The Integrated Regulation of a Cyber-Physical System*

Vlada M. Zhernova (0000-0001-7320-6569)[1(*)], and Aleksey V. Minbaleev (0000-0001-5995-1802)[2]

[1] South Ural State University (National Research University), Chelyabinsk, Russia
zhernovavm@susu.ru

[2] Kutafin Moscow State Law University, Moscow, Russia
alexmin@bk.ru

Abstract. The paper focuses on the integrated regulation of cyber-physical systems, which is currently a relevant issue. The IT evolution calls for regulating the process of creating and operating such systems. However, to devise and implement such regulation, one needs to comprehensively analyze its subject matter – the cyber-physical system with all its constituents rather than only the commonly recognized entities. We present a cyber-physical system that reflects the entire composition of its agents and objects, as well as the relations between these entities. The study dwells on the need to create and expand legal, technical, and ethical regulations of these relations. We analyze the existing technical-legal standards governing the creation and operation of cyber-physical systems. In such systems, one needs to protect the information the system utilizes from malicious manipulation. Moreover, we presented recommendations on how to minimize the loss of data that is integral to a cyber-physical system.

Keywords: Cyber-physical system · Law · Technical and ethic regulation

1 Introduction

Today, Russia is facing a conundrum: its regulatory frameworks lack the definition of a cyber-physical system, while the country has a committee dedicated to regulating such systems. A cyber-physical system (CPS) is a complex object comprising digital data (Blazheev & Egorova, 2020), including Big Data, Internet of Things (IoT), smart cities, smart manufacturing, and artificial intelligence (AI) technologies.

Undoubtedly, recent IT developments call for a new technical standard applicable to CPS. The standard will serve as the foundation for legal and ethical norms that regulate newly emerging, CPS-associated relations. A CPS is a complex, organized, multi-level system that cannot be regulated only technically or legally. Therefore, a CPS regulation system must also be complex, multi-level,

and appropriate for its subject matter. The creation and use of a CPS involve multifaceted human-machine interaction and a complex set of human-human, human-technology, human-technology-human, and technology-technology relations. The latter may not involve any human persons at all, which causes a strong controversy. Analysis of CPS as the subject matter of relations arising from its development and operation is a necessary step towards adequate and proportionate regulatory standards.

2 Materials and Methods

CPS features a complex tri-layer structure: (1) physical layer, (2) software layer, and (3) network layer (Rehman, Allgaier & Gruhn, 2018). This is what actually dictates the model of the technical system itself, as well as the regulatory model applicable to the creation and use of such systems. Physical, the system comprises sensors. It would be logical to include *the environment* in the physical layer. Although the environment is not a part of the subject matter of legal relations, it can indeed affect the general operations within the system.

The physical form of a CPS can be included here, too, since CPS as a physical object is a product of personal or corporate work, even if that work involves automation. The next layer comprises a data communication network in the form of various data transmission technologies using appropriate protocols. Currently, the correct implementation and operation of this level determine how the CPS will function in general. The third layer consists of software that utilizes the second layer to collect and process information from the first layer.

A CPS itself, without associated entities, is of no interest for legal regulation. Therefore, one needs to find and systematize the agents of relations arising from the creation and use of a CPS. These include CPS owners, users, end customers, engineers, software developers, and data service providers. All these individuals and organizations interact with each other through CPS. This interaction is subject to a triad of information security requirements, namely the (1) integrity, (2) confidentiality, and (3) accessibility requirements. CPS regulation is undeniably an interdisciplinary issue that must be studied by computer scientists, lawyers, and other researchers. Personal data security is also an urgent issue. While a data leak *per se* is not much of a concern, smart home, IoT, or data from the CPS of critical infrastructures can provide a complete picture of a person's life.

Legal, technical, ethical, and other regulations of CPS should guarantee the physical safety of persons. Information security, cybersecurity, internal compatibility, and the compatibility of external components are no less critical requirements.

Since a CPS is an interdisciplinary product, it needs comprehensive regulation on the part of public authorities and individual associations, unions, self-regulatory organizations, and standardization organizations. Russian regulating authorities should include the *Ministry of Digital Development, Communications and Mass Media* of the Russian Federation, the *Ministry of Economic Development* of the Russian Federation, the *Federal Agency for Technical*

Regulation and Metrology, the *Ministry of Industry and Trade* of the Russian Federation, *Federal Service for Supervision of Communications, Information Technology and Mass Media*, *Technical Committee 194*, and several other associations and alliances in the field of digital development. Internationally, regulations are provided by the relevant authorities and standardization organizations, such as International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), etc.

To date, Russia has ad-hoc regulation of CPS components and technologies, mainly by virtue of national programs such as the *Digital Economy of the Russian Federation* (Government of the Russian Federation, 2019), federal laws *On Personal Data*; *On Information, Information Technology and Information Protection* (Russian Federation, 2006b), *National Technical Initiative* (Government of the Russian Federation, 2016), *Information Society Development Strategy* (President of the Russian Federation, 2017) and other strategic documents regulating the creation and implementation of CPS. Unfortunately, regions are currently only copying the federal laws or are in the initial stages of drafting their own regulations.

3 Results

Technical standards are fundamental to regulating the creation and use of CPS. As of late March 2020, the *Technical Committee 194* has drafted a set of preliminary national standards and submitted them for review. These preliminary standards "seek to optimize the industrial adoption of digital technology in Russia, to help develop high-quality independent solutions, and to ensure the inter-compatibility of such solutions." The number of national standards governing the creation and operation of CPS components on an ad-hoc basis is quite substantial as it already is: Information Technology (Standartinform Rossiiskoi Federatsii, 2019), Information Security Standards Family (Standartinform Rossiiskoi Federatsii, 2013), Robots and robotic devices (Standartinform Rossiiskoi Federatsii, 2012). Emphasis should also be made on the standards dedicated to the software layer of CPS (Standartinform Rossiiskoi Federatsii, 2015). Technical standards of CPS regulation will be focused on further in the paper. Emphasis will also be made on the standards dedicated to the software layer. Besides, humanity has so far realized that CPS and AI need to be governed by codes of ethics, too. This has been showcased by a study carried out by the *European Parliamentary Research Service Scientific Foresight Unit* (STOA) titled *Ethical Aspects of Cyber-Physical System* (Ethical Aspects of Cyber-Physical Systems, 2016). In addition, the US Department of Defense formalized the ethical principles of using artificial intelligence in the military.

Robo-ethics is concerned with the ethical consequences of adopting and using CPS and robots in human and public life; it also searched for solutions to the emerging problems. South Korea was one of the first countries to adopt ethics officially with its *Robot Ethics Charter* of 2017. However, the project came to a halt after a series of discussions. Private ethical initiatives are not uncommon; they are a product of multi-company cooperation to advance the use of AI and consolidate the basic principles of such use. For instance, the *Asilomar AI Principles* seek to create useful intelligence, maintain human values, and protect the privacy of personal data (Asilomar ai principles, 2017).

In recent years, Canada, China, Denmark, the EU Commission, Finland, France, India, Italy, Japan, Mexico, the Scandinavian-Baltic region, Singapore, South Korea, Sweden, Taiwan, and the UAE have issued national strategies pertaining to AI and the promotion of AI technologies. Each of those documents focuses on the individual aspects of AI policies: (1) research, (2) talent support, (3) development of skills and education, (4) public-private cooperation, (5) ethics, (6) coexistence, (7) regulations, (8) data, and (9) digital infrastructure (Dutton, 2018). The documents emphasize the AI-associated issues of ethics.

In the context of CPS and AI, these issues are numerous. The government and the public need to address them. The issues include:

- Unemployment and social stratification caused by CPS and robotics. "Robotization, according to some experts, could render at least half of the existing professions obsolete. Other experts point out that robotization *creates* rather than *destroys* jobs, since the disappearing professions are compensated by the emergence of new ones." (Analytical review of the global robotics market. 2018).
- Replacement of human personality by artificial intelligence. This issue is in the spotlight today because once humans stop seeking, processing, and transmitting information (even if not entirely), they become completely dependent on robots, willing to sacrifice some human freedoms and legitimate interests, as robots take over some human process.
- AI capabilities. Artificial intelligence can surpass human one, which threatens human safety. This is why ethical and various regulatory bodies must impose restrictions on the use and development of artificial intelligence.

The *National Strategy for the Development of Artificial Intelligence until 2030* states, "To incentivize the development and use of AI, legal regulations that govern human-AI interaction need to be adjusted, and appropriate ethical standards shall be in place. However, overregulation of AI may hinder its development and adoption." Thus, the President of the Russian Federation has effectively tasked the responsible agencies to devise legal and ethical regulations for the use of AI. The President, however, noted that overregulation should not take place.

The Government of the Russian Federation drafted *Model Rules* for the use of CPS and AI by government agencies and local governments. The *Rules* could enshrine ethical standards based on the acts of international organizations and the recommendations made by the professional expert community. Besides, the *Rules*

could provide recommendations on their use by non-governmental legal entities, individual entrepreneurs, and natural persons using AI. We believe that such an approach will prevent the coexistence of multiple redundant codes of ethics in public and private sectors (Neznamov & Naumov, 2018; Sinyukov & Egorova, 2019).

The CPS components, as outlined above, can be illustrated by the chart in Figure 1:

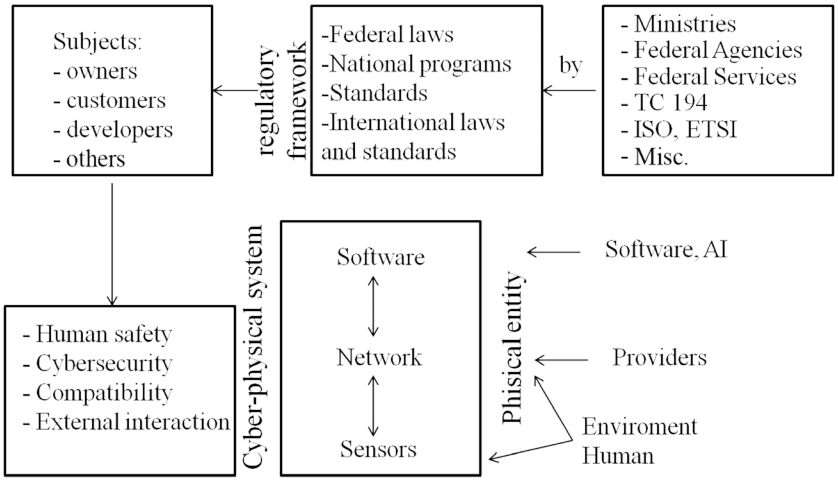

Fig.1. CPS ecosystem chart. *Source:* Compiled by the authors

Thus, the key finding so far is that the CPS ecosystem goes far beyond the generally accepted model.

4 Discussion

Once the CPS components have been identified, one needs to determine the public relations associated with the creation and use of CPS and how to regulate them.

First, we noted that the Russian legislature was amended with the definition of digital rights (Russian Federation, 2006b), a step necessitated by the recent years of digitalization. This concept refers to liability rights and other rights recognized by law as digital rights, the scope and conditions of which are established within an information system compliant with the law. The change is also evident in the form of transactions, which are now taking more diverse forms, including by electronic or other technical means capable of reproducing the transaction volume on an exact paper medium, with any method that reliably identifies the signer.

These innovations lead to the generation of various information in large volumes, which is facilitated by new sensors that collect and process information. This requires the regulation of massive amounts of information, an issue already reflected in legislative efforts for enacting appropriate regulations in their bills.

ISO has already introduced technical regulations, releasing a series of standards for big data reference architecture starting in 2018 (International Organization for Standardization, 2019). In particular, the preliminary national standard (PNST), entitled *Information Technology. Big data. Reference architecture (Preliminary national standards of the Russian Federation, 2020)* is based on *ISO / IEC 20547-3 Information technology. Big data reference architecture. Part 3. Reference architecture*.

Big Data is generated using sensors and transmitted through the communication channels to another part of the CPS for processing. Data transmission is protocol-driven. Notably, IoT or data communication between independent objects is integral to CPS. Unfortunately, while the technology has long been used, it still lacks unambiguous legal and technical regulation. *Technical Committee 194* drafted the regulations titled *Information technology. Internet of Things. General provisions* (Preliminary national standards of the Russian Federation, 2020), which defines IoT as an infrastructure comprising interconnected entities, systems, and information resources plus services that enable processing physical and virtual world data and responding to it. More PNSTs are being discussed.

Intra-CPS data transmission requires the identification of facilities. This is facilitated by *GOST R ISO / IEC 29161-2019 Information technology. Data structure. Unique identification for the IoT*. Besides, technical requirements for electronic identification are laid out in NIST *Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management*.

Whilst human-human or people-to-people (P2P) interaction is regulated by the Civil Code of the Russian Federation, including intellectual property relations, contractual law, etc. Business interactions are also partly covered by it. Regulations on the interaction between physical and virtual entities are still being drafted, even though the process of such interaction and its outcomes do already affect human persons. Therefore, intra-CPS data transmission needs particular emphasis.

Data transmission is provided by appropriate service providers. In this regard, information law has long identified the problem of information provider liability; however, the information intermediary as a concept was first defined in Russia in Article 1253.1 of the Civil Code, rather than in information-related laws.

Data transmission is controlled by protocols. Earlier data communication between computers was mediated by the OSI networking model that enabled different devices to communicate. This is a seven-level model, and each level has its own functions that ultimately enable error-free data communication from the query received by the database to the response delivery via fiber optical fiber.

The data transmission model for CPS can and has to change. The network level of the OSI model features certain protocols – IP/IPv4/IPv6 (Internet Protocol), IPX (Internetwork Packet Exchange), X.25, CLNP, and IPsec (Internet Protocol Security). More protocols are employed to organize data communication: DDS (Data Distribution Service), UDP, CoAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), MQTT

(Message Queue Telemetry Transport), and TCP. MQTT has served as a foundation for MQTT-SN, a specialized protocol for sensor networks.

IoT protocols are strikingly diverse. As the technology advanced, the OSI model had to be reviewed; it now comprises eight layers. The desire to optimize and improve the quality of data transmission has led to the emergence of novel types of data communication networks (e.g., mesh networks). A characteristic feature of CPS networks is that they communicate in small data packages – a phenomenon covered in the recently adopted NB-IoT standard (GSM Association, 2019), that describes an LTE-based cellular technology for low-power, low-data stationary devices.

CPSs carry out a multitude of transactions, which has unavoidably drawn the attention of malicious users. Thus, *the UK Department for Digital, Culture, Media & Sport* published its *Code of Practice for Consumer IoT Security* to improve the cybersecurity of CPS users and lists several security guidelines: (1) not using default passwords, (2) regular software updates, (3) making systems more robust, etc. The document also introduces the concept of *security-sensitive data*, which differs from other types of sensitive data. Security-sensitive data could include, for example, cryptographic initialization vectors. This *Code of Practice* is based on ETSI's *Cyber Security for Consumer IoT*.

5 Conclusion

Despite the recommended security measures in place, CPS networks are not safe from integrity, confidentiality, and accessibility breaches that lead to:

- Decrease in personal privacy with the growth of the Internet;
- Excessive regulation of the flow of private information can lead to a delay in the use of CPS;
- The difficulty of receiving user privacy notices on connected devices;
- IoT giving non-governmental organizations access to bulk personal data (Rither & Hoxie, 2017).

Even where there are data protection regulations and documents in place (European Parliament and Council of the European Union, 2016), there is no guarantee of complete and uncompromised data protection. For this reason, scholars advise analyzing the security requirements and tailoring the security measures for each CPS individually (Rehman et al., 2018).

CPS is a complex system made by humans for humans, but wrong use could be problematic. Therefore, it calls for appropriate regulations, including technical, legal, and ethical standards.

Acknowledgement

This study was funded by RFBR, project number 18-29-16014, project number "Role and Functions of Legal Regulation in the Advancement of Digital Tech:

Legal Regulation and Self-Regulation in the Context of Law Branches and Their Specifics".

References

Asilomar ai principles. (2017). *Future of life institute*. Retrieved from: http://robopravo.ru/matierialy_dlia_skachivaniia#ul-id-2-3

Blazheev, V., & Egorova, M. *Digital Law: Study.* Moscow, Russia: Prospect.

Dutton, T. (2020). *An overview of national ai strategies.* Retrieved from: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd.

Government of the Russian Federation. (2016). *Decree of "On the Implementation of the National Technological Initiative"* (April 18, 2016 No. 317). Moscow, Russia.

Government of the Russian Federation. (2019). *Decree of "On the system for managing the implementation of the national program 'Digital Economy of the Russian Federation'"* (March 2, 2019 No. 234). Moscow, Russia.

GSM Association. (2019). *NB-IoT deployment guide to basic feature set requirements.* Retrived from: https://www.gsma.com/iot/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf

European Parliamentary Research Service Scientific Foresight Unit (STOA). (2016). *Ethical Aspects of Cyber-Physical Systems.* Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU%282016%29563501_EN.pdf

Information technology. Big data. Overview and vocabulary. (2019). ISO/IEC 20546:2019 from February, 2019. Geneva, Switzerland: International Organization for Standardization.

Information technology. Data structure. Unique identification for the Internet of Things. (2019). HOST R ISO / IEC 29161-2019 from March 01, 2020. Moscow, Russia: Standartinform Rossiiskoi Federatsii.

Information Technology (IT). Security methods and tools. Information Security Management Systems. General overview and terminology. (2012). HOST R ISO / IEC 27000-2012 from December 01, 2013. Moscow, Russia: Standartinform Rossiiskoi Federatsii.

Neznamov A. V., & Naumov V. B. (2018). *Strategy for the regulation of robotics and cyberphysical systems.* Retrieved from: https://zakon.ru/magazine/zakon/496

Sinyukov V. N., & Egorova M. A. (2019). *Legal regulation of the digital economy in modern conditions of high-tech business development in the national and global context.* Moscow, Russia: Prospect.

Technical committee 194 of "Cyber physical systems". (2019). *Preliminary national standards of the Russian Federation by technical committee*. Retrieved from http://tc194.ru/publichnoe_obsuzhdenie_proektov

President of the Russian Federation. (2017). *Decree of "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 – 2030"* (May 09, 2017 No. 203). Moscow, Russia.

Rehman S., Allgaier C., & Gruhn V. (2018). Security requirements engineering: A framework for cyber-physical systems. *International Conference on Frontiers of Information Technology (FIT).*

Rither, A., & Hoxie, C. (2017). Legal Considerations of Cyber-Physical Systems and the Internet of Things: Foundations, Principles and Applications. *Security and Privacy in Cyber-Physical Systems: Fundamentals, Principles and Applications, 2*, 93-115. DOI: 10.1002/9781119226079.ch5

Robots and robotic devices. Terms and Definitions. (2012). HOST R 60.0.0.4-2019/ISO 8373:2012 from September 01, 2019. Moscow, Russia: Standartinform Rossiiskoi Federatsii.

Sberbank. (2019). *Analytical review of the global robotics market.* Retrieved from: https://www.sberbank.ru/common/img/uploaded/pdf/sberbank_robotics_review_2019_17.07.2019_m.pdf

System and software engineering. The content of information products of the life cycle of systems and software (documentation). (2015). HOST R 56713-2015 from August 01, 2016. Moscow, Russia: Standartinform Rossiiskoi Federatsii.

System and software engineering. Software testing. Part 1. Concepts and definitions. (2016). HOST R 56920-2016/ISO/IEC/IEEE 29119-1:2013 from June 01, 2016. Moscow, Russia: Standartinform Rossiiskoi Federatsii.

European Parliament and Council of the European Union. (2016). *General Data Protection Regulation* (April 27, 2016 No. 2016/679). Brussels, Belgium.

Russian Federation. (2006a). *Federal Law of "On Personal Data"* (July 27, 2006 No. 152-FZ, edited by December 08, 2020 No. 429-FZ). Moscow, Russia.

Russian Federation. (2006b). *Federal Law of "On Information, Information Technologies and Information Protection"* (July 27, 2006 No. 149-FZ, edited by June 08, 2020 No. 177-FZ). Moscow, Russia.

Russian Federation. (2006c). *Civil Code of the Russian Federation (part four)* (December 18, 2006 No. 230-FZ; edited by July 31, 2020 No. 262-FZ). Moscow, Russia.