The Value and Use of the Internet of Things During the Pre-trial Investigation of Criminal Offenses

Oleksandr Zaiets [1 * [0000-0002-4426-5241]], Serge Yeskov [2],
Yuri Kononenko [1 [0000-0001-6908-9881]]

[1] *Odesa State University of Internal Affairs, Odesa, Ukraine*
[2] *Centre for European Reforms Studies, a.s.b.l. Grand Duchy of Luxembourg*
* *zaec_1985@meta.ua*

ABSTRACT

This article introduces the active dissemination and development of new social relations related to the Internet of Things. The concept of the Internet of Things (IoT) is seen as a growing network of facilities, from industrial devices to consumer goods and services that can share information and perform their tasks while working, relaxing or playing sports. The main problems of the Internet of Things include information security and protection of personal data. Internet of Things technologies significantly increase the risks of violating the confidentiality of personal data due to the fact that they involve the accumulation, circulation and use of a large, territorially and technologically distributed amount of information (data) about a particular person. This raises quite natural questions about the reliability of storage of such data and ensuring their protection against unauthorized use. The article also discusses the need to implement EU legal standards on personal data protection defined by EU legislation (Data Protection Package), in particular, Regulation (EU) 2016/679 of 27.04.2016, Directive (EU) 2016/680 of 27.04 .2016 of the European Parliament and of the Council, Directive (EU) 2016/681 of 27.04.2016 19 of the European Parliament and of the Council and making the necessary amendments to the legislation of Ukraine. It should be noted that the norms of these EU legal acts should be applied from May 2018 not only in the EU member states, but also in the countries that cooperate with them.

Keywords: internet of things, control system, cloud computing, security, privacy, encryption, wireless.

1. INTRODUCTION

One of the key factors in the formation of the new paradigm was the rapid transition from the Internet of People to the Internet of Things (Internet of Things). The conditional starting point for the social conceptualization of the Internet of Things is considered to be the period from 2008 to 2009, when the number of devices integrated into the global network exceeded the population of the planet. Of course, the problem of uneven social, technological and economic development between different countries of the world makes some adjustments to assess the global nature of the Internet of Things. But given the fact that there has already been some objectification of the Internet of Things in the system of social relations, we can talk about changing the nature of human activity in production and other processes.

In recent years, new social relations related to the Internet of Things have been actively spreading and developing in the world. The concept of the Internet of Things (IoT) is seen as a growing network of facilities, from industrial devices to consumer goods and services that can share information and perform their tasks while working, relaxing or playing sports.

The term "Internet of Things" was coined by Kevin Ashton in 1999. "Internet of Things" should be understood as complexes and systems consisting of sensors, microprocessors, actuators, local and / or distributed computing resources and software, artificial intelligence programs, cloud computing technologies, data transmission between which is carried out via the Internet, and are intended for the provision of services and work in the interests of legal entities or individuals [1].

We consider it necessary to analyze the existing doctrinal definitions of this term. Studies have shown that the same goal was set in the article by a well-known specialist in the field of information law OA Baranova [2]. Acquaintance with the positions of various researchers (in particular, A. Luces, S. Haller [3], Rose K. [4], Roman Alex [5], Mohamed M. Samy [6], Nurwijayanti. K.N. [7], Asifa Nazir [8], etc.), which are presented in [2], allowed us to see the lack of common, established definition of the term "Internet of Things".

Specific examples of Internet of Things are household appliances (alarm clock, air conditioner, refrigerator, coffee

maker, washing machine, etc.), home systems ("smart home" system, garden watering system, lighting system, security system, including surveillance cameras), various sensors and sensors (thermal sensors, light sensors, traffic), telecommunications devices (including routers and Wi-Fi access points), as well as elements of traffic control infrastructure (traffic lights). The most primitive IoT system consists of a sensor that includes the hardware, its software, the data transfer technology between the device and the system, and the system itself that receives the data. Receipt and exchange of information is carried out by two methods: identification system; data transmission technology between the sensor and the system.

Many countries pay considerable attention to the formation of public policy in the field of the Internet of Things: the United States: the decision was made to develop a national strategy for the Internet of Things (2016); the bill "Development of innovations and promotion of the Internet of Things" was submitted to the Senate (January 2017); Great Britain - adopted "Digital Strategy of Great Britain 2017"; South Korea - the IoT Master Plan (2014) was adopted; Japan - adopted "Japan Growth Strategy - 2016" (Industry 4.0, IoT development, big data, robotics); China - a state program for the development of the Internet of Things ($ 127.5 billion) until 2020 has been developed and is being implemented; it is planned to transform 500 cities into smart cities (2017); UAE - Minister of Artificial Intelligence appointed (October 2017) [9].

2. RESEARCH METHODOLOGY

To achieve this goal, a number of scientific methods were used, namely: theoretical - to study and analyze the national and international methodology for regulating the Internet of Things; logical analysis - to formulate basic concepts and carry out a classification; concrete historical - to demonstrate the dynamics of analytical work; dialectics - to determine the content and characteristics of the constituent elements of the Internet of Things; empirical methods - to summarize the best practices of the G20 countries. We searched PubMed and Mecs-press for articles on leading the value and use of the internet of things during the pre-trial investigation of criminal offenses. The purpose of the scholarly article was to provide non-technical readers with a non-professional explanation of the machine learning methods used in world today.

3. RESEARCH RESULTS

The possibilities of the Internet of Things are also considered in terms of use by law enforcement and the military. In particular, today's technical capabilities to detect the enemy and the availability of high-precision weapons force high mobility and rapid decision-making. This is possible only with the prompt receipt of information from various sources in real time by all units involved in the operation. One way to solve this problem was to use solutions called the Internet of Battle Things (IoBT). The capabilities of the Internet of Warfare include the collection and processing

of any useful information; it acts as an agent to help coordinate defensive actions; provide management and logistical support of combined operations; monitor the condition of vehicles, environmental monitoring. It should be noted that in 2016, the Netherlands became the first country in the world to fully cover itself with a national network for the Internet of Things. The idea is based on the creation of an energy-efficient network that would allow the transmission of small amounts of information over long distances [10].

The use of the Internet of Things can also provide a qualitatively new level of crime prevention, as evidenced by foreign experience. Thus, in the United States, the Internet of Things is not only used in practice to prevent crime, but is also seen as one of the elements of artificial intelligence. The idea of this project is that the crimes are relatively predictable, but it is necessary to analyze the relevant data in a short period of time. This type of analysis was technologically impossible several decades ago, but the situation has changed with the advent of the Internet and the development of information technology. At the same time, the use of the Internet of Things is envisaged both to detect crimes and to prevent them. This is achieved primarily by making the city's infrastructure "smarter" and more connected. And this, in turn, allows you to receive information in real time - from CCTV cameras to special sensors. At the same time, the level of technical capabilities of video cameras, sound and other sensors has increased significantly. For example, the new generation of cameras is able to better scan license plates on cars, perform face recognition to search for potential criminals or missing people, as well as automatically detect suspicious situations, such as left unattended various objects in public places, and others. Video surveillance also allows you to analyze human behavior [5].

A separate area of development of the Internet of Things to prevent crime is the use of sensors to track gunshots. The technical capabilities of the equipment allow to recognize the type of weapon, location, to form an appropriate database [11].

Another way to use the Internet of Things to prevent crime is unmanned aerial vehicles. It should be noted that in 2012, the US Federal Aviation Administration gave permission to law enforcement agencies to train operators of unmanned aerial vehicles. The use of unmanned aerial vehicles for general surveillance, detection of potentially dangerous situations, search for people, control of the traffic situation and other needs of law enforcement agencies is envisaged. In general, they should fill the gaps in video surveillance and create conditions for fast and high-quality information [12].

The use of the Internet of Things with the involvement of unmanned aerial vehicles for crime investigation and crime prevention is also practiced by the British police. The main tasks that are solved, in particular, are: the implementation of photo and video recording of crimes, manifestations of antisocial behavior, traffic accidents, assistance in the search for missing persons, etc. The information obtained can be

used in court, for example, to demonstrate the crime scene to a jury. It is also important that the use of unmanned aerial vehicles is much cheaper than the use of helicopters.

Internet of Things devices connect and interact using standard data protocols over wireless and wired networks at various levels, namely: HHTP / HTTPS, TCP, UDP, IP, XMPP, Ethernet, ICMP, Telnet and others. There are also new protocols of interaction between "things", which aim to ensure data transmission in low-speed wireless communication, examples of which are: MQTT, ZeroMQ, ZigBee, WirelessHART, CoAP [13, 14]. The Internet of Things has the following architecture (Figure 1):
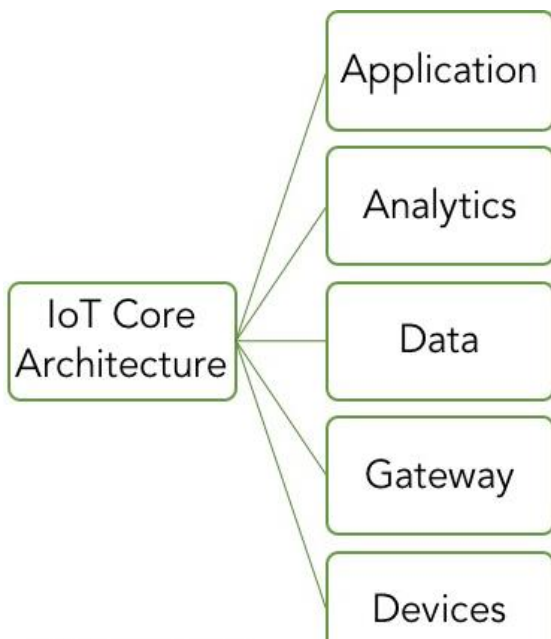

Figure 1 The IoT Core Architecture

Integration with the Internet involves assigning its own IP address to each "smart" device and its subsequent use as an identifier, forcing the use of IPv6 instead of IPv4, due to the limited number of unique addresses of the latter. Several technologies are needed to integrate everyday things into a network. Simple, compact technology is required to identify each object. Only in the presence of a system of unique identification can collect and accumulate information. This jobs can be provided using RFID chips which they are able to transmit information to readers without their own current source. Each chip has an individual number. As an alternative to this technology, QR codes can be used to identify objects. GPS technology, which is effectively used today in smartphones and navigators, is suitable for determining the exact location of a thing. Objects must be equipped with sensors to monitor changes in the state of an element. An embedded computer must be used to process and store sensor data. Wi-Fi, Bluetooth, ZigBee, 6LoWPAN - wireless technologies can which be used to exchange information between devices [15]. Network Media - Internet integration

means that devices will use an IP address as a unique identifier.

However, due to the limited address spaces in IPv4, IP facilities will have to use IPv6, which provides unique network-level addresses of at least 300 million devices per capita. Objects in IP will be not only devices with sensory capabilities, but also devices that perform actions (for example, light bulbs or locks, which are controlled via the Internet). To a large extent, the future of the Internet of Things will not be possible without IPv6 support, so the global implementation of IPv6 in the coming years will be crucial for the successful development of IP in the future.

The main interest in this sense is the IEEE 802.15.4 standard, which controls access for the organization of energy-efficient 46 personal networks, and is the basis for such protocols as ZigBee, WiFi, Bluetoot [16, p. 69].

ZigBee has features such as low power consumption, low data rate, low cost and high bandwidth. Currently, ZigBee is used mainly in the transfer of information between various things of electronic equipment, which are within a short distance and the data rate is not very high. This technology is very well suited for transferring large amounts of data over a wireless network between devices, but it also requires a lot of power to operate and has a low level of data throughput. When using this technology, you will need to replace the batteries in all devices on a regular basis [16, p. 69].

Bluetooth is a wireless technology used to transfer data over personal networks. It transmits data on the frequency band from 2.4 to 2.485 GHz and operates at shorter distances than Wi-Fi. You can sync a couple of devices such as phones, headphones, speakers, computers and more. With the development of Bluetooth v 4.0, it became possible to implement the function of low power consumption and increased range up to several tens of meters [16, p. 69].

Among the leading technologies, PLC solutions play an important role in the spread of the Internet of Things - technologies for building data transmission networks over power lines, as many applications have access to power grids (eg, vending machines, ATMs, smart meters, lighting controllers first connected to the power grid). PLC, being an open protocol standardized by the IETF, is noted as particularly important for the development of the Internet of Things.

Technologies that enable the implementation of the Internet of Things solve four main tasks: identification, data collection, data storage and information exchange. It should be borne in mind that this causes certain consequences, in particular [11, 12]: continuous monitoring becomes a big part of the life of the average person; getting the right and enough information about the things that people interact with, at any time; voice command creates a whole "army of cyber servants"; communication of devices with artificial intelligence - "computerization" (Computication); sensors and observations of movements and even human eyes, more advanced machine learning algorithms will make interaction

with technology more convenient; in production it can improve the speed and quality of production of goods and services, change business models; growth of mutual level of trust in society; increasing the participation of citizens in important social and political events and organizations; creation of expert networks for the development of specialized projects (government orders), thus facilitating reforms in various spheres of society (e-education, e-medicine, e-commerce, etc.) based on the consolidation of resources of all public sectors, as well as their equality [17, 18] (Figure 2).
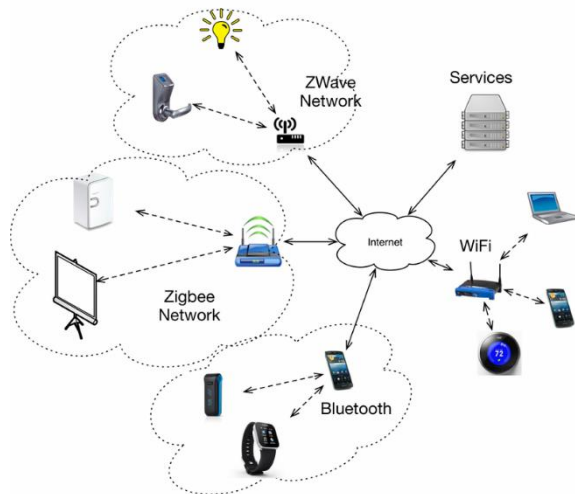

Figure 2 The state of the IoT network architecture

4. DISCUSSION OF RESULTS

At the same time, the widespread use of Internet of Things technologies will lead to the emergence and further identification of many new problems related to personal data protection (Internet of Things technologies significantly increase the risks of personal data breach due to the accumulation, circulation and use of large technologically distributed amount of information (data) about a particular person). It will be more difficult to maintain your privacy and privacy because users will compromise, sometimes reluctantly, to gain access to any important information.

The most important group of risks will be legal problems, which will be due to the emergence of a fundamentally new set of social relations based on the use of Internet of Things technology [19]. This will be associated primarily with the emergence and implementation of legal relations that will arise in the process of using the technology of the Internet of Things with elements of artificial intelligence; legal mechanisms for regulating the infrastructure security of the introduction and use of Internet of Things technologies; ensuring

cybersecurity in case of cross-border use of such technologies; use of radio frequency resource in the conditions of mass use of radio devices, ensuring confidentiality, as well as protection of personal data, etc.

In our opinion, the main problems of the Internet of Things include information security and protection of personal data. Internet of Things technologies significantly increase the risks of violating the confidentiality of personal data due to the fact that they involve the accumulation, circulation and use of a large, territorially and technologically distributed amount of information (data) about a particular person. This raises quite natural questions about the reliability of storage of such data and ensuring their protection against unauthorized use.

5. CONCLUSIONS

According to our estimates, the results of the study of the problem of data collection in the use of Internet of Things technologies allow us to draw some conclusions: protection against unauthorized use; b) the widespread use of Internet of Things technologies leads to the need to address the following main legal issues: the definition of mechanisms for implementing the principle of prior consent to the use and removal of personal data; regulation of the procedure for the use of personal data by intellectual complexes operating without the participation of legal entities or individuals; the need to create a multilevel and multi-object system of personal data protection and regulation of cross-border flows of personal data in the context of Ukraine's European integration.

Regarding the latter, it is necessary to implement EU legal standards on personal data protection defined by EU legislation (Data Protection Package), in particular, Regulation (EU) 2016/679 of 27.04.2016, Directive (EU) 2016/680 of 27.04. 2016 of the European Parliament and the Council, Directive (EU) 2016/681 of 27.04.2016 19 of the European Parliament and the Council and making the necessary changes to the legislation of Ukraine [20; 21]. It should be noted that the norms of these EU legal acts should be applied from May 2018 not only in the EU member states, but also in the countries that cooperate with them.

The introduction of the Internet environment in all spheres of human life can potentially change many surrounding objects, lead to global economic, political and universal transformations. The introduction of the Internet of Things in Ukraine in the relevant types of economic activity will significantly reduce the lag in economic development from the advanced industrialized countries of the world.

REFERENCES

[1]   1Tribune of comparative and international law, Tribuna Juridica, available at: tribunajuridica.eu

[2]   Baranov, O.A. (2016) "Internet of Things" as a legal term", *Yurydychna Ukraina*, no. 5-6, pp. 96–103.

[3]   Haller, S. (2010), "The Things in the Internet of Things", *Poster paper presented at Internet of Things Conference*, Tokyo, Japan, available at: http://www.iot2010.org.4/

[4] Rose, K. Eldridge, S. and Chapin, L. (2015), "The Internet of Things: An Overview", *Understanding the Issues and Challenges of a More Connected World, The Internet Society (ISOC),* October, available at: https://www.internetsociety. org/sites/default/files/ISOC-IoT-Overview2015

[5] Roman Alex F. Lustro (2021), "Modified Key Derivation Function for Enhanced Security of Speck in Resource-Constrained Internet of Things", *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 13, no. 4, pp. 14-25. DOI: 10.5815/ijcnis.2021.04.02

[6] Mohamed M. Samy, Wagdy R. Anis., Ahmed A. Abdel-Hafez and Haitham D. Eldemerdash (2021), "An Optimized Protocol of M2M Authentication for Internet of Things (IoT)", *International Journal of Computer Network and Information Security (IJCNIS),* vol. 13, no. 2, pp. 29-38. DOI: 10.5815/ijcnis.2021.02.03

[7] Nurwijayanti K.N. and Rhekaz Eka Adhytyas (2021), "Garbage Bin Monitoring System Based on the Internet of Things at University Dirgantara Marsekal Suryadarma", *International Journal of Education and Management Engineering (IJEME)*, vol. 11, no. 2, pp. 1-12. DOI: 10.5815/ijeme.2021.02.01

[8] Asifa, Nazir Sahil, Sholla and Adil, Bashir (2021), "An Ontology based Approach for Context-Aware Security in the Internet of Things (IoT)", *International Journal of Wireless and Microwave Technologies (IJWMT),* vol. 11, no. 1, pp. 28-46. DOI: 10.5815/ijwmt.2021.01.04

[9] Mohylnyi, S.B. (2016), *Tekhnolohii «Internetu rechei» - pidhotovka fakhivtsiv aktualno v chasi. Zbirnyk materialiv MNK* [Technologies of the Internet of Things - training of specialists is relevant in time. Collection of MNC materials. 2016], Ukrainian.

[10] Baranov, O.A. $ Bryzhko, V.M. (2016), "Protection of personal data in the field of Internet of Things", *Informatsiia i pravo*, no. 2 (17), pp. 85-91.

[11] Evans, D. (2011), "The Internet of Things. How The next Evolution of the Internet Is Changing Everything", *CISCO white paper*, p. 11, available at: http://www.cisco.com/web/about/ac79/docs /innov/ IoT_IBSG_0411FINAL.pdf

[12] Advancing the Internet of Things in Europe Accompanying the document 19.4.2016 SWD (2016), 110 final, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52016SC0110

[13] Kovalenko, L.P. (2012), *Teoretychni problemy rozvytku informatsiinoho prava Ukrainy: monohrafiia* [Theoretical problems of development of information law of Ukraine: monograph], Pravo, Kharkiv, Ukraina.

[14] Kormych, B.A. (2003), *Orhanizatsiino-pravovi zasady polityky informatsiinoi bezpeky Ukrainy: monohrafiia* [Organizational and legal principles of information security policy of Ukraine: monograph], Yuryd. l-ra, Odesa, Ukraina.

[15] Arquilla, J. and Ronfeldt, D. *The Advent of Netwar*, available at: https://www.rand.org/pubs/monograph_ reports/MR789.html

[16] Rolf H. Weber (2010), *Governance of the Internet of Things*, Legal Perspectives, Springer-Verlag Berlin Heidelberg.

[17] Bondarev, O. Lectures. What is the Internet of Things and why do you need it?, available at: http://nv.ua/ukr/science/lectures/lektorijshcho-take-internet-rechej-i-navishcho-vin-potriben-1326653.html

[18] Nalinsak, Gnotthivongsa Huangdongjun, Khamla Non Alinsavath (2020), "Real-time Corresponding and Safety System to Monitor Home Appliances based on the Internet of Things Technology", *International Journal of Modern Education and Computer Science(IJMECS)*, vol. 12, no. 2, pp. 1-9. DOI: 10.5815/ijmecs.2020.02.01

[19] The Societal Impact of the Internet of Things. A report of a workshop on the Internet of Things organized by BCS – The Chartered Institute for IT, on Thursday 14 February 2013. The Chairs were Jeremy Crump (BCS) and Ian Brown (Oxford Internet Institute, University of Oxford), available at: https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf

[20] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Amendment to Convention ETS No. 108 allowing the European Communities to accede. Strasbourg, 28.1.1981. (Article 5 – Quality of data) , available at: http://www.convention. coe.int/treaty/en/ Treaties/Html/108.htm

[21] 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 (General Data Protection Regulation): Regulation (EU) 2016/679 of the European Parlament and of the council of 27 April 2016, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R06 79&from=