to analyze their pulse, movement data so on. Medical telemetry and

[10] Staying Ahead of Privacy and Security Risks in Internet of Things, 2017, [online], available at: https://www.natlawreview.com/ article/staying-ahead-privacy-and-security-risks-internet-things [Accessed 10 Sep. 2019].

other indicators are sent to the cloud, from which the coaching team receives all the information about the condition of the athletes, without waiting for a break in the competition, and according to the received data makes changes to the game. All the necessary information also comes online to medical professionals. Thanks to this, they can provide timely assistance to an athlete who is injured or overworked.[11]

In this area, new unresolved legal issues also arise, for example, the possibility of remote exposure of an athlete's body to improve its performance, preventing the abuse of distance doping, etc.

4) Industry. In this area the Internet of things is used most actively. One such example is the remote control of industrial machines.

In particular, the South Korean construction company Doosan recently showed the possibility of using 5G technology for remote control of construction equipment at a construction exhibition. From a control panel located at the company's booth at an exhibition in Munich, a company representative led the work of a 40-ton tracked excavator, located at a distance of 8500 km, in South Korea. The control panel in Munich was equipped with a 3D machine flood system, real-time diagnostics, and full-format display systems[12].

As scholars rightly point out, IoT-related products and services will be offered in just about every sector of the economy, from agriculture to energy and utilities, industrial manufacturing, transportation, consumer electronics, retail, finance and insurance or the public sector.[13]

In this situation, many legal issues also arise, for example, the problem of compensation for damage caused by such mechanisms.

5) Entertainment. In this area the Internet of things is developing very intensively. The technologies VR (virtual reality) and AR (augmented reality) are becoming increasingly popular. Google glasses, invented several years ago, can not only entertain the user with objects of virtual or augmented reality, but also display any information that is useful to the user on the Internet.

Again, there is a need to supplement the legal rules on the regulation of games and the sphere of entertainment, taking into account the development of new technologies.

---

[11] Горпин В., *Интернет вещей (в примерах) – что это такое и как он работает* [Gorpin V., *Internet of Things (on examples) – what is this and how does it work*], 2017, [online], available at: https://finfocus.today/internet-veshhej.html. [Accessed 10 Sep. 2019].

[12] Digger Blogger, *Doosan aspires to tech leadership*, 2019, [online], available at: https://www.theconstructionindex.co.uk/the-digger-blog/view/doosan-aspires-to-techno-leadership [Accessed 8 Sep. 2019].

[13] Gallego B.C., Drexl J., *IoT Connectivity Standards: How Adaptive is the Current SEP Regulatory Framework?* "IIC - International Review of Intellectual Property and Competition Law", 50 (1), 2019, pp. 135-156.

4. The system of legal issues in the field of the internet of things and ways of their solution

The variety of components the Internet of Things consists of, as well as the variety of areas of its application create a significant number of legal issues related to the Internet of things. In particular, these are issues of the legal regime of information, the protection of personal data and privacy, information security, the development of a conceptual framework, the problem of identifying persons responsible for violations in the field of the Internet of Things, the problem of collecting evidence etc.

The list of these problems is not exhaustive today, but attempts are being made in the world to determine exactly what problems may arise in connection with the spread of the phenomenon of the Internet of Things and to settle relations that appear in this area.

Thus, in 2014 the European Commission published a position on this issue after examining in detail wearable devices and devices of the 'smart house' system. Among the recommendations made by the Commission is the requirement to provide users full control over their data. These recommendations also indicate measures that organizations have to take to ensure compliance with European Union data protection legislation. In early 2015 a US Congress faction was formed

on issues of the Internet of Things. The goal of the faction was to increase the awareness of members of the Congress about the opportunities and challenges connected to IoT solutions as well as find a balance between the data collection and the protection of personal data of consumers.

Around the same time, the Federal Trade Commission published a report containing recommendations on minimizing data and developing self-regulatory programs to increase privacy and security[14]. In particular, the report of the Federal Trade Commission contains three key recommendations for companies developing IoT devices. The first one is data security, that is, IoT companies should design devices in such a way that they have integrated security. Secondly, there should be consent to data processing, that is, IoT companies should give users the opportunity to choose what information they disseminate and immediately report data protection violations. The third recommendation is data minimization, that is, IoT companies should not collect more data than they need[15].

Later, in 2016, the international law firm Dentons, together with the Non-Profit Partnership RUSSOFT, developed an open concept of legal regulation of the Internet of Things. The main goal of creating the concept is the formation of legal terminology and of a common vision of the issues in the field of legal regulation of

---

[14] Интернет вещей. Безграничные возможности взаимодействия человека и машины, [Internet of Things. Boundless possibilities of the human-machine interaction], 2016, [online], available at: http://docplayer.ru/80646555-Internet-veshchey-bezgranichnye-vozmozhnosti-vzaimodeystviya-cheloveka-i-mashiny-mediasektor-i-industriya-razvlecheniy.html [Accessed 10 Sep. 2019].

[15] The 'Internet of Things': Legal Challenges in an Ultra-connected World, 2016, [online], available at: https://www.mhc.ie/latest/ blog/the-internet-of-things-legal-challenges-in-an-ultra-connected-world [Accessed 10 Sep. 2019].

the Internet of Things. The concept poses a question about possible general principles of regulation of the Internet of Things, among which there are principles of user awareness and free participation in the Internet of Things. There are also indicated main issues that arise in the field of the Internet of Things, among which the issues of user identification, protection of personal data, determination of jurisdiction, responsibility of information intermediaries etc[16].

There are already some precedents for solving problems arising in the field of the Internet of Things, although many more questions remain unanswered. In particular, questions about liability for malfunction of connected devices and accidents caused by this, responsibility for loss of information, problems of consumers rights protection. Another important question that needs to be answered is the question of who owns the information: the sensor manufacturing company, the device manufacturing company or the person whose data is being measured and collected[17]. Representatives of the EU legislative bodies emphasize that the rights to personal data belong to citizens, but this is not always the case. Even in cases where the right to information is not in doubt, the question of the duration of the rights to the collected data remains open[18].

5. Personal data protection in the field of the internet of things

It is widely known, that data today is one of the most valuable assets[19]. That is why it is so important to insure protection of personal data in every sphere. 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]. It includes new notification rules around personal data breaches i.e. “a breach of security leading to the accidental or unlawful destruction, loss, alteration,unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” [art. 4(12)][20].

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

---

[16] *Supra* note 6.

[17] Nekit K., Ulianova H., Kolodin D., *Web-site as an object of legal protection by Ukrainian legislation.* “Amazonia investiga”, 21(8), 2019, pp. 222-230.

[18] *Supra* note 14.

[19] Farkas T.J., *Data created by the Internet of Things: the new gold without ownership?* “Revista la Propiedad Inmaterial”, 23, 2017, pp. 5-17; Baldwin H., *Drilling into the value of data*. “Forbes”, 2015, [online], available at: https://www.forbes.com/sites/howard baldwin/2015/03/23/drilling-into-the-value-of-data/#77ee6cc965fa [Accessed 10 Sep. 2019].

[20] Urquhart L., McAuley D., *Avoiding the Internet of Insecure Industrial Things.* “Computer law & security review”, 34, 2018, pp. 450-466.

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[21].

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

[21] European Union, *'Regulation 2016/679 General Data Protection Regulation'*, 2016, 59 OJ 4.

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[22].

The above mentioned provisions on the personal data protection should be taken into consideration by all countries outside the EU as well. This is necessary both to ensure the protection of personal data of 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[23].

We should mention that one of the drawbacks of the GDPR is the lack of any agreements with countries outside the European Union on the procedure for protecting the rights of EU citizens in case of violation in a country that is not a member of the EU. To date, the only way to protect will be to appeal to the court at the location of the defendant. For EU citizens, this situation greatly complicates the realization of their rights.

Thus, today the important issue is development of a regulatory framework for regulating standards for the collection and dissemination of information obtained while using the Internet of Things. Some countries are already working in this direction. In particular, the United States is actively discussing draft amendments to the US Digital Millennium Copyright Act (DMCA) of 1998, which will regulate some aspects of the protection of confidential data[24].

6. Liability for damage caused by the internet of things

This question is rather complicated, since the Internet of Things consists of various components. The rights to these components may belong to different entities. This raises the issue of how to identify the person responsible for the

[22] Кавукиан А., *Privacy by Design: 7 основополагающих принципов* [Cavoukian A., *Privacy by design: 7 basic principles*], 2011, [online], available at: https://online.zakon.kz/Document /?doc_id=31633216#pos=0;0 [Accessed 10 Sep. 2019].

[23] Nekit K.G., *The implementation of information security and personal data protection in the field of the Internet of things.* "ECHR`s Jurisprudence in Digital Era". Odessa: Helvetica, 2019, pp. 245-248.

[24] Mishchenko L., *The Internet of Things: Where Privacy and Copyright Collide*. "Santa Clara High Technology Law Journal", 33, 2016, pp. 90-115.

damage. This question cannot be left unresolved, since the number of cases of cybercrime using the Internet of Things is constantly growing.

Objects that are elements of the Internet of Things are much less protected from hacking than computers, and therefore are often used by hackers to commit offenses. Thus, in June 2016, the so-called botnet (zombie network) was discovered, which consisted of more than 25,000 city and private cameras and was used by hackers to carry out DDoS attacks[25]. This situation becomes possible since more than 70% of devices included in the Internet of Things have vulnerabilities, and 60% of them have a dangerous web interface. However, most of them have access to personal data of their owners, such as address, e-mail, and even a bank account. Often this is because manufacturers, trying to reduce their costs, tend to save on security. For example, suppliers of cheap cameras almost ignore the security issues in their products, since, according to their estimates, low cost is much more important than security for most camera users[26].

Another example of an unfair approach by manufacturers to protection of devices connected to the Internet can be the situation with hacking the Samsung refrigerator, from which security specialists were able to obtain data from a Gmail account. This became possible because the manufacturer did not take care of the correct verification of the SSL certificate when establishing a secure connection to the Google server. Despite the fact that SSL support was implemented in the refrigerator, de facto certificate verification was not carried out, which made it possible to conduct a MiTM attack. Given that the device was connected to the network via Wi-Fi, such an attack could be carried out from outside the apartment, for example, from the street[27].

Today, there are already cases of filing lawsuits in court due to the failure to ensure the proper security of devices included in the Internet of Things. Thus, on January 9, 2017, the U.S. Federal Trade Commission filed a lawsuit against the Taiwanese company D-Link for the fact that the manufacturer did not ensure the safety of its products, leaving them vulnerable to hacker attacks. According to the lawsuit, D-Link did not implement the necessary protection mechanisms in routers and camcorders connected to the Internet, and this jeopardized the security of thousands of consumers. The reason for going to court was the use by cybercriminals of unprotected IoT devices 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 unreliable factory passwords, with the help of which the most powerful DDoS attacks in history have been carried out. At the same time, D-Link, through advertising, misled users about

---

[25] Упитт О., *Опасные предметы: кто и зачем взламывает Интернет вещей и как с этим быть*. [Upitt O., *Dangerous items: who and why breaks into the Internet of Things and how to deal with it*], 2017, [online] Available at: https://apparat.cc/world/internet-of-things/ [Accessed 10 Sep. 2019].

[26] *Ibid*

[27] Ализар А., *Умный холодильник выдал хакерам пароль от Gmail* [Alizar A., *Smart refrigerator gives Gmail password to hackers*], 2015, [online], available at: https://xakep.ru/2015/08/25/smart-fridge/. [Accessed 10 Sep. 2019].

the security of its products, claiming that all security measures were taken against all known threats, including unchangeable passwords. Therefore, due to the fact that the manufacturer did not take care of the security of its software, its products allowed hackers to monitor the location of users in order to commit thefts or other crimes[28].

To prevent such situations, cybersecurity researchers emphasize the need for the professional community to take responsibility on this issue, including putting pressure on consumers. Instruments of such pressure could be state regulatory bodies and consumer protection societies. Responding to these kinds of initiatives, the US Federal Trade Commission has initiated over fifty cases involving companies that do not provide sufficient security for the networks, products, and services they use. They also conducted a series of Start With Security seminars on the need to include the development of privacy practices and safe use in the early stages of product development[29].

In addition to regulatory actions in this area, the possibility of self-regulation is also discussed. That would contribute to the development of the Internet of Things without inhibiting innovative technologies. Such an alternative is possible by introducing a certification system, as in the National Transportation Safety Administration in the United States. The need for certification of IoT gadgets is noted by experts in the field of the Internet of Things, in particular, this was stated by a specialist in software development, chairman of the San Francisco Internet Society IoT Working Group. He noted that if we imagine all IoT devices as moving along one road, today each of the manufacturers believes that it is the only one who moves along this path. While in fact there is the only road with many cars, and they all move along this road, sharing resources - an external IP address, Wi-Fi, radio frequencies, and sooner or later these cars will start to collide, clash with each other. Therefore, it is necessary to coordinate their coexistence by introducing open certification of IoT products. Certification will help ensure that a device is not obviously accessible to any hacker[30].

The most important IoT security issues were discussed at the RightsCon event, in particular: data security, separation of security and functionality updates, security updates for the reasonable life of this product and wider digital security - using encryption and information security to ensure confidentiality and the integrity of the devices, services, and data they create. It was emphasized that in spite of the fact that the authorities can implement some means of protecting

---

[28] Федеральная торговая комиссия США подала в суд на D-Link [US Federal Trade Commission sues D-Link], 2017, [online] Available at: http://www.securitylab.ru/news/484958.php [Accessed 10 Sep. 2019].

[29] *Supra* note 25.

[30] Виндерских Н., *Опасность Интернета вещей: зачем IoT рынку сертификация*. [Vinderskih N., *The danger of the Internet of Things: why IoT market needs certification*], 2017, [online] Available at: https://ain.ua/2017/09/01/opasnost-interneta-veshhej [Accessed 10 Sep. 2019]; Spiegelmock M., *IoT Security Through Open Certification*, 2017, [online], available at: http://www.sfbayi soc.org/2017/06/21/iot-security-through-open-certification/ [Accessed 10 Sep. 2019].

human rights, companies should also activate and introduce means of protection at the level of software and/or hardware and, of course, users themselves should be able to build their protection. This requires sustained collaboration between civil society, consumer advocacy groups and technology companies[31].

7. Conclusions

There is an urgent need to ensure the protection of rights from violations in the field of the Internet of things. In particular, it is necessary to establish control over the use of consumers' personal data and create a clear mechanism for compensation of damage caused by elements of the Internet of Things. However, in the process of ensuring the protection of rights from violations, there is need to prevent unnecessary interference by the state in regulation of the Internet of Things, since this will inhibit the development of technologies. There are already some regulatory barriers threatening IoT technologies in Europe. In order to ensure security, it is planned at the state level to introduce mandatory certification of all devices connected to the Internet. EU member states are considering developing a set of measures aimed at ensuring the cybersecurity of the Internet of Things. There is an intension to control not only devices connected to the Internet, which can be protected by chips to repel hacker attacks, but also the networks to which they are connected, as well as cloud storage[32]. Such an approach will indeed contribute to the protection of consumer rights, but can negatively affect the development of the Internet of Things. Besides, it would be quite difficult to ensure control over cloud storage. Services using IoT sensor data often store collected data in servers located outside of the EU. From the perspective of ensuring GDPR compliance, users will struggle to know where their data is, or how they can access and control it when its storage location is likely unknown or geographically distant[33].

Self-regulation seems to be more appropriate for ensuring information security in the field of the Internet of Things and preventing damage caused by the Internet of Things. This would be possible in case of close cooperation between technology companies and civil society. Such an approach would minimize government intervention in this area, which would contribute to the rapid development of innovative technologies.

Thus, there is a need for legal regulation of relations between civil society, consumer protection organizations and technology companies. First of all, efforts should be aimed at protecting human rights from violations related to the functioning of the Internet of Things. Such violations can be prevent by monitoring

---

[31] Как защитить права человека в пространстве Интернета вещей [How to protect human rights in the field of the Internet of things], 2017, [online], available at: https://rublacklist.net/28562/ [Accessed 10 Sep. 2019].

[32] Lucie Krahulcova, *What the EU is getting wrong about the Internet of Things*, 2018, [online], available at: https://www.access now.org/what-the-eu-is-getting-wrong-about-the-internet-of-things/ [Accessed 10 Sep. 2019]

[33] Urquhart L., Lodge T., Crabtree A., *Demonstrably doing accountability in the Internet of Things*. "International Journal of Law and Information Technology", 27, 2019, pp. 1-27.

on the part of civil society and consumer protection organizations over the installation of appropriate security software on all devices included in the Internet of Things.

Talking about the compensation of damage caused by the Internet of things, it should be taken into account the specifics of the conditions for compensation of such damage. These conditions should include: 1) the existence of damage; 2) the wrongful behavior of an injurer (which will be the manufacturer of the device), expressed in the failure to take measures to ensure the safety of the device; 3) a causal link between the wrongful behavior of an injurer and the harm; 4) the fault of the injurer.

It should also be noted that when determining the amount of damage caused by the Internet of Things, it is necessary to take into account the guilt of the consumer for not using personal safety equipment if the manufacturer has warned about the need of such measures. Besides, it seems appropriate to impose on consumers the obligation to apply all possible security measures, since the rule on the need to take into account the public interest when using property comes into force here. Since property (devices connected to the Internet) in this case can be used by hackers to commit crimes, which poses a threat to the interests of the state and society, it is permissible to impose on owners the obligation to take all possible actions aimed at ensuring the protection of the device from outside interference (hacker attacks).

Bibliography

1. Храмцов П., *Всеобъемлющий интернет: прогнозы и реальность.* ”Открытые системы”, 4, 2013 [Hramtsov P., *Comprehensive Internet: forecasts and reality*, ”Open Systems”, 4, 2013]. [online], available at: http://www.osp.ru/os/ 2013/04/13035552/ [Accessed 28 Aug. 2019].
2. Gartner IT Glossary, *Internet of Things*, 2019, [online], available at: https://www.gartner.com/it-glossary/internet-of-things/ [Accessed 28 Aug. 2019].
3. Баранов О.А., *Інтернет речей (IoT): огляд правових проблем*. “Інтернет речей: проблеми правового регулювання і впровадження”. Київ: «Політехніка», 2017 [Baranov O.A. *Internet of Things (IoT): legal review*. “Internet of Things: problems of legal regulation and implementation”. Kyiv: “Politehnica”, 2017].
4. Горпин В., *Интернет вещей (в примерах) – что это такое и как он работает* [Gorpin V., *Internet of Things (on examples) – what is this and how does it work*], 2017, [online], available at: https://finfocus.today/ internet-veshhej.html. [Accessed 10 Sep. 2019].
5. Digger Blogger, *Doosan aspires to tech leadership*, 2019, [online], available at: https://www.theconstruction index.co.uk/the-digger-blog/view/doosan-aspires-to-techno-leadership [Accessed 8 Sep. 2019].
6. Gallego B.C., Drexl J., *IoT Connectivity Standards: How Adaptive is the Current SEP Regulatory Framework?* ”IIC - International Review of Intellectual Property and Competition Law”, 50 (1), 2019, pp 135–156.
7. Nekit K., Ulianova H., Kolodin D., *Web-site as an object of legal protection by Ukrainian legislation.* “Amazonia investiga”, 21(8), 2019, pp. 222-230.

8. Farkas T.J., *Data created by the Internet of Things: the new gold without ownership?* "Revista la Propiedad Inmaterial", 23, 2017, pp. 5-17.
9. Baldwin H., *Drilling into the value of data*. "Forbes", 2015, [online], available at: https://www.forbes.com/ sites/howardbaldwin/2015/03/23/drilling-into-the-value-of-data/#77ee6cc965fa [Accessed 10 Sep. 2019].
10. Urquhart L., McAuley D., *Avoiding the Internet of Insecure Industrial Things.* "Computer law & security review", 34, 2018, pp. 450-466.
11. Кавукиан А., *Privacy by Design: 7 основополагающих принципов*. [Cavoukian A., *Privacy by design: 7 basic principles*], 2011, [online] available at: https://online. zakon.kz/Document/?doc_id=31633216#pos=0;0 [Accessed 10 Sep. 2019].
12. Nekit K.G., *The implementation of information security and personal data protection in the field of the Internet of things*. "ECHR`s Jurisprudence in Digital Era", Odessa: Helvetica, 2019, pp. 245-248.
13. Mishchenko L., *The Internet of Things: Where Privacy and Copyright Collide*, "Santa Clara High Technology Law Journal", 33, 2016, pp. 90-115.
14. Упитт О., *Опасные предметы: кто и зачем взламывает Интернет вещей и как с этим быть* [Upitt O., Dangerous items: who and why breaks into the Internet of Things and how to deal with it], 2017, [online], available at: https://apparat.cc/world/internet-of-things/ [Accessed 10 Sep. 2019].
15. Ализар А., *Умный холодильник выдал хакерам пароль от Gmail*. [Alizar A., *Smart refrigerator gives Gmail password to hackers*], 2015 [online], available at: https://xakep.ru/2015/08/25/smart-fridge/ [Accessed 10 Sep. 2019].
16. Федеральная торговая комиссия США подала в суд на D-Link [US Federal Trade Commission sues D-Link], 2017, [online], available at: http://www.securitylab. ru/news/484958.php [Accessed 10 Sep. 2019].
17. Виндерских Н., *Опасность Интернета вещей: зачем IoT рынку сертификация*. [Vinderskih N., *The danger of the Internet of Things: why IoT market needs certification*], 2017 [online], available at: https://ain.ua/ 2017/09/01/opasnost-interneta-veshhej [Accessed 10 Sep. 2019].
18. Spiegelmock M., *IoT Security Through Open Certification*, 2017, [online], available at: http://www.sfbayisoc .org/2017/06/21/iot-security-through-open-certification/ [Accessed 10 Sep. 2019].
19. Lucie Krahulcova, *What the EU is getting wrong about the Internet of Things*, 2018, [online], available at: https://www.accessnow.org/what-the-eu-is-getting-wrong-about-the-internet-of-things/ [Accessed 10 Sep. 2019].
20. Urquhart L., Lodge T., Crabtree A., *Demonstrably doing accountability in the Internet of Things*, "International Journal of Law and Information Technology", 27, 2019,
pp. 1-27.