ATLANTIS PRESS

Advances in Social Science, Education and Humanities Research, volume 298

2nd International Conference on Education Science and Social Development (ESSD 2019)

Intellectualization Risk Analysis of the IoT Components and Technology as Objects of New Legal Relations

Igor L Kaftannikov
Federal State Autonomous Educational Institution of Higher Education
"South Ural State University (National Research University)"
Chelyabinsk, Russia

Vlada M Zhernova
Federal State Autonomous Educational Institution of Higher Education
"South Ural State University (National Research University)"
Chelyabinsk, Russia

Alexey V Minbaleev
The Institute of State and Law
Russian Academy of Sciences
Moscow, Russia

***Abstract*-The article describes the processes of alienation of industrial activity from a person and analyzes the associated risks of different categories of objects included in the system of industrial Internet of things or operated with the introduction of digitalization. One of the main challenges facing the legislator today in the field of the Internet of things of any direction is the task of identifying entities that are now indirectly responsible for the possibility of new risks of production processes and its provision. In addition, it is necessary to pay special attention to the problems of damage in the incorrect functioning of objects involved in the Internet of things, both legal entities, individuals and the state as a whole in case of violation of the operation of critical information infrastructure.**

Keywords-industrial internet of things, risks of technological processes, responsibility in the sphere of internet of things

I. INTRODUCTION

Modern achievements of information technologies, designated as the Internet of things (IoT), have made it possible to formulate recommendations on the global technical and technological development of society, presented, in particular, by the programs "Digital economy of the Russian Federation" and "Industry 4.0" (Germany) [1,2,3].

The first program defines the goals and objectives within the 5 basic directions of development of the digital economy in the Russian Federation for the period up to 2024th. The basic directions include regulatory, personnel and education, the formation of research competencies and technical reserves, information infrastructure and information security. The main directions of the second program are defined as "management of complex systems", "resource Efficiency", "Education and training", "Standardization and creation of reference architecture" [4]. In 2015-2017th recommendations on smart services - Smart service Welt 2025 and Smart Service Welt II were additionally published [5,6].

Considering undoubted prospects of new technical solutions in this direction, it is necessary to take into account that, in contrast to locally operating machines, devices or their combination, performing their functions under the control and control of people, the conglomerate of automatically working and interacting devices has increased risks of possible consequences of using incorrect or inaccurate models, formalization procedures, the presence of algorithmic errors and inaccuracies, programming errors and incorrect functioning of technical devices, data processing or transmission respectively. These errors and inaccuracies can significantly affect the correct flow of implemented technological processes, business processes and processes of human existence in general.

The main idea of the Internet of things is to combine local devices that perform various actions into some conglomerates with the expansion of sensor technology, functionality, quality and properties. Moreover, the corresponding increase in the intelligence of actions and decisions is carried out without or with minimal human involvement. It is obvious that the withdrawal of a person beyond the scope of action control, decision-making, forecasting the consequences, comparing the results with the target values, ultimately changes the forms, formats and the very essence of human relations and technical mean that implement these functions. At the same time, zones of formation and occurrence of various risks appear and expand, for example, because of possibly different approaches to intellectualization and interpretation of situations of interaction of industrial conglomerate and the IoT components produced by different suppliers operating at different technological sites. It is also necessary to take into account the use of initially different systems of knowledge representation and algorithms of data processing as well as methods of automatic generation of conclusions for decision-making and subsequent actions.

Thus, on the one hand, the task of initial coordination of a set of factors of knowledge representation, construction of a complex of the coordinated models of functioning and interaction of a conglomerate of devices, and also intersystem and human-machine interfaces for cumulative estimation not just of a condition of separate objects, and the situations including actions of sets of devices and people is designated. On the other hand, there are many issues of regulatory and legal regulation of the use of systems and technologies of the Internet of things in the lives of people, things and industry. Even ethical issues are beginning to be discussed.

II. STRUCTURING RISKS AND THE LEGAL RELATIONS

The main feature and the main problem of cyber-phisical systems (further – CPS) participation in the activities carried out earlier only by a person is the transfer of intellectual components of human activity in the CPS environment with all the ensuing consequences. While this is happening to a minimum extent, but the entire experience of the development and dissemination of information technology predicts explosive development. Humanity must be ready and work ahead of the curve.

In the examples presented as Industry 4.0, production activities are mainly carried out by one or more CPS complexes. Artificial objects such as production tools, machines, equipment, conveyors, etc., jointly solve the problems of production activities while having a level of intelligence which was previously the prerogative of only subjects, that is, people with their intelligence. And many parameters of CPS exceed the parameters of human activity. However, such actions and results may also be more or less exposed to risks similar to human activities. And the main problem now, when embedding CPS-activities in the human world, is the lack of actors who were given full responsibility for the implementation of any activity and obtaining the necessary results. Therefore all legally significant rules, actions, regulations, laws and other elements of legal relations and law enforcement now require a thorough detailed review, adjustment and transformation.

Further, it should be noted the following: one can imagine 2 approaches to reforming the legal framework with respect to CPS:

a) full responsibility of people for all the consequences of human activities in conjunction with cyber-physical systems if it stays in the current legal field. In this case, it is necessary to introduce the concept of indirect responsibility of people for the actions of cyberphysical systems.

b) it is necessary to structure and/or evaluate in any way the actions of cyber-physical systems and the results of these actions (risks, damage, human activities, etc.). Giving certain properties or rights of quasi-subjects of legal relations with the definition of the relevant elements of legal liability to CPS should be in respect of them. For example, limiting the application of any principle of analysis, decision-making, prohibition of any class of CPS or CPS management system with the imposition of certain penalties or restrictive on subjects allowed the development, production or use of CPS of a certain class.

Before analyzing the issues related to the regulation and formation of legal relations arising from the use and application of cyberphysical systems, it is necessary, first of all, to analyze the risks arising from the fact that CPS without human intervention exercise less control over the static state of objects and processes, and more - control of situations in the environment. At the same time, it makes certain decisions and perform appropriate actions, changing the current situation .

Risk is understood as "a combination of the probability of causing damage and the severity of the damage" according to [8]. Concretizing this definition, it will be considered the probability of causing damage to the probability of this event for a certain period of time, for example, during the existence of an information system. We denote this probability as v_i. The significance of the damage can be determined in various metrics, for example, when causing harm to human health, in the cost of treatment plus the cost of the salary paid during treatment. We denote the amount of damage as z_i. The combination is defined as the multiplication operation "*". Then the specific risk r can be defined as

$$r_i = v_i * z_i \tag{1}$$

Due to the wide variety of risks, probability and damages, it makes sense to perform some decomposition of the set of risks, which can be further used to improve the system of legal relations.

There are new forms of legal relations that require the formation of new classes of liability regulation with the corresponding correction of the modern legal field [9].

Structurally, according to the levels of risks and legal support of IoT, there are five levels:

1. In the industrial sphere, at the 4th stage of technological development, locally operating components of production processes are combined into a certain system, which should assess the current production situation, change the action plan of local components, transport and logistics subsystems and analyze the results of combined actions and inform the system of a higher level about the current state of the process, the costs of its implementation and the results obtained. At the level of locally operating components, this leads to the expansion of functionality, obtaining technological and control information. In addition, information can be obtained on the reconfiguration of its own technological process to provide a new mode of action, control and inform the system of a higher level of results. Thus, the risks of the level of automation are complemented by the risks of intellectualization:

- increase and expansion of functionality and increase the corresponding risks of its implementation

- risks of migration arising from the migration of equipment; the risks of obtaining the source incorrect control actions reconfigure

- increase of technological risks during the production process
- risks of assessing the results of changed activities

2. A simple structural element of the Internet of things is two or more interacting devices.

The main functions of the elements of such a subsystem are: a) generation or transmission of information; b) execution of actions – the implementation of physical, chemical and other actions or transformations performed in accordance with the received signals/messages (switches, actuators, displays, etc.).

The risks inherent in the first level are typical for this level.

A distinctive feature of this level is the emergence of risks associated with the interaction of components of a simple structural element and the exchange of information with the external environment and the parent subsystem. There are cumulative risks of information exchange (material and information exchange to be processed by a simple structural element):

- The risks of addressing
- Risks of using different interfaces
- Risks of failure to provide the required noise immunity
- Risks of interception and substitution of data
- The risks of incompatibility of data formats

3. A conglomerate /a complex of simple structural elements. The main risks of the third level are the risks of inaccurate assessment of the situation, which are understood as a set of states of simple structural elements and their interactions. There are also risks of interaction between different interfaces, the use of incompatible data formats, the possibility of external influence, because at this level is meant the use of Internet interaction. In most cases a conglomerate / complex is characterized by a single control center that receives signals and manages commands. The main object of vulnerability of such a system in most cases is the center-controller, which is more vulnerable and vulnerable to attacks [10].

4. At the industrial level, the concept of "industrial Internet of things", "smart enterprise", "industry 4.0"is actively used. Such a complex involves multi-level communication, a large number of objects that are part of an enterprise or organization as a certain property complex, a large amount of data transmitted, several control centers that interact with each other. Since there are a lot of devices for receiving/transmitting data, there are a lot of vulnerabilities and opportunities for their implementation [11]. Often, the complex is subject to one of the most common types of attacks - ddos-attack, when some device is overloaded with information flow and cannot cope with its processing. In addition, it is necessary to take into account the risks of the system itself: coarsening models, algorithmic, interference effects, etc., which arise in situations not provided for in the design of the Internet of things systems.

5. The next level, after smart production, it is necessary to consider the risks arising from the inclusion of smart production in the system that provides smart support for business processes, logistics, operation, logistics of created products, support, technical support and interaction with customers. This level is typical for large commercial organizations, as well as for state and transnational organizations.

The proposed level classification of risks reflects the fact that the change in the level (volume) of participation of CPS objects in the implementation of production activities leads to an increase in their share of participation in achieving the result. At the same time, not only the number of risks of the previous level increases linearly, but also there are types and types of risks of the new level, as well as a combination of risks of different levels. In general, the amount of risk is now defined as the number of combinations

$$C_{nk} = N!/K!(N-K)! \qquad (2),$$

this means a nonlinear increase in the total (total) risk attributable to the use of CPS and, accordingly, should be taken into account to determine the responsibility and its metrics.

To reduce the number of possible negative situations and their risks, it is already necessary to form a system of state control, management and legal support of the processes of creation and operation of such systems. At the moment, the concepts related to the Internet of things are contained in the state standards [see, for example, GOST R 57100-2016/ISO/IEC/IEEE 42010:2011 System and software engineering. Description of architecture], which are not normative acts; the basic laws in this sphere [12] do not contain the concepts of the studied sphere, and the programs "Digital economy" and "Industry 4.0" are based on the entities of the sphere of the Internet of things.

The introduction of the terminology of "unambiguous interpretation" in normative legal acts is an integral part of the creation of successful regulations. Therefore, it is necessary to pay special attention to the conceptual apparatus. Some attempts to define the Internet of things at the legal level are presented in the Open concept "Internet of things: legal aspects (Russian Federation)" [13]. Taking into account that certain defined elements of the Internet of things are present in some normative acts of the Russian Federation, it is necessary to consolidate this definition at the legislative level.

The use of elements of all areas of the Internet of things, according to Russian legislation, is possible both in the relations of individuals and legal entities, and in their interaction with public authorities and local self-government, as well as in the interaction of authorities with each other.

Often, legal entities act as independent business structures, representatives of public authorities and local self-government act in civil circulation as, in the direction of the risks of IoT, it makes sense to combine many legal entities and authorities into one group, thus dividing all users at risk of IoT into two groups - individuals and organizations. The division into groups is necessary not only to determine the functionality, volume and quality of the use of IoT (and it is, of course, different), but, first of all, to determine the types and levels of risks of unauthorized situations, as well as the formation of adequate legal support.

In the first case, the object of the threats will be the person using the IoT. Ways of harming can be violation of integrity of work of cyber physical systems which are used by the person directly [14] (personal belongings – IoT), or in the household purposes [15]. In the second case, not individual individuals may be at risk, but industrial enterprises that produce the items, devices, equipment and technologies necessary for the normal functioning and protection of the state and the state institutions themselves.

Thus, in order to form a regulatory and legal framework for regulating the sphere of the Internet of things, it is necessary, primarily at the legislative level, to determine the structure of the Internet of things as a whole and its complex systems, the boundary conditions of such systems (and hence the boundaries of responsibility of manufacturers, operators, users).

Consider the hierarchy of the industrial Internet of things and the possible risks to which the cyberphysical system may be exposed.

The basis of the industrial Internet of things are devices that receive information from the external environment (for example, sensors). The information is then sent to the smart system over a wired or wireless network. The information is analyzed (processed) and then used to make a decision. Information about the further action (inaction) is transmitted to the devices of this or other level, which function depending on the information received. The functions at each level of such a system are different: for example, at the first level it is necessary to obtain the correct source data. it is necessary to prevent the receipt of false data due to forgery, distortion, or incorrect acceptance/reading of information.

At the second level, it is necessary to ensure the correct processing of the data in accordance with the models used and the relevant programs. In case of using the software it is necessary to take into account the factor of appearance/manifestation of errors. Since such a complex system, from the point of view of functional and technical, is a multi-component system, it makes sense to allocate the components of the systems in order to possible detail the legal responsibility for the processing, storage and transmission of information of each of these components, resulting from the incorrect operation of the system, as in the processing of information can occur various kinds of errors: failure errors, algorithmization errors, input errors, etc. In view of the fact that operators of separate components of systems can be different divisions of the organization, it is necessary to distinguish areas of responsibility for the incorrect operation of those or other components of the information system as a whole.

When designing complex information systems, it is necessary to determine the boundaries of parts of the information system, the operation of which is carried out by groups of subjects with different legal status. Control over the performance of duties and the technical component of the work on input, transmission and processing of information is necessary not only for the state, but also for any other information systems.

Unfortunately, at the moment the legal basis for determining legal liability is not sufficient for the above therefore, the relations arising when working with information systems are regulated, first of all, by the norms of the Civil code of the Russian Federation (Chapter 38 of the civil code) [16], but this is clearly not enough, because it will have to determine any levels of intellectualization of the components of the Internet of things. It is necessary to determine the legal status of both the components themselves and the decisions allowed to be taken by these components.

Thus, it can be concluded that when putting into operation information systems based on the ideology of the Internet of things, it is necessary to provide a means of delineating the areas of responsibility of the components of the IoT. Zones can be temporary – untimely performance of duties by operators, spatial – transfer of information from one legally significant subject to another, functional – the correct processing and storage of data, the correct functioning of the processed data.

Kaspersky Lab in the report on cybersecurity of industrial systems noted that 92% of Automated process control systems has vulnerabilities [17]. In this case, it makes sense to talk about a complex risk, since any part of the process control system can be vulnerable, and there are a large number of components of the industrial system, as well as ways of data transfer between them, respectively, the risks increase exponentially. The Russian legislation, if it is necessary to implement a set of measures to detect, prevent and eliminate the consequences of computer attacks on the information resources of the Russian Federation, does not sufficiently define the measures for the survey required before the introduction of systems into operation, or, for example, with the territorial expansion or scaling of the components of automated process control system (APCS).

Most APCS use subjects of critical information infrastructure. It should be noted that such entities include state or commercial organizations that use automated control systems to perform their functions in the field of health, transport, energy, nuclear energy, defense and other industries. Since, often, such entities are not manufacturers / suppliers of ACS components, it is necessary to introduce measures to determine compliance with the quality of the components used, which include both components and software, means of data transmission, etc. and the consolidation of such measures should be in the regulations, to which most of the documents of a recommendatory nature (for example, state standards) do not apply.

Since the APCS already allows to make further decisions on the basis of many input parameters, the next level of decision-making can be considered the intellectual level. And no matter who or what is acting at this level. Modern technologies (artificial neural networks, other methods of artificial intelligence) allow humanity to make a decision based on the methods used, the peculiarities of their implementation and the algorithms used. If the decision is made directly by a person or a group of people, it is necessary to exclude the decision in the presence of subjective factors, or minimize their impact.

It is necessary to realize the possibility of the negative impact of artificial intelligence on humanity since many actions in industrial cyber-physical systems are carried out on the basis of calculations and conclusions of artificial intelligence systems. Since the artificial intelligence system is implemented by complex software, in this case, artificial intelligence is characterized by the same risks as for software development. On the other hand, failures and malfunctioning of such systems can have serious negative consequences, especially in the case of military use.

III. CONCLUSIONS

The article presents a step-by-step analysis of the processes of transformation of the production sphere with the gradual alienation of a person from production activities and shows the transition of risks of technological and operational processes from the sphere of subjects to the sphere of objects of the industrial Internet of things. It is possible to consider the risk as "a combination of the probability of causing damage and the severity of the damage", and on the basis of this definition to classify the risks arising at each level of use of objects and systems included in the Internet of things system. This classification system is necessary for the transformation of the subjective grounds of legal relations arising in the sphere of production, in the object, as well as to demarcate areas of responsibility and relevant rules of the legal personality with the intellectualization of the production.

The use of the latest intelligent technologies on the one hand can significantly increase production capacity and reduce costs. But on the other hand, it increases the risks and will require the transformation of legal regulation to ensure the procedures of adequate and multifactorial legal relations in the field of the Internet of things. The absence at the present time in the Russian legislation of the norms regulating the relations arising from the implementation and operation of the objects included in the specified area may slow down the process of such implementation and ensure effective operation.

Also quite acute is the question of the introduction of unambiguously understood terminology for unambiguous formation of a circle of objects and subjects of relations arising in this area. In this regard, Russian legislators and legal activists have already begun to take the first steps (for example, the technical Committee "Cyber-physical systems 194"): http://tc194.ru:,). On the other hand, the question of the empowerment and degree of responsibility of persons who are subjects of indirect responsibility has not been studied. In view of the wide spread in the industrial sphere of artificial intelligence systems and decision-making systems, based on algorithms and computer programs, it becomes possible to give legal personality not only to those responsible for the flow of the process, but also objects that implement this process-robots, ACS, artificial intelligence systems, etc.

ACKNOWLEDGEMENT

This research was financially supported by the Russian Foundation for Basic Research in the framework of Project No. 18-29-16014 «The place and role of legal regulation in the development of digital technologies, legal regulation and self-regulation, including taking into account features of branches of law».

REFERENCES

[1] Order of the Government of the Russian Federation of 28.07.2017 N 1632-p "about the approval of the program "Digital economy of the Russian Federation". Approved by order of the Government Russian Federation. [Online]. Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (in Russian);

[2] Digital Enterprise for process industries [Online]. Available: https://www. siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/digitalenterprise.html

[3] Industry 4.0: new challenges and labour market opportunities [Online]. Available: https://foresight-journal.hse.ru/data/2017/12/24/1159810745/0-%D0%9A%D0%B5%D1%80%D0%B3%D1%80%D0%BE%D1%83%D1%87-6-8.pdf

[4] B. Hiller the VI INTERNATIONAL FORUM "Information modeling for infrastructure projects and development of businesses Big Eurasia". Moscow, 7 June 2017

[5] Smart Service World - Innovation Report 2017 [Online]. Available: https://www.digitale -technologien.de/DT/Redaktion/DE/Downloads/Publikation/ssw_publikation_innovationsbericht%202017.html

[6] Smart Service World - Innovation Report 2017 [Online]. Available: https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-service-welt-2-broschuere.pdf?__blob=publicationFile&v=8

[7] GOST R IEC 61508-4-2007. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 4. Terms and definitions.

[8] V.M. Zhernova, Legal regime of information systems. [Online]. Available: http://www.igpran.ru/prepare/a.persons/Zhernova_VM/Zhernova_VM_Dissert.pdf. (in Russian)

[9] How to hack smart home. [Online]. Available: https://www.kaspersky.ru/blog/mwc2018-insecure-iot/19780/. (in Russian);

[10] Anatomy of an Attack on the Industrial IoT. [Online]. Available: https://www.darkreading. com/vulnerabilities---threats/anatomy-of-an-attack-on-the-industrial-iot-/a/d-id/1331097?

[11] Federal law of 07.07.2003 No. 126-FZ "About the connection". " Rossiiskaya gazeta ", N 135, 10.07.2003 (in Russian)

[12] Federal law of 27.07.2006 N 149-FZ "On information, information technologies and information protection". "Rossiiskaya gazeta", N 165, 29.07.2006 (in Russian)

[13] Open concept on legal aspects of the Internet of things [Online]. Available: https://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 (in Russian)

[14] Pacemakers from several manufacturers can be commanded to deliver a deadly, 830-volt shock from someone on a laptop up to 50 feet away, the result of poor software programming by medical device companies. [Online]. Available: https://www.computerworld.com /article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html

[15] Your baby monitor Is an Internet-connected spy cam vulnerable to voyeur sand crooks [Online]. Available: https://boingboing.net/2015/09/08/your-baby-monitor-is-an-intern.html

[16] The civil code of the Russian Federation (part four): Federal law N 230-FZ of 18.12.2006. "Rossiiskaya gazeta", 22.12.2006 (in Russian)

[17] Cyber security of industrial systems: the threat landscape [Online]. Available: https://securelist.ru/industrial-cybersecurity-threat-landscape/28866/ (in Russian)